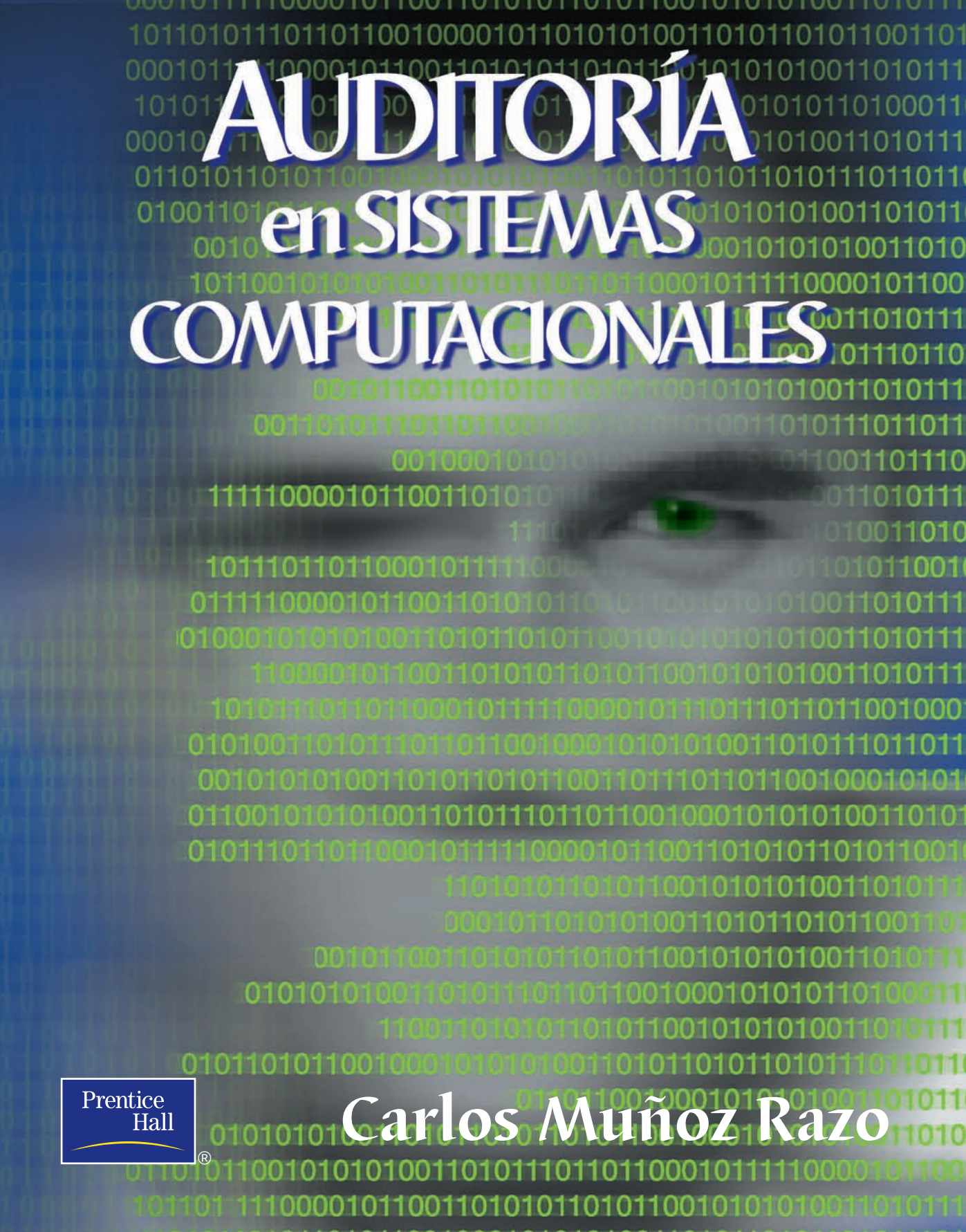
AUDITORÍA en SISTEMAS COMPUTACIONALES



Carlos Muñoz Razo

Prentice Hall®

Auditoría en sistemas computacionales

Carlos Muñoz Razo
Catedrático-Investigador de la Universidad del Valle de México

Revisor técnico
Jorge Rivera Albarrán
Universidad Iberoamericana

Pearson Educación ®

MÉXICO • ARGENTINA • BRASIL • COLOMBIA • COSTA RICA • CHILE
ESPAÑA • GUATEMALA • PERÚ • PUERTO RICO • VENEZUELA

Datos de catalogación bibliográfica

MUÑOZ RAZO, CARLOS
Auditoría en sistemas computacionales

PEARSON EDUCACIÓN, México, 2002

ISBN: 970-17-0405-3
Área: Universitarios

Formato: 18.5 × 23.5 Páginas: 816

Editor: Guillermo Trujano Mendoza
e-mail: guillermo.trujano@pearsoned.com
Supervisor de edición: Antonio Núñez Ramos
Supervisor de producción: José D. Hernández Garduño

PRIMERA EDICIÓN, 2002

ISBN 970-17-0405-3

Impreso en México/*Printed in Mexico*

1 2 3 4 5 6 7 8 9 0 05 04 03 02

Pearson Educación ®

A mi esposa **Mercedes** y mis hijas
Lizeth Mercedes y **Karla Liliana.**

Representan la razón de ser de mi existencia
y son mi fuente permanente de inspiración
y deseo de superación.

A mis padres: **Carlos** (QEPD) y **Rosa.**

Juntos formaron ilusiones en la vida
y las vieron cristalizadas como
familia. Gracias.

A mis hermanos y hermanas, cuñados y cuñadas,
sobrinos y sobrinas.

Compartimos el camino de la vida, el presente
y el porvenir, con
alegrías, entusiasmo y cariño.

AGRADECIMIENTOS

A mis amigos maestros y alumnos de la **Universidad del Valle de México.**

Además de la amistad, compartimos la honorífica vocación de la docencia. Gracias por el permanente intercambio de conocimientos.

(No menciono los nombres de estos amigos, porque podría caer en el pecado de omisión.)

En especial a las academias de sistemas, investigación y administración del Campus San Rafael, y al comité de rediseño de administración 2001 de la UVM.

A los señores **Antonio Núñez Ramos** y **José Hernández Garduño**, y a sus equipos de trabajo.

Gracias por su valiosa aportación de conocimientos, experiencia y voluntad para la revisión técnica y editorial de este libro.

Al **Ing. Salvador Vázquez Amaya.**

Autor del prólogo de este libro, y con quien he compartido muchas experiencias en la docencia, sistemas e investigación.

A la **Universidad del Valle de México.**

Institución de educación superior que a través de la docencia me ha permitido realizar mis anhelos y vocación.

CONTENIDO

PRESENTACIÓN

Es fundamental la operación de los sistemas, es deseable la profesionalización en éstos, y es mejor la especialización en su uso; pero es aún superior la auditoría en sistemas computacionales

Estimado lector, la función de auditoría lleva un largo recorrido en la evaluación de las actividades de las empresas y, en estos tiempos, se ha consolidado como la única profesión reconocida para auditar las funciones, operaciones y resultados de todas las áreas de las mismas; sin embargo, la auditoría de los sistemas computacionales todavía es un campo novedoso, innovador y de aplicación muy reciente, lo cual hace que, en los albores del siglo XXI, esta moderna disciplina sea un territorio parcialmente inédito, del que poco se ha estudiado y del cual se exige una mayor incorporación para revisar las acciones informáticas de las empresas de nuestros días. Precisamente, para subsanar estos aspectos, el libro que tiene en sus manos le presenta los principales cimientos, aplicaciones e instrumentos que le permitirán auditar de manera profesional los sistemas computacionales.

Durante la lectura de este texto encontrará los cimientos teórico-prácticos que fundamentan la aplicación de los métodos, procedimientos, técnicas y herramientas que le habilitarán para realizar, de manera eficaz y eficiente, la evaluación profesional de la administración, el funcionamiento, la utilización y el aprovechamiento de los modernos sistemas computacionales en las empresas; del mismo modo, aplicando las bases de evaluación aquí presentadas, podrá auditar el cumplimiento de las funciones, las actividades, la operación, el desarrollo y la implementación de estos sistemas y de sus responsables, así como la correcta administración, el aprovechamiento, la seguridad y el control de equipos de cómputo, hardware, software, bases de datos, información, periféricos y de todos los componentes relacionados con los recursos informáticos de las instituciones que cuenten con sistemas computacionales.

En el devenir del tiempo, la profesión de auditor se ha fortalecido como la disciplina fundamental para evaluar todas las áreas de las instituciones públicas y privadas, incluyendo los sistemas computacionales. Es por ello que, pensando en la importancia que ha cobrado la evaluación de estos sistemas, el ánimo de este libro fue concebido con las siguientes intenciones:

- La primera es presentar al profesional de auditoría, cualquiera que sea su especialidad en esta materia, los fundamentos teóricos, técnicos y prácticos de la auditoría de los sistemas computacionales, con el propósito de que complemente

su embalaje profesional y aproveche, en la evaluación de los sistemas informáticos, la experiencia, habilidades y conocimientos de su inicial profesión de auditor. Todo ello en aras de una mayor eficiencia y eficacia en la realización de este tipo de trabajos tan especializados, amén de incrementar su potencial profesional en la materia de auditoría que practique actualmente.

- Una segunda finalidad es que se beneficie de los conocimientos informáticos de los profesionales dedicados a los sistemas computacionales, no necesariamente auditores, a fin de proporcionar a quienes ya son especialistas en estos sistemas un acervo teórico, técnico y práctico sobre los aspectos fundamentales de esta especialidad de evaluación, lo cual les permitirá conocer y aplicar los principios y puntos básicos sobre los cuales descansa la práctica de la auditoría, en este caso de los sistemas computacionales.
- El siguiente propósito del libro es presentar este material a los maestros, estudiantes, pasantes y profesionales de las carreras de sistemas, ingeniería, contabilidad, administración y áreas similares, a fin de que adquieran los conocimientos necesarios para capacitarlos en la práctica de esta cada vez más solicitada actividad profesional en el ámbito de los sistemas de cómputo, y con ello fomentar su plena incorporación a esta innovadora disciplina profesional.

La aspiración fundamental del autor es, en todos los casos, mostrar a los lectores, de una manera sencilla, didáctica y fácil de comprender, los cimientos sobre los cuales se apoya la práctica de la auditoría de sistemas computacionales, a fin de que, con los conocimientos aquí vertidos, el profesional universitario que se dedique a esta actividad tenga los elementos necesarios para realizar su mejor práctica de esta especialidad en las empresas, y para que con su estudio pueda incrementar su acervo profesional en materia de sistemas computacionales.

Para llevar a cabo la mejor de las auditorías de los sistemas computacionales en las empresas, en las páginas de este libro encontrará los fundamentos técnicos, teóricos y prácticos de esta especialidad, los cuales se proponen en once aplicaciones que comprende el capítulo 12 de auditorías especializadas en sistemas informáticos, mismas que pueden utilizarse para la evaluación de casi todos estos ambientes de trabajo. Concretamente, se proponen estas especialidades de auditoría:

- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática del área de sistemas
- Auditoría al sistema computacional
- Auditoría alrededor de la computadora
- Auditoría de la seguridad de los sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría outsourcing en los sistemas computacionales
- Auditoría ISO 9000 a los sistemas computacionales

- Auditoría ergonómica de los centros de cómputo
- Auditoría integral a los centros de cómputo

De conformidad con esta propuesta de división de las principales formas de evaluación de los sistemas de cómputo, el auditor puede identificar, adoptar, cambiar o complementar el tipo de auditoría especializada que sea de su preferencia, para ajustarla al tipo de auditoría que requiera practicar a los sistemas. Asimismo, puede elegir entre seguir los puntos e instrumentos de evaluación que se sugieren en cada categoría de las auditorías señaladas, o modificarlos de acuerdo con sus necesidades específicas de evaluación.

Amable lector, el libro que tiene en sus manos es un documento innovador para la práctica de esta especialidad de auditoría. En su contenido encontrará los elementos que le ayudarán a reforzar, adquirir o especializar sus conocimientos en materia de auditoría de sistemas computacionales, capacidades que pueden ser empleadas con mucho éxito en disciplinas profesionales como contabilidad, ingeniería, administración y áreas similares de responsabilidad, a fin de que pueda hacer una acertada evaluación de sistemas computacionales en las empresas de nuestro tiempo.

El equipo responsable de esta publicación desea que la lectura de este libro sea el vehículo profesional que le permita traspasar las fronteras del éxito en esta novedosa especialidad que hoy demandan las empresas.

Cualquier comentario acerca del contenido de este libro, el autor pone a su disposición las siguientes direcciones electrónicas:

cmuñoz@uvmnet.edu, cmunrazo@prodigy.net.mx.

Carlos Muñoz Razo

PRÓLOGO

La apertura cada vez mayor que México está dando a las empresas nacionales e internacionales, el uso creciente de las tecnologías de información como herramienta para lograr ventaja competitiva, y tratar de controlar, a través de sistemas computacionales, el creciente volumen de transacciones generadas por las actividades comerciales y financieras de las instituciones mexicanas, han hecho que se requiera una vigilancia y evaluación constantes de estos sistemas.

Al respecto, el autor nos presenta, en forma sencilla e interesante, los métodos y las técnicas que todo auditor, o toda persona interesada en la auditoría de sistemas computacionales, podría necesitar para diagnosticar el desempeño y desarrollo de dichos trabajos.

Además, el autor nos narra, en forma clara y amena, los orígenes de la actividad de auditor, profesionista independiente capaz de dictaminar sobre la veracidad y confiabilidad de los registros de las operaciones comerciales y financieras de las instituciones. Asimismo, nos menciona que la primera auditoría nació desde el momento en que surgió la necesidad de rendir cuentas de algún negocio y revisar que éstas fueran correctas. Dicha función fue evolucionando conforme crecía la actividad de registro de operaciones mercantiles.

Es de llamar la atención la forma en que el autor narra los antecedentes de la auditoría financiera, administrativa, operacional y de sistemas a través de investigaciones profesionales hechas en diversas instituciones de educación superior en México.

Al tratar la auditoría de sistemas computacionales, el autor incluye, de manera acertada, la evaluación del hardware, software, de la gestión informática, de la información, del diseño de sistemas, de las bases de datos, de la seguridad, de las redes de cómputo y otros conceptos o recursos especializados de los sistemas computacionales.

Cabe mencionar, en palabras del autor, que "Las principales técnicas, métodos y procedimientos de auditoría se ubican en tres grandes apartados: instrumentos de recopilación de datos, técnicas de evaluación y técnicas especiales de auditoría de sistemas computacionales".

Especial atención merece la manera en que esta obra hace énfasis en las normas ético-morales que regulan la actuación del auditor, con el propósito, como menciona el autor, de "que el lector identifique los criterios y obligaciones que debe satisfacer la actuación profesional del auditor en los campos ético, moral y profesional. El autor hace una recopilación muy profesional de las bases fundamentales de los valores, los cuales, en estos tiempos, han sido abandonados o quizás olvidados, por lo que son motivo de reflexión en este libro. El autor logra esta reflexión dentro de su amena lectura, en el capítulo correspondiente.

En combinación con las normas de comportamiento ético-morales, el autor nos menciona que hay normas de carácter social y normas de carácter profesional permanente, que son las normas mínimas de actuación que todo profesional de esta área debe observar.

Para concluir este apartado, deseo agradecer al autor por haberme dado la oportunidad de conocer en forma precisa y clara, a través de este libro, las normas, métodos, herramientas y procedimientos que deben conocer todos los profesionales que se dediquen a tan loable labor.

M. en C. Ing. Salvador Vázquez Amaya.
Presidente de la Academia de Información y Sistemas.
Universidad del Valle de México.
Campus San Rafael.

INTRODUCCIÓN

El proyecto de esta obra se realizó a lo largo de doce capítulos, en los cuales usted encontrará los fundamentos teóricos, prácticos y especializados que deben aplicarse para realizar con éxito una auditoría de sistemas computacionales. En detalle, este libro se configuró como se describe enseguida:

En el capítulo 1, *Conceptos generales*, se presentan los antecedentes, conceptos y definiciones que se agrupan en torno a la auditoría; el propósito es que usted identifique la esencia y razón de ser de esta disciplina, así como su importancia como actividad profesional en la evaluación de los sistemas computacionales.

El capítulo 2 nos muestra los elementos fundamentales para el estudio de esta disciplina; señalándose las diferentes propuestas de clasificación de la auditoría, las propuestas de estructuras de organización del área de auditoría de sistemas, así como una presentación preliminar de las áreas, actividades y elementos que se pueden auditar en los sistemas informáticos.

En el capítulo 3 encontrará un amplio y generoso tratamiento de las normas éticomorales que regulan la actuación del auditor en las empresas, en su profesión y en su conducta personal. Además, se incluye el marco conceptual de la ética y los principios axiológicos de los valores aplicables a la actividad de auditoría. El propósito es destacar la importancia que tiene la conducta del auditor ante las empresas.

Una parte sustantiva de esta obra se presenta en el capítulo 4, en donde se exponen los principios y fundamentos del control interno para su aplicación en las empresas, así como el estudio de sus conceptos, definiciones y componentes, tanto del concepto control como del control interno.

Complementando el anterior apartado, en el capítulo 5 se presenta una propuesta de estudio del control interno informático; en dicha propuesta se analiza la aplicación del control interno en los principales aspectos de la actividad de sistemas. El propósito es que usted identifique la importancia del contenido del control interno informático, con lo cual se entiende y justifica la esencia de la auditoría de los sistemas computacionales.

De igual importancia es la presentación de una metodología exclusiva para este tipo de auditoría, en donde se destaca y detalla cada uno de los pasos y componentes de la planeación, aplicación y presentación de los resultados obtenidos de una evaluación de los sistemas informáticos de las empresas. Metodología que ha sido ampliamente avalada por la práctica profesional en la evaluación de estos sistemas, la cual se analiza punto por punto en el capítulo 6, junto con los componentes y fundamentos para su uso correcto.

Así como es importante seguir la metodología propuesta para la auditoría de los sistemas computacionales, no menos trascendental es el correcto y confiable soporte documental de la evaluación practicada, razón por la cual, en el capítulo 7 se muestran los principales aspectos relacionados con la elaboración y el contenido de los llamados *papeles de trabajo*. En ese capítulo se presenta la manera de elaborar, concentrar y conservar los respaldos documentales de pruebas, evaluaciones, documentos y demás instrumentos que servirán para fundamentar las desviaciones encontradas durante la auditoría de los sistemas evaluados.

El producto final de la auditoría de sistemas computacionales es la exposición profesional de los resultados obtenidos durante la evaluación. Debido a la importancia que tiene esta función del auditor, en el capítulo 8 se puntualizan todos los aspectos que permiten elaborar, de la mejor manera, el dictamen de la auditoría de los sistemas computacionales. Para elaborar este importante documento, en este apartado encontrará un profundo análisis de los principales componentes del informe y dictamen que emite el auditor como resultado de su trabajo, en el que se señalan las características del informe, sus formas de presentación y las sugerencias para elaborarlo correctamente.

En los tres capítulos siguientes, relacionados con los procedimientos, métodos, técnicas y herramientas de aplicación exclusiva en la auditoría de sistemas computacionales, encontrará un soporte para los conocimientos en esta especialidad de sistemas.

En el capítulo 9 se presentan *los instrumentos de recopilación aplicables en la auditoría de sistemas;* se explican el diseño, la elaboración y la aplicación de herramientas como el cuestionario, la entrevista, la observación, los inventarios, el muestreo y la experimentación.

En el capítulo 10 se presentan *las técnicas de evaluación aplicables en la auditoría de sistemas computacionales.* En dicho capítulo se muestran instrumentos de evaluación como el examen, la inspección, la confirmación, la revisión documental, el acta testimonial, la matriz de evaluación y la matriz DOFA. Todos ellos instrumentos indispensables para la evaluación de los sistemas computacionales.

En el capítulo 11 se detallan *las técnicas especiales de la auditoría de sistemas computacionales.* En dicho capítulo se presentan las herramientas especializadas para evaluar los sistemas informáticos, como la guía de evaluación, la ponderación, los modelos de simulación, la lista de chequeo, la evaluación, el diagrama de círculo de evaluación, el análisis de la diagramación de sistemas, el diagrama de seguimiento de una auditoría y los programas de revisión por computadora.

En estos tres capítulos se hace un estudio profundo y detallado de los instrumentos que se presentan, con el propósito de que usted conozca los fundamentos para su diseño, instrumentación y aplicación a sus necesidades específicas de evaluación de sistemas computacionales. Con estas herramientas el auditor puede recopilar, analizar y evaluar la información sustantiva de esos sistemas, para fundamentar su informe de resultados de la auditoría practicada.

En el capítulo 12 encontrará una propuesta de los principales puntos a evaluar de los sistemas computacionales, en donde se definen, por cada tipo de auditoría propuesto, los aspectos básicos que deben auditarse. También se sugieren las herramientas, métodos y procedimientos que le serán de suma utilidad al practicar su auditoría.

Además, se presentan apéndices sobre los principales puntos a evaluar para cada uno de los tipos de auditoría propuestos a lo largo de esta obra. En dichos apéndices encontrará sugerencias sobre los aspectos que pueden serle de utilidad para realizar su auditoría de sistemas computacionales, respetando su libertad de adoptar, modificar o proponer puntos e instrumentos de evaluación que complementen los ahí señalados, a fin de adecuar los mismos a sus necesidades concretas de revisión.

Apreciable lector, el libro que ponemos a su consideración pretende exponerle los nuevos derroteros que se pueden seguir para realizar una evaluación mejor y más profesional de los sistemas computacionales en las empresas de nuestro tiempo. Aspiramos a poder mostrarle los fundamentos teóricos, prácticos y técnicos que intervienen en la práctica de esta naciente actividad profesional de auditoría de la gestión de los sistemas computacionales. La mejor recompensa para nosotros será saber que su lectura le será útil para el aprendizaje, la aplicación y el desarrollo de auditorías en el campo de la computación.

Sinceramente, el autor.

Conceptos generales

1

Estructura del capítulo:

Objetivos del capítulo

Que el lector conozca los antecedentes y conceptos fundamentales de la materia de auditoría, así como la clasificación y definiciones de los tipos de auditorías. El propósito es mostrarle los elementos que cimentan la existencia de la disciplina de auditoría en general para que entienda los aspectos básicos de la auditoría de sistemas computacionales que encontrará a lo largo de este libro. También se presenta un cuadro concentrado donde se señalan los objetivos generales de esta materia.

Introducción del capítulo

El desarrollo normal de las actividades comerciales y financieras de las empresas requiere una constante vigilancia y evaluación; asimismo, las empresas necesitan una opinión, preferiblemente independiente, que les ayude a medir la eficiencia y eficacia en el cumplimiento de sus objetivos. Por lo general, la evaluación consiste en una revisión metódica, periódica e intelectual de los registros, tareas y resultados de la empresa, con lo cual se busca medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones. *Eso es auditoría*.

Los inicios de la auditoría se remontan a la revisión y el diagnóstico que se practicaban a los registros de las operaciones contables de las empresas; después se pasó al análisis, verificación y evaluación de sus aspectos financieros; posteriormente se amplió al examen de algunos rubros de la administración, siguiendo con el análisis de aquellos aspectos que intervenían en todas sus actividades y, por último, su alcance se incrementó conforme se avanzó en la llamada revisión integral. Actualmente se ha llegado a las revisiones especializadas de algunas áreas y actividades específicas que se desempeñan en las instituciones. Entre algunas de estas últimas encontramos: auditoría de sistemas computacionales, auditoría del desarrollo de proyectos de mercadotecnia, auditoría de proyectos económicos, y en sí a muchas ramas de la actividad empresarial.

Con el propósito de dar a conocer cuál ha sido el desempeño y desarrollo de este tipo de trabajos, a continuación veremos los aspectos más destacados que intervienen en una auditoría, empezando por sus antecedentes, conceptos básicos y los diferentes tipos o métodos de auditorías, así como sus definiciones. Estos aspectos son sólo una introducción, ya que en capítulos posteriores nos enfocaremos exclusivamente a la auditoría de sistemas computacionales.

1.1 Antecedentes de la auditoría

Conforme se expandía el comercio, después de pasar por el trueque primero en pueblos, ciudades, estados y finalmente en continentes, y motivados por su constante crecimiento, tanto en volumen como en el monto de operaciones comerciales, los incipientes comerciantes tuvieron la necesidad de establecer mecanismos rudimentarios de registro que les permitieran dominar las actividades mercantiles que realizaban. Después, conforme los comerciantes crecieron y se agruparon en gremios y mercados locales, surgió la necesidad de contar con un mejor registro de sus actividades, tanto individuales como conjuntas. Posteriormente, con el crecimiento de estas agrupaciones, que se convirtieron en incipientes empresas, fue necesario establecer un mayor control para conocer de sus actividades financieras.

Gracias a ese crecimiento se inició el registro de operaciones mercantiles a través de escribas, quienes al principio asentaban dichas operaciones en forma rudimentaria; posteriormente, con el nacimiento de la partida doble y el registro de operaciones financieras, surgió la llamada teneduría de libros. Conforme esta técnica evolucionó, se llegó a impulsar la contabilidad y el registro de operaciones en libros y pólizas. En la actualidad, la contabilidad se lleva a cabo en sistemas de cómputo.

A la par que esto evolucionaba, fue necesario que alguien evaluara que estos registros y resultados fueran correctos y veraces. Entonces se requirió también de alguien que verificara la veracidad y confiabilidad de esas operaciones. En ese momento nació el acto de auditar.

Las primeras revisiones fueron rudimentarias y poco meticulosas, enfocadas exclusivamente a comprobar la veracidad y confiabilidad de los registros contables y su correcta expresión en los resultados que se entregaban; su principal objetivo consistía en saber si las transacciones eran registradas de manera correcta y si las cantidades en ellas asentadas eran exactas. Con ello se buscaba que los encargados de la administración de los negocios llevaran y reportaran con precisión sus anotaciones, para comprobar que no existieran desfalcos ni sustracciones de los bienes que se les encomendaban.

Conforme creció la actividad empresarial y los bancos tuvieron más injerencia en las empresas, a través de la custodia de sus depósitos y el otorgamiento de préstamos a las mismas, se requirió la elaboración de *estados financieros*, en los cuales las empresas anotaban los resultados obtenidos durante los ejercicios anteriores; estos estados financieros también les servían para demostrar su solvencia cuando solicitaban algún préstamo.

En sus inicios, los bancos aceptaban los resultados que emitían las empresas sin objetar sus estados financieros y sin necesidad de dictamen alguno, siempre y cuando estos resultados fueran hechos por un profesional de la contabilidad. Sin embargo, como consecuencia del propio crecimiento de las actividades empresariales, se hizo ne-

cesario que el reporte de los resultados de una empresa también fuera avalado por un profesional independiente, a quien se le encargaba que comprobara y dictaminara sobre la veracidad y confiabilidad de los resultados presentados por los financieros de la empresa. Así nació formalmente la actividad del auditor.

1.1.1 Antecedentes históricos de la auditoría

"En tiempos históricos, auditor era aquella persona a quien le leían los ingresos y gastos producidos por un establecimiento (de ahí su raíz latina del verbo **audire***,* oír, escuchar*), práctica muy utilizada por civilizaciones muy antiguas [...]"* [1]

Podemos intuir que la primera auditoría nació desde el momento en que fue necesario rendir cuentas de algún negocio y revisar que éstas fueran correctas; es evidente que dicha función fue evolucionando a la par que el crecimiento de la actividad de registros de operaciones mercantiles. Sin embargo, de acuerdo con los primeros antecedentes de auditoría, ésta nació antes que la teneduría de libros a finales del siglo XV, pero se profesionalizó con la contabilidad financiera a finales del siglo pasado.

Los primeros antecedentes formales se encuentran en 1284, al subir al trono Sancho VI "El Bravo", quien ordenó a algunos de sus hombres de confianza que controlaran el destino de los caudales públicos. Como resultado de esta medida y como producto de su reinado, se originó el tribunal de cuentas en España.[2]

Se estima que el verdadero nacimiento de la auditoría fue a finales del siglo XV, cuando nobles, ricos y familias pudientes de España, Inglaterra, Holanda, Francia y los demás países poderosos de ese entonces, recurrían a los servicios de revisores de cuentas, quienes se encargaban de revisar las cuentas manejadas por los administradores de sus bienes, y se aseguraban de que no hubiera fraudes en los reportes que se les presentaban.

El descubrimiento de América (1492) contribuyó también al crecimiento de la actividad de la auditoría, pues la Corona envió visitadores a revisar las cuentas y resultados de sus colonias; dichos visitadores supervisaban que el registro y manejo de las cuentas fueran correctos y emitían una opinión sobre la actuación de los encargados. En México, los virreyes representaban a la Corona y los visitadores venían a revisar el manejo de los tesoros, las recaudaciones, los gastos y la forma en que sus encargados gobernaban en la Nueva España. Igual ocurrió en sus otras colonias de América.

"El origen de los auditores (ESPASA-CALPE, 1988) es la Curia Romana, tiene su origen en la Edad Media [...] El auditor Papae, que en un principio daba consejos en materia de teología [...]; luego ejercía el poder civil y eclesiástico y desde 1831 se entendió en ciertos asuntos disciplinarios."[3]

Aquí se presentan otros de los antecedentes que se pueden citar: a mediados del siglo XIX, la *Ley de Empresas del Reino Unido de Inglaterra*, que impuso la obligación de ejecutar auditorías a los resultados financieros, el balance general, los registros con-

tables y las actividades financieras de las empresas públicas. Dicha costumbre, aunque no fue de carácter impositivo en Estados Unidos, también se adoptó en las empresas de ese país, y se hizo extensiva a los contadores norteamericanos, quienes tuvieron que admitir una práctica similar, principalmente por los requisitos y disposiciones emitidos por la Comisión de Valores y Bolsa, los cuales solicitaban a los auditores independientes que dictaminaran sobre los estados de resultados de las empresas que cotizaban en la Bolsa de Valores de ese entonces.

Otro posible origen lo representaron *los auditores eclesiásticos de la Rota Romana*, a través de tribunales pluripersonales, compuestos por 12 eclesiásticos: ocho italianos, dos españoles, un alemán y un francés.

También se conocieron *los auditores de la Marina y Guerra* en 1894, a quienes se les considera como los responsables del cumplimiento de las leyes y principios de esta disciplina.

A manera de concentrado de los antecedentes no contables de la auditoría, se pueden señalar los siguientes:

- *Auditores canónigos*
- *Auditores de la nunciatura*
- *Auditores de la Rota Romana*
- *Auditores de la Marina y Guerra*
- *Auditores de camareta*
- *Oidores de la colonia en la Nueva España*

Algunos antecedentes más recientes aparecen con la Revolución Industrial, a partir de la séptima década de 1800; en ese entonces, algunas empresas habían alcanzado gran auge en las actividades fabriles y mercantiles, lo cual trajo consigo un notable crecimiento en sus operaciones; obviamente, aumentó también la necesidad de registrar las operaciones contables, y con ello se hizo casi indispensable la existencia de la profesión de contador para satisfacer esa creciente necesidad. A la par creció la demanda de ejercer una mayor vigilancia del registro de operaciones financieras y la emisión de resultados financieros que realizaban esos nuevos profesionales, llegando a darse el caso de que el dictamen emitido por un contador independiente, que ejerciera la función de auditor, se consideraba totalmente confiable. Así adquirió popularidad la función de la auditoría y se destacó como una actividad preponderante en la administración de las empresas de ese entonces.

En un principio, la auditoría se consideró como una rama complementaria de la contaduría pública, y sólo se dedicaba a examinar los registros contables y la correcta presentación de los estados financieros de las empresas. Posteriormente, dicha aplicación se extendió a otros campos profesionales para ampliar su revisión; primero a los de carácter administrativo, después a los asociados a otras actividades de la empresa, luego se extendió a las ramas de ingeniería, medicina, sistemas y así sucesivamente, hasta que su práctica alcanzó a casi todas las disciplinas del quehacer humano. A pe-

sar de la amplia gama de áreas en donde se pueden aplicar auditorías, en cualquiera de ellas se tienen que considerar los mismos principios y fundamentos teóricos y prácticos que le dan vigencia a esta profesión.

Aunque la revisión de registros y cuentas se pueden considerar como el inicio de la auditoría, su reconocimiento como profesión se inició en los albores del presente siglo. No obstante, también hay evidencias de que, a mediados del siglo pasado, los británicos, españoles, estadounidenses, e incluso los mexicanos, iniciaron la actividad formal de la auditoría.

Debido a la abundancia de literatura sobre la auditoría financiera, y a la profundidad con que numerosos autores han realizado el análisis a la auditoría de los estados financieros, en este capítulo sólo nos enfocaremos en conocer los antecedentes generales de la auditoría de carácter administrativo y operacional, ya que de la conjugación de esos tipos de auditoría nacieron otros más especializados, entre ellos *la auditoría de sistemas computacionales*.

1.1.2 Antecedentes de la auditoría (siglo XX)

Para hacer las referencias a estas auditorías, vamos a tomar como válidos los antecedentes presentados en la tesis profesional de recientes titulados de la UVM,[4] quienes culminaron su carrera de *Licenciatura en Sistemas de Computación Administrativa*, producto de un profundo estudio e investigación de carácter documental, complementados con otras investigaciones; al respecto encontramos los siguientes datos, enfocados exclusivamente a los antecedentes de la auditoría de carácter administrativo y operacional, pero que pueden ser válidos como antecedentes para este libro.

En 1912, en el Instituto de Contadores Públicos de España, surge en forma colegiada la actividad del auditor, la cual tuvo una duración muy efímera.

En 1917, el Colegio de Censores de Bilbao.

En 1932, T. G. Rose, consultor inglés en el Instituto de Administración Industrial, expuso la tesis "[...] *Independientemente de la utilidad de la auditoría financiera, también es útil la auditoría administrativa*..."

En 1932, James McKinsey llega a la conclusión de que la empresa tenía que hacer periódicamente una autoauditoría, la cual consistiría en una evaluación de la empresa en todos los aspectos.

En 1936, el Colegio de Contadores Jurados de Madrid.

En 1945, el Instituto de Auditores Internos, en Estados Unidos, proporcionó los primeros escritos sobre lo que sería la auditoría de operaciones, tratando en una discusión de "expertos" lo referente al alcance de la auditoría interna de operaciones técnicas.

En 1946, el Instituto de Censores Jurados de Cuentas de España.

En 1948, Artur H. Kent, funcionario de la empresa Standard Oil of California, hizo importantes aportaciones sobre la auditoría de operaciones.

En 1950, Jackson Martindell, fundador del *American Institute of Management*, desarrolló uno de los primeros programas de auditoría administrativa, con un procedimiento de control directo y un sistema de evaluación, el cual se publicó en su libro *Apreciación de la gerencia para ejecutores e inversionistas.*

En 1955, Larke A. G. planteó la necesidad de llevar a cabo autoauditorías para las pequeñas empresas, con el fin de evaluar su forma de actuar.

En 1962, Willian P. Leornard realizó un estudio completo de la auditoría administrativa. En éste trata los métodos para iniciar, organizar, interpretar y presentar una revisión de carácter administrativo.

En 1964, Cadmus y Bradford, quienes eran trabajadores del Instituto de Auditores Internos (en N. Y.), plantean en su publicación *Operational Auditing Handbook, N.Y.*, la necesidad de una auditoría denominada auditoría operativa, en la cual se selecciona una actividad para un cuidadoso y profundo estudio, apreciación y evaluación.

En 1968, Rigg F. J., autor británico, desarrolló en su país un moderno enfoque de la auditoría administrativa, cuya aplicación se extendió a través de su obra *The Management Audit, the Internal Auditor*.

En 1968, John C. Burton, en su trabajo *The Journal of Accountancy, N. Y.,* planteó la importancia de estudiar de qué índole sería la auditoría administrativa y el grado de calificación del auditor, así como de construir un marco total para la auditoría administrativa.

En 1969, Langenderfer H. Q. y Robertson J. C. exploraron brevemente el problema de la definición y cuestión de una exposición detallada de la auditoría administrativa. Propusieron también una estructura teórica para extender la función de la auditoría a todos los ámbitos de la empresa, buscando con ello abarcar las auditorías independientes de gerencias.

En 1970, Keith D. y Bloomstrom R. exponen que las auditorías administrativas se han desarrollado a través de los años como una forma de evaluar la eficiencia y la eficacia de varios sistemas de una organización, los cuales van desde la responsabilidad administrativa hasta su preocupación social. Esta auditoría se utiliza principalmente para los propósitos de planeación, entre los cuales están los siguientes:

Investigar empresas para posibles fusiones o adquisiciones
Determinar la solidez de un proveedor principal
Averiguar los puntos débiles y fuertes de una empresa competidora para explorar mejor las ventajas competitivas de la propia empresa

En 1977, Clark C. Arb presenta una perspectiva sobre el conocimiento de la medición de la conducta social de las empresas. En sus conceptos de auditoría social

destaca la responsabilidad social, mediciones del comportamiento, auditorías sociales en decisiones administrativas y la implantación de las auditorías.

En 1980, Whitmore G. M. expone que la auditoría administrativa se utiliza para apoyar a los funcionarios públicos y gerentes de empresas privadas. Los aspectos que señala principalmente sobre el uso de esta técnica en el ámbito gubernamental, son las estrategias y los pasos necesarios para la conducción de una auditoría administrativa, haciendo énfasis en sus ventajas.

En 1983, Spencer Hayden expuso la necesidad de evaluar los procedimientos administrativos y de aplicar las correcciones necesarias para lograr una máxima eficiencia en las actividades futuras. También abundó sobre un procedimiento propio de la auditoría, el tratamiento con detalle del tema de la consultoría administrativa, y enfocó a esta auditoría dentro del camino al cambio organizacional.

En 1984, Robert J. Thierauf habló sobre la auditoría administrativa como una técnica utilizada para evaluar las áreas operacionales de una organización, enfocando su trabajo desde el punto de vista administrativo.

Podríamos seguir profundizando en los antecedentes de la auditoría en los Estados Unidos y otros países, pero no es el objetivo de este libro detallar sobre todos los antecedentes de la auditoría administrativa, ni operacional, ni integral ni de cualquier otro tipo, sino que, al presentar estos antecedentes, se busca reconocer que la auditoría de sistemas es el resultado de varias evoluciones de otros tipos de auditorías y que se apoya en ellas para su revisión, incluyendo varias de sus técnicas y metodologías de evaluación.

1.1.3 Antecedentes de la auditoría en México (siglo XX)

En México existe también una gran cantidad de información sobre la auditoría financiera, o por lo menos más que en otros tipos de auditorías. Por esta razón consideraremos únicamente los antecedentes de la auditoría operacional, administrativa e integral. Apoyados en las referencias de la tesis ya citada, a continuación se muestran, en orden cronológico, los escritores mexicanos más relevantes en este campo:[5]

En 1960, A. Mejía Fernández destacó la importancia de la auditoría en su tesis recepcional, *Auditoría de las funciones de la gerencia de las empresas,* presentada en la FCA de la UNAM en ese año.

En 1962, R. Macías Pineda presentó el trabajo recepcional, *La auditoría administrativa para el curso Teoría de la Administración*, para el Doctorado de Ciencias Administrativas de la Escuela Superior de Comercio y Administración (ESCA) del Instituto Politécnico Nacional.

En 1964, M. D'Azaola S. presentó, en la FCA de la UNAM, la tesis *La revisión del proceso administrativo*.

En 1966, J. A. Fernández Arenas propuso la realización de la auditoría administrativa, combinando los análisis de objetivos, de recursos y del proceso administrativo.

En 1969, Santillán González propuso la realización de la auditoría interna integral mediante una revisión total, tanto de los aspectos financieros como de los aspectos administrativos de las empresas.

En 1970, R. Jiménez Reyes estudió el alcance, desarrollo y planeación de la auditoría administrativa.

En 1978, el Colegio Nacional de Licenciados en Administración (CONLA) publicó, como resultado del 7º Congreso Nacional de Administración, el trabajo donde se regulan las bases de las normas, alcances del auditor y del informe de auditoría.

En 1978, S. Cervantes Abreu presentó un trabajo en ese mismo foro, en el cual analizó la dinámica de la auditoría administrativa, destacando los cuatro pasos básicos para su desarrollo: *la recolección, la verificación de datos, el estudio de las funciones, la revisión y evaluación del control interno y del informe de la auditoría*.

En 1981, V. M. Rubio y J. Hernández F. presentaron una guía práctica de auditoría administrativa, como parte de un método para el diagnóstico de la capacidad administrativa de las instituciones públicas y privadas, con el fin de determinar sus puntos vulnerables y sugerir las medidas correctivas.

Así como en el punto anterior, podemos seguir profundizando sobre los antecedentes de la auditoría administrativa, operacional y de otros tipos, pero el enfoque de este capítulo no es hablar únicamente sobre esas auditorías, sino sobre la auditoría de sistemas. Por esa razón, presentamos exclusivamente lo antes anotado.

1.1.4 Antecedentes de la auditoría de sistemas

Al igual que en los puntos anteriores, en la auditoría de sistemas computacionales también existen antecedentes en el ámbito internacional. Sin embargo, el propósito de este libro no es profundizar en los orígenes de este tipo de auditoría, debido a que sería ocioso y sin ningún beneficio práctico al carecer de evidencias comprobables sobre tales inicios. Sin embargo, para complementar este libro, citaremos a los principales autores sobre este tema en nuestro país:

En 1988, Echenique publicó su libro *Auditoría de sistemas*, en el cual establece las principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico-práctico sobre el tema.

En 1992, Lee presentó un libro en el cual enuncia los principales aspectos a evaluar en una auditoría de sistemas, mediante una especie de guía que le indica al auditor los aspectos que debe evaluar en este campo.

En 1993, Rosalva Escobedo Valenzuela presenta en la UVM una tesis de auditoría a los centros de cómputo, como apoyo a la gerencia, destacando sus aspectos más importantes.

En 1994, G. Haffes, F. Holguín y A. Galán, en su libro sobre auditoría de los estados financieros, presentan una parte relacionada con la auditoría de sistemas, que profundiza en los aspectos básicos de control de sistemas y se complementa con una serie de preguntas que permiten evaluar aspectos relacionados con este campo.

En 1995, Ma. Guadalupe Buendía Aguilar y Edith Antonieta Campos de la O. presentan un tratado de auditoría informática (apoyándose en lo señalado por el maestro Echenique), en el cual presentan metodologías y cuestionarios útiles para realizar esta especialidad.

En 1995, Yann Darrien presenta un enfoque particular sobre la auditoría de sistemas.

En 1996, Alvin A. Arens y James K. Loebbecke, en su libro *Auditoría. Un enfoque integral*, de Prentice Hall Hispanoamericana, S. A., nos presentan una parte de esta obra como Auditoría de Sistemas Complejos de PED.

En 1996, Hernández Hernández propone la auditoría en informática, en la cual da ciertos aspectos relacionados con esta disciplina.

En 1997, Francisco Ávila obtiene mención honorífica en su examen profesional, en la UVM, Campus San Rafael, con una tesis en la cual propone un caso práctico de auditoría de sistemas realizado en una empresa paraestatal.

En 1998, Yann Darrien presenta *Técnicas de auditoría*, donde hace una propuesta de diversas herramientas de esta disciplina.

En 1998, Mario G. Piattini y Emilio del Peso presentan *Auditoría informática, un enfoque práctico,* donde mencionan diversos enfoques y aplicaciones de esta disciplina.

1.2 Conceptos básicos sobre la auditoría

Como ya hemos mencionado, los campos de aplicación de la auditoría han evolucionado mucho, desde su uso en los aspectos netamente contables, hasta su uso en áreas y disciplinas de carácter especial, como la ingeniería, la medicina y los sistemas computacionales. Evidentemente, junto con ese progreso, también se ha registrado el desarrollo de las técnicas, métodos, procedimientos y herramientas de cada uno de estos tipos de auditorías, así como un enfoque cada vez más característico y especializado hacia el uso de técnicas más apegadas al área que se va a evaluar.

Debido a esos constantes cambios, a continuación citaremos el concepto más amplio de la auditoría, para de ahí analizarlo de acuerdo con lo aportado por la *Real Academia Española* y después, con esa conceptualización, trasladarlo a una propuesta de clasificación de los tipos de auditoría.

En forma general, la definición que se propone para la auditoría es la siguiente:

Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.

Como antecedentes académicos, se encontraron las siguientes expresiones:

Auditor

"Del latín. ***Auditor*****,** ***oris*** *s. m 1. Persona capacitada para realizar auditorías en empresas u otras instituciones. Pertenece a un colegio oficial [...] 3. Auditor de guerra. Funcionario miembro del cuerpo jurídico del ejército que informa en los tribunales militares sobre la interpretación o aplicación de las leyes. 4. [...] auditor de la Rota. Cada uno de los doce miembros del tribunal romano de la Rota."*[6]

"F. **Auditeur**; It. **uditore**; In., C. P. **uditor**; A.; **Zahöurer***[....] Del latín* ***uditor****; el que oye, del verbo* ***audire****. Oír. Anteriormente, oyente."*[7]

Auditoría:

"[...] Supervisión de las cuentas de una empresa, hecha por decisión de un tribunal o a instancias de particular."[8]

"[...] Revisión a la economía de una empresa [...]"[9]

"[...] Revisión de cuentas [...]"[10]

"1. Profesión de auditor. 2. Despacho o tribunal del auditor. 3. Revisión de cuentas, examen y evaluación de la situación financiera y administrativa de una institución o empresa, realizados por especialistas ajenos a la misma."[11]

"[...] Empleo, cargo de auditor. Tribunal o despacho de auditor."[12]

Audit:

"[...] Revisión o intervención de cuentas [...] Verificar o revisar la contabilidad."[13]

"Es un examen profesional y revisión de los registros, los procedimientos y las transacciones financieras de una organización hechas por especialistas [...] involucrados en la preparación de esos informes. Con base en este examen, en su informe los auditores dan una opinión independiente de la organización de su posición financiera, si los procedimientos y los controles apropiados se han seguido, y si los otros criterios han estado satisfechos en el desembolso de fondos. [...] Una revisión interna, conducida por empleados de la compañía, donde se prueba la suficiencia de los procedimientos y sistemas de contabilidad. [...] para determinar si la corporación encuentra sus responsabilidades a empleados y sociedad."[14]

"Constituye adaptación popular del verbo inglés ***to Audit****, el cual significa examinar, revisar cuentas."*[15]

1.3 Clasificación de los tipos de auditorías

Para iniciar nuestro estudio, aquí proponemos que el análisis de los conceptos anteriores se realice al amparo de la siguiente clasificación de los tipos de auditorías, con el fin de identificar los criterios, características y especificaciones de esta disciplina profesional. Posteriormente nos concentraremos exclusivamente en los conceptos y definiciones de la auditoría de sistemas computacionales.

La clasificación que se propone está integrada por el siguiente cuadro:

Auditorías por su lugar de aplicación

- Auditoría externa
- Auditoría interna

Auditorías por su área de aplicación

- Auditoría financiera
- Auditoría administrativa
- Auditoría operacional
- Auditoría integral
- Auditoría gubernamental
- Auditoría de sistemas

Auditorías especializadas en áreas específicas

- Auditoría al área médica (evaluación médico-sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoría laboral
- Auditoría de proyectos de inversión
- Auditoría a la caja chica o caja mayor (arqueos)
- Auditoría al manejo de mercancías (inventarios)
- Auditoría ambiental
- Auditoría de sistemas

Auditoría de sistemas computacionales

- Auditoría informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría alrededor de la computadora
- Auditoría de la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo

- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsourcing
- Auditoría ergonómica de sistemas computacionales

1.3.1 Clasificación de la auditoría por su lugar de origen

La primera clasificación se refiere a la forma en que se realiza este tipo de trabajos, y también a cómo se establece la relación laboral en las empresas donde se llevará a cabo la auditoría; esto nos da un origen externo si el auditor no tiene relación directa con la empresa, o un origen interno si existe alguna relación de dicho auditor con la propia empresa.

1.3.1.1 Auditoría externa

La principal característica de este tipo de auditoría es que la realizan auditores totalmente ajenos a la empresa, por lo menos en el ámbito profesional y laboral; esto permite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación de las actividades y operaciones de la empresa que audita y, por lo tanto, la emisión de resultados será absolutamente independiente. Su definición es la siguiente:

> *Es* la revisión independiente* *que realiza un profesional de la auditoría,* con total libertad de criterio y sin ninguna influencia, *con el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de sus resultados financieros. La* relación de trabajo del auditor es ajena a la institución donde se aplicará *la auditoría y esto le permite emitir un dictamen libre e independiente.*

Generalmente, estas auditorías externas son realizadas por grandes empresas y despachos independientes de auditores, los cuales, casi siempre gozan de gran popularidad y prestigio dentro del ambiente profesional. El mercado en el cual tienen mayor demanda y aplicación estas auditorías es el ámbito contable, fiscal y financiero de las instituciones, así como en aquellas actividades específicas que demandan una auditoría externa a la empresa cuando existen condiciones especiales que se pretenden evaluar.

Ventajas

Al no tener ninguna dependencia de la empresa, el trabajo de estos auditores es totalmente independiente y libre de cualquier injerencia por parte de las autoridades de la empresa auditada.

* Para el mejor entendimiento y distinción entre cada uno de los tipos de auditoría que se proponen, en cada definición se ponen en cursivas sus aspectos más sobresalientes; el propósito es que usted, amigo lector, pueda distinguir la esencia de cada descripción.

En su realización, estas auditorías pueden estar apoyadas por una mayor experiencia por parte de los auditores externos, debido a que utilizan técnicas y herramientas que ya fueron probadas en otras empresas con características similares.

Estas auditorías tienen gran aceptación en las empresas para certificar registros contables, impuestos y resultados financieros. Además, sus dictámenes pueden ser válidos para las autoridades impositivas, y con ello pueden satisfacer requisitos de carácter legal, siempre que sean realizadas por auditores de prestigio que tengan el reconocimiento público.

Desventajas

La principal desventaja es que, como el auditor conoce poco la empresa, su evaluación puede estar limitada a la información que pueda recopilar.

Dependen en absoluto de la cooperación que el auditor pueda obtener de parte de los auditados.

Su evaluación, alcances y resultados pueden ser muy limitados.

Muchas auditorías de este tipo se derivan de imposiciones fiscales y legales que pueden llegar a crear ambientes hostiles para los auditores que las realizan.

En algunos casos son sumamente costosas para la empresa, no sólo en el aspecto numerario, sino por el tiempo y trabajo adicional que representan.

1.3.1.2 Auditoría interna

En la realización de estos tipos de evaluación, el auditor que lleva a cabo la auditoría labora en la empresa donde se realiza la misma y, por lo tanto, de alguna manera está involucrado en su operación normal; debido a esto, el auditor puede tener algún tipo de dependencia con las autoridades de la institución, lo cual puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa. La definición que se sugiere es:

> *Es la revisión que realiza un profesional de la auditoría,* cuya relación de trabajo es directa y subordinada a la institución *donde se aplicará la misma, con el propósito* de evaluar en forma interna *el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros. El objetivo final* es contar con un dictamen interno *sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados y funcionarios de las áreas que se auditan.*

Ventajas

Debido a que el auditor pertenece a la empresa, casi siempre conoce integralmente sus actividades, operaciones y áreas; por lo tanto, su revisión puede ser más profunda

y con un mayor conocimiento de las actividades, funciones y problemas de la institución. Por esta razón, el contenido de su informe es mucho más valioso.

El informe que rinde el auditor, independientemente del resultado, es sólo de carácter interno y por lo tanto no sale de la empresa, ya que únicamente le sirve a las autoridades de la institución.

Esta auditoría consume sólo recursos internos, por lo tanto no representa ninguna erogación adicional para la empresa en la cual se realiza.

Es de gran utilidad para la buena marcha de la empresa, ya que permite detectar problemas y desviaciones a tiempo.

Puede llevarse un programa concreto de evaluación en apoyo a las autoridades de la empresa, lo cual ayudará a sus dirigentes en la evaluación y la toma de decisiones.

Desventajas

Su veracidad, alcance y confiabilidad pueden ser limitados, debido a que puede haber cierta injerencia por parte de las autoridades de la institución sobre la forma de evaluar y emitir el informe.

En ocasiones la opinión del auditor tal vez no sea absoluta, debido a que, al laborar en la misma empresa donde realiza la auditoría, se pueden presentar presiones, compromisos y ciertos intereses al realizar la evaluación.

Se pueden presentar vicios de trabajo del auditor con relativa frecuencia, ya sea en las formas de utilizar las técnicas y herramientas para aplicar la auditoría, como en la forma de evaluar y emitir su informe sobre la misma.

1.3.2 Clasificación de auditorías por su área de aplicación

La clasificación aquí propuesta se refiere al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditadas, ubicando a cada tipo de auditoría de acuerdo con el área de trabajo e influencia de la rama o especialidad que será evaluada.

En atención a dicho criterio, y debido a que podemos encontrar un sinnúmero de clasificaciones de estos tipos de auditorías, todas válidas, para nuestro análisis de los *conceptos generales* sólo nos concentraremos en presentar su clasificación y una breve definición de cada uno de los tipos, tomando en cuenta solamente su área de aplicación sin ir más allá, es decir, no se analizarán sus ventajas ni desventajas.

1.3.2.1 Auditoría financiera (contable)

Inicialmente llamada auditoría contable, en realidad fue el primer tipo de auditoría que existió en el ámbito comercial; en este tipo de auditoría la principal actividad del auditor consiste en revisar la correcta y oportuna aplicación de los registros contables y operaciones financieras de las empresas, con el propósito de comprobar que la emisión de los resultados financieros de un ejercicio fiscal cumpla con los principios contables que regulan las actividades del contador público y así poder emitir un dictamen sobre sus resultados financieros. La definición que analizaremos es la siguiente:

> *Es la revisión sistemática, explorativa y crítica* que realiza un profesional de la contabilidad *a los* libros y documentos contables, a los controles y registros de las operaciones financieras y a la emisión de los estados financieros *de una empresa, con el fin de evaluar y opinar sobre la razonabilidad, veracidad, confiabilidad y oportunidad* en la emisión de los resultados financieros *obtenidos durante un periodo específico o un ejercicio fiscal. El propósito final es* emitir un dictamen contable *sobre la correcta presentación de los resultados financieros a los accionistas, clientes, autoridades fiscales y terceros interesados,* en relación con las utilidades, pago de impuestos y situación financiera y económica *de la institución.*

Actualmente este tipo de auditoría se complementa con un análisis financiero de los resultados obtenidos durante dicho ejercicio, para lo cual se utilizan diversas técnicas de la ingeniería financiera y del análisis contable.

1.3.2.2 Auditoría administrativa

Después de lo anterior, el siguiente paso de la auditoría, muy importante por cierto, fue ampliar su ámbito de evaluación a las actividades administrativas de las empresas. Los auditores ya no se contentaban solamente con auditar los resultados financieros de las empresas, sino que les hacía falta completar su trabajo; por eso procedieron a evaluar el adecuado cumplimiento de las funciones, actividades y operaciones de la empresa, principalmente en el aspecto administrativo. Por esta razón se le llamó auditoría administrativa. Su definición es la siguiente:

> *Es la revisión sistemática y exhaustiva que se realiza* a la actividad administrativa *de una empresa, en cuanto a* su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades *que regulan sus operaciones.* Su propósito es evaluar tanto el desempeño administrativo de las áreas de la empresa, como la planeación y control de los procedimientos de operación, y los métodos y técnicas de trabajo *establecidos en la institución, incluyendo la observancia de las normas, políticas y reglamentos que regulan el uso de todos sus recursos.*

Inicialmente esta auditoría fue aplicada por contadores, pero debido a su propio campo de acción, así como a la importancia de esta materia, se extendió con rapidez a la profesión de licenciado en administración y carreras similares, siendo éste uno de los principales espacios de acción de estos profesionales. Entre los primeros representantes del tema se encuentran Leonard, de Estados Unidos, y Fernández Arena, de México.

1.3.2.3 Auditoría operacional

En un principio formó parte de la evaluación a las operaciones contables y administrativas de las empresas, pero su peso e importancia fueron tales que fue necesario ha-

cer auditorías a las operaciones de toda la institución, dándose así una nueva especialidad, no sólo en el campo de los administradores, sino en otras áreas especializadas como la ingeniería, relaciones laborales y otras ramas que la utilizaban para evaluar las operaciones de cualquier área de una institución.

Incluso en algunos casos fue de gran utilidad para el campo de organización, métodos y procedimientos, las actividades fabriles y en sí de la ingeniería aplicada. La definición propuesta es la siguiente:

> *Es la revisión exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de* evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que éstas sean, *tanto en el establecimiento y cumplimiento de los métodos, técnicas y procedimientos de trabajo necesarios para el desarrollo de sus operaciones, en coordinación con los recursos disponibles, como en las normas, políticas, lineamientos y capacitación que regulan el buen funcionamiento de la empresa.*

1.3.2.4 Auditoría integral

Debido al constante crecimiento de las ramas en las que se podía utilizar la auditoría, y a que cada vez existía una mayor interrelación entre todas las operaciones y actividades de una empresa, casi siempre vinculadas entre sí pero distintas con relación a su contribución a la actividad fundamental de la empresa, surgió la necesidad de avanzar en la rama de auditoría, con el fin de buscar una forma de evaluación global de todas las áreas que participan en la vida productiva de las corporaciones. Por tal razón hubo la exigencia de encontrar mecanismos especiales con los cuales se pudieran evaluar conjuntamente todas esas actividades.

Tras varias experimentaciones se logró lo anterior mediante la participación de un grupo interdisciplinario de profesionales de diversas especialidades, quienes se agruparon en torno a la disciplina de la auditoría con el fin de poder evaluar conjuntamente todas las áreas, actividades, funciones y operaciones de las instituciones. La definición de esta auditoría es la siguiente:

> *Es la revisión exhaustiva, sistemática y global que* realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, *el correcto desarrollo de las funciones* en todas sus áreas administrativas, *cualesquiera que éstas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional; dicha revisión se lleva a cabo también a las normas, políticas y lineamientos sobre el uso de todos los recursos de la empresa.*

El propósito fundamental de este nuevo tipo de auditoría tan especializado, es poder auditar de manera conjunta todas las actividades, funciones y operaciones de todas las áreas de una empresa, con la posibilidad de evaluar al total de las ramas que conforman una empresa. En esta auditoría se conjuga la participación colegiada de muchos profesionales de distintas especialidades, quienes aparentemente no tienen relación entre sí por lo diferente de sus áreas de actuación, pero que al conjuntar sus trabajos contribuyen en gran medida a elevar los alcances, la profundidad y eficacia de la evaluación de todas las áreas de una misma empresa.

1.3.2.5 Auditoría gubernamental

Esta auditoría se realiza debido a que los gobiernos federal, estatal y/o municipal son los responsables de captar los ingresos aportados por los contribuyentes, y son también los encargados de manejar los egresos de carácter público para proporcionar el bienestar de la sociedad. Se realiza también debido a lo especializado que resulta el manejo apropiado de las actividades y operaciones gubernamentales requeridas para satisfacer las necesidades de la población, y debido al cúmulo de funciones especializadas de gobierno, las cuales regulan la actuación de una entidad gubernamental a otra, aparentemente distintas entre sí.

Todo esto en conjunto hace que su evaluación sea también muy especializada y con características muy particulares, ya que existe la necesidad de una vigilancia más detallada de las funciones gubernamentales. Esta vigilancia debe ser muy estrecha en cuanto al adecuado manejo y cumplimiento de los programas, ingresos, egresos, acciones y funciones por parte de quienes tienen esta responsabilidad ante la sociedad, y además se debe vigilar que todas esas acciones gubernamentales se cumplan conforme a lo regulado en las leyes federales, estatales y/o municipales.

Debido al alto grado de especialidad que se requiere para auditar estas actividades y resultados gubernamentales, la auditoría tradicional fue incapaz de evaluar esta necesidad. Por esta razón nació la llamada auditoría gubernamental, la cual se puede definir de la siguiente manera:

> *Es la revisión exhaustiva, sistemática y concreta que* se realiza a todas las actividades y operaciones de una entidad gubernamental, *cualquiera que sea la naturaleza* de las dependencias y entidades de la Administración Pública Federal. *Esta revisión se ejecuta con el fin de evaluar el correcto desarrollo de las* funciones de todas las áreas y unidades administrativas de dichas entidades, así como los métodos y procedimientos *que regulan las actividades* necesarias para cumplir con los objetivos gubernamentales, estatales o municipales; *también se lleva a cabo en la* aplicación y cumplimiento de presupuestos públicos, programas, normas, políticas y lineamientos *que regulan la participación de los recursos de la entidad en la prestación de servicios a la sociedad.*

Esta definición nos indica claramente cómo se satisfizo la necesidad de evolucionar hacia una auditoría más especializada con la cual se pudiera evaluar la correcta aplicación de los presupuestos y gastos del gobierno, y con la que se tuviera la suficiente capacidad para dictaminar acerca del adecuado cumplimiento de las actividades que son encomendadas a las diferentes dependencias gubernamentales e instituciones paraestatales de la federación, los estados y municipios, mediante las técnicas y procedimientos de la auditoría.

1.3.2.6 Auditoría informática

Motivada por lo especializado de las actividades de cómputo, así como por el espectacular avance que han tenido estos sistemas en los últimos años, ha surgido una nueva necesidad de evaluación para los auditores, quienes requieren una especialización cada vez más profunda en sistemas *computacionales* para dedicarse a este tipo de auditorías. Por ello nació la necesidad de evaluar no sólo los sistemas, sino también la información, sus componentes y todo lo que está relacionado con dichos sistemas. La definición propuesta es la siguiente:

> *Es la revisión técnica, especializada y exhaustiva que se realiza* a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. *El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.*

Las definiciones anteriores son las más comunes y conocidas en el ambiente de la auditoría; sin embargo, existen otros tipos de auditorías más especializados, por lo que es de suma importancia conocer las definiciones de esos modelos, mismas que se presentan a continuación. Con esto se pretende establecer los diferentes criterios y áreas especializadas de evaluación que existen en esta materia para que el lector conozca dichos tipos de auditorías y pueda llegar a dominar su aplicación.

1.3.3 Definiciones de auditorías especializadas en áreas específicas

El avance de la auditoría no se detiene y requiere una mayor especialización en la evaluación de las áreas y ramas del desarrollo tecnológico de nuestros días; por esta ra-

zón, las auditorías son cada vez más singulares y tienen aplicaciones muy peculiares, las cuales están enfocadas a satisfacer las necesidades concretas de revisión y dictamen, según la especialidad de que se trate.

Es evidente que estos tipos de auditorías requieren algo más que el uso de métodos, técnicas, herramientas y procedimientos tradicionales de la auditoría, ya que deben evolucionar y adaptarse a las necesidades específicas de cada una de las áreas en donde se llevará a cabo la evaluación. Por ello cada día se tecnifican más las auditorías.

Existen muchos tipos de auditorías especializadas, pero de entre todas ellas citaremos sólo las siguientes:

- *Auditoría al área médica (evaluación médico-sanitaria)*
- *Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)*
- *Auditoría fiscal*
- *Auditoría laboral*
- *Auditoría de proyectos de inversión*
- *Auditoría a la caja chica o caja mayor (arqueos)*
- *Auditoría al manejo de mercancías (inventarios)*
- *Auditoría ambiental*

A continuación se proponen las definiciones formales para cada uno de los tipos de auditoría aquí expuestos, con el propósito de dar a conocer sus antecedentes y conceptos generales. En estas definiciones no se presenta ningún comentario adicional.

1.3.3.1 Auditoría al área médica (evaluación médico-sanitaria)

Es la evaluación sistemática, exhaustiva y especializada que se realiza a las ciencias médicas y de la salud, aplicada sólo por especialistas de disciplinas médicas o similares, *con el fin de emitir un dictamen especializado sobre el correcto* desempeño de las funciones y actividades del personal médico, paramédico, técnicos en salud y similares, *así como sobre la atención que las dependencias y el personal de esta especialidad prestan a pacientes, familiares y proveedores.*

1.3.3.2 Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)

Es la revisión técnica especializada que se realiza a la edificación de construcciones, cimientos, obra negra, acabados y servicios urbanísticos complementarios de casas, edificios, puentes, caminos, presas y cualquier otro tipo de construcción, *ya sea de tipo civil y/o arquitectónico; dicha revisión se realiza también a los planos, presupuestos, adquisiciones, cálculos y programas de obra, así como al cumplimiento y desarrollo de las mismas. Su propósito es*

emitir un dictamen especializado sobre la correcta aplicación de las técnicas, cálculos, métodos y procedimientos de la ingeniería civil y la arquitectura.

1.3.3.3 Auditoría fiscal

Es la revisión exhaustiva, pormenorizada y completa que se realiza a los registros y operaciones contables *de una empresa, así como la evaluación de la correcta elaboración de los resultados financieros de un ejercicio fiscal, con el propósito de* dictaminar sobre el correcto ejercicio financiero y la razonabilidad en la presentación de los estados de resultados y, como consecuencia de ello, comprobar el correcto pago de los impuestos y demás contribuciones tributarias, *tanto de la empresa como de sus empleados, acreedores y compradores.*

1.3.3.4 Auditoría laboral

Es la revisión y evaluación especializadas que se realizan a las actividades, funciones y operaciones relacionadas con el factor humano *de una empresa; su propósito* es dictaminar sobre el adecuado cumplimiento en la selección, capacitación y desarrollo del personal, la correcta aplicación de las prestaciones sociales y económicas, el establecimiento de las medidas de seguridad e higiene en la empresa, la elaboración de los contratos colectivos e individuales de trabajo, los reglamentos internos de trabajo, *normas de conducta y demás actividades que intervienen en la gestión de personal de una empresa.*

1.3.3.5 Auditoría de proyectos de inversión

Es la revisión y evaluación que se realizan a los planes, programas y ejecución de las inversiones de los recursos económicos de una institución pública o privada, con el propósito de dictaminar sobre el uso y control correctos de esos recursos, evaluando que su aplicación sea exclusivamente para cumplir el objetivo del proyecto. *Dicha revisión se realiza también a la ejecución y control de los presupuestos, a la adquisición y uso de recursos conforme a las normas y al cumplimiento correcto de las demás actividades especializadas del ejercicio presupuestal.*

1.3.3.6 Auditoría a la caja chica o caja mayor (arqueos)

Es la revisión periódica del manejo del efectivo que se asigna a una persona o área de una empresa, y de los comprobantes de ingresos y egresos generados por sus operaciones cotidianas; *dicha revisión se lleva a cabo con el fin de verificar el adecuado manejo, control y custodia del efectivo disponible para gastos menores, así como de evaluar el uso, custodia y manejo correctos de los*

fondos de la empresa. Por lo general, estas revisiones se realizan en forma periódica y de manera exhaustiva, dependiendo del monto asignado.

1.3.3.7 Auditoría al manejo de mercancías (inventarios)

Es la revisión física que se realiza a través del conteo (inventarios) de los bienes, productos y materias primas, intermedias o de consumo final *de una empresa, los cuales se encuentran almacenados para su consumo final o para su distribución a clientes y terceros;* su propósito es verificar que las existencias físicas concuerden con los registros contables, con los justificantes de las salidas y entradas y con las incidencias de éstas, *así como verificar el correcto manejo y control de las entradas, salidas, registros y ajustes necesarios que se hacen conforme a las características y políticas de la institución.*

1.3.3.8 Auditoría ambiental

Es la evaluación que se hace de la calidad del aire, la atmósfera, el ambiente, las aguas, ríos, lagos y océanos, así como de la conservación de la flora y la fauna silvestres, con el fin de dictaminar sobre las medidas preventivas y, en su caso, correctivas que disminuyan y eviten la contaminación *provocada por los individuos, las empresas, los automotores y las maquinarias, y así preservar la naturaleza y mejorar la calidad de vida de la sociedad.*

Es indudable que existen más definiciones y tipos de auditorías especializadas; sin embargo, no citaremos más conceptos, esto obedece a que la intención de este libro no es presentar ni hacer un tratamiento de las diferentes formas de auditar, sino presentar algunas definiciones de auditoría con el único propósito de que a usted, amigo lector, le sirvan de referencia para entender los antecedentes e importancia de la auditoría de sistemas computacionales, la cual trataremos más adelante.

1.3.4 Auditoría de sistemas computacionales (Auditoría informática)

Motivados por la importancia de continuar con la exposición de las definiciones de cada uno de los tipos de auditorías, y debido a que la esencia de este libro es enfatizar la trascendencia, utilidad y especialidad de la *auditoría de sistemas computacionales (ASC),* a continuación presentamos cada una de las definiciones de auditorías especializadas de los sistemas computacionales, las cuales se aplican para las diferentes áreas y disciplinas de este ambiente informático. Estas definiciones contendrán únicamente la exposición de los principales conceptos de esta auditoría y, si es el caso, un breve comentario, ya que en los siguientes capítulos profundizaremos en su estudio y aplicaciones.

Las definiciones propuestas para la auditoría de sistemas computacionales son las siguientes:

- Auditoría informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría en el entorno de la computadora
- Auditoría sobre la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsorcing
- Auditoría ergonómica de sistemas computacionales

A continuación, únicamente se hace la presentación de las definiciones de cada uno de los tipos de auditoría que se proponen en este estudio. Posteriormente se tratarán las aplicaciones específicas de cada clasificación.*

1.3.4.1 Auditoría informática

Esta primera definición se cita sólo de manera general, debido a que alrededor de esta conceptualización se engloban todas las demás definiciones de auditoría de sistemas, la cual se conoce también como auditoría en sistemas, auditoría en informática o con otros nombres similares. Esta auditoría se presenta en esta parte con el fin de completar las definiciones de auditoría, ya que a lo largo de este libro no se utilizará más este concepto de auditoría global, sino que se particularizará de acuerdo con cada especialidad. La definición de auditoría de sistemas es la siguiente:

> *Es la revisión técnica, especializada y exhaustiva que se realiza* a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.** *El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus*

* Aunque a primera vista pareciera que estas definiciones son repetitivas, tanto en sus conceptos, alcances y contenidos, me tomé la libertad literaria para presentar en esta parte cada una de las definiciones tal y como es, con el único propósito de que sirvan de referencia e identificación para un mejor entendimiento de cada una de las descripciones de auditoría. Espero que usted, amigo lector, me otorgue la dispensa necesaria para tolerar la aparente repetición de conceptos.

** La letra cursiva de los párrafos nos indica los aspectos más relevantes de la clasificación.

resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.

1.3.4.2 Auditoría con la computadora

En este tipo de auditoría se puede distinguir como factor fundamental que su evaluación se realiza con el apoyo de los sistemas computacionales, aunque pudiera darse el caso de que la auditoría no se refiera a la evaluación de estos sistemas, sino a cualquier otra disciplina ajena a ellos. Lo relevante es que dichos sistemas se utilizan para ayudar en tal evaluación. Su definición es la siguiente:

Es la auditoría que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas, pero sí susceptibles de ser automatizadas; *dicha auditoría se realiza también a las actividades del propio centro de sistemas y a sus componentes. La principal característica de este tipo de auditoría es que, sea en un caso o en otro, o en ambos, se aprovecha la computadora y sus programas para la evaluación de las actividades a revisar, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoría.*

1.3.4.3 Auditoría sin la computadora

En este tipo de auditoría se busca evaluar a los sistemas desde una óptica tradicional, contando con el apoyo de las técnicas y procedimientos de evaluación acostumbrados y sin el uso de los sistemas computacionales, aunque éstos sean los que se evalúen. Por lo general, esta auditoría se enfoca en los aspectos operativos, financieros, administrativos y del personal de los centros de sistemas computacionales. Su definición es la siguiente:

Es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional *del comportamiento y validez de las transacciones económicas, administrativas y operacionales* de un área de cómputo, *y en sí de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos,* pero dicha evaluación se realiza sin el uso de los sistemas computacionales. *Es también la* evaluación tanto a la estructura de organización, funciones y actividades de funcionarios y personal de un centro de cómputo, así como a los perfiles de sus puestos, *como de los reportes, informes y bitácoras de los sistemas, de la existencia y aplicación de* planes, programas y presupuestos *en dicho centro, así como del uso* y aprovechamien-

to de los recursos informáticos *para la realización de actividades, operaciones y tareas. Asimismo, es la evaluación de los* sistemas de seguridad y prevención de contingencias, de la adquisición y uso del hardware, software y personal informático, *y en sí de todo lo relacionado con el centro de cómputo, pero sin el uso directo de los sistemas computacionales.*

1.3.4.4 Auditoría a la gestión informática

Esta auditoría es, por lo general, de carácter administrativo y operacional; con su realización se busca evaluar la actividad administrativa de los centros de cómputo, con todo lo que conlleva esta gestión. La definición propuesta es la siguiente:

Es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, *tales como la* planeación, organización, dirección y control *de dicho centro. Esta auditoría se realiza también con el fin* de verificar el cumplimiento de las funciones y actividades asignadas a los funcionarios, empleados y usuarios *de las áreas de sistematización, así como para revisar y evaluar* las operaciones del sistema, el uso y protección de los sistemas de procesamiento, los programas y la información. *Se aplica también para verificar el correcto desarrollo, instalación, mantenimiento y explotación de los sistemas de cómputo, así como sus equipos e instalaciones. Todo esto se lleva a cabo con el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático.**

1.3.4.5 Auditoría al sistema de cómputo

Esta auditoría es más especializada y concreta, y está enfocada hacia la actividad y operación de sistemas computacionales, con mucho más de evaluación técnica y especializada de éstos y de todo lo relacionado con esta especialidad. Su definición es la siguiente:

Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, su hardware, software y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o ex-

* Aunque aparentemente esta definición y la siguiente son muy similares a la anterior, cada una tiene diferencias sustanciales, aunque también similitudes. La intención de presentarla así, con aparentes repeticiones, es que el lector capte la esencia de cada auditoría, la cual se utilizará de acuerdo a las necesidades concretas de evaluación, eligiendo el tipo de auditoría más adecuado a sus requerimientos de evaluación, a fin de que sea más completa y de mayor alcance.

ternas, *así como al* diseño, desarrollo y uso del *software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se encuentra el equipo de cómputo que será evaluado. Se incluye también* la operación del sistema.

1.3.4.6 Auditoría alrededor de la computadora

En este tipo de auditoría se trata de evaluar todo lo que involucra la actividad de los sistemas computacionales, procurando, de ser posible, dejar a un lado todos los aspectos especializados, técnicos y específicos de los sistemas, a fin de evaluar únicamente las actividades vinculadas que se llevan a cabo alrededor de éstos. La definición propuesta es la siguiente:

Es la revisión específica que se realiza a todo lo que está alrededor de un equipo de cómputo, como son sus sistemas, actividades y funcionamiento, *haciendo una evaluación de sus métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del propio centro de cómputo, los aspectos operacionales y financieros, la gestión administrativa de accesos al sistema, la atención a los usuarios y el desarrollo de nuevos sistemas, las comunicaciones internas y externas y, en sí, a todos aquellos aspectos que contribuyen al buen funcionamiento de un área de sistematización.*

1.3.4.7 Auditoría de la seguridad de los sistemas computacionales

Hablar de seguridad es un aspecto muy importante en los sistemas computacionales, lo cual en algunos casos puede estar relacionado con otras auditorías aquí presentadas. Sin embargo, por lo especializado y profundo del tema, es indispensable que se evalúe por separado; por esta razón se propone la siguiente definición:

Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, *así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a* salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. *Es también la revisión de los planes de contingencia y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí para todos aquellos aspectos que contribuyen a la protección y salvaguarda en el buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos.*

1.3.4.8 Auditoría a los sistemas de redes

Es reciente el crecimiento e importancia que han cobrado las redes de cómputo, razón por la cual es necesario enfocar la auditoría hacia este campo específico; no obstante, en ciertos casos, esta evaluación parecería estar contemplada en algunos tipos de auditoría aquí señalados. Su definición es la siguiente:

> *Es la revisión exhaustiva, específica y especializada que se realiza* a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración *y demás aspectos que repercuten en su* instalación, administración, funcionamiento y aprovechamiento. *Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.*

1.3.4.9 Auditoría integral a los centros de cómputo

Esta definición trata de agrupar a todos los tipos de auditoría que se analizan en estas conceptualizaciones, buscando concentrar todas las evaluaciones bajo una misma auditoría con un enfoque global del área de sistemas, según su tipo y tamaño. La definición que se propone es la siguiente:

> *Es la revisión* exhaustiva, sistemática y global que se realiza por medio de un equipo multidisciplinario de auditores, de todas las actividades y operaciones de un centro de sistematización, *a fin de evaluar,* en forma integral, *el uso adecuado de sus sistemas de cómputo, equipos periféricos y de apoyo para el procesamiento de información de la empresa, así como* de la red de servicios de una empresa *y el desarrollo correcto de las funciones de sus áreas, personal y usuarios. Es también la revisión de la administración del sistema, del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, la adquisición del hardware y software institucionales, de la adecuada integración y uso de sus recursos informáticos y de la existencia y cumplimiento de las normas, políticas, estándares y procedimientos que regulan la actuación del sistema, del personal y usuarios del centro de cómputo.* Todo esto hecho de manera global por medio de un equipo multidisciplinario de auditores.

1.3.4.10 Auditoría ISO-9000 a los sistemas computacionales

Las empresas en el mundo han adoptado la calidad ISO-9000 como parte fundamental de sus actividades. Por esta razón, los sistemas están relacionados también con es-

te tipo de auditorías de certificación de calidad, las cuales son muy especializadas y específicas en cuanto a los requerimientos establecidos en ellas. La definición propuesta es la siguiente:

> *Es la revisión exhaustiva, sistemática y especializada que realizan únicamente* los auditores especializados y certificados en las normas y procedimientos ISO-9000, *aplicando exclusivamente los lineamientos, procedimientos e instrumentos establecidos por esta asociación. El* propósito fundamental de esta revisión es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa se apegue a los requerimientos del ISO-9000.

1.3.4.11 Auditoría outsourcing

Otra de las especialidades que se ha adoptado en los sistemas computacionales, es la relacionada con la prestación de servicios de cómputo a las empresas, los cuales abarcan desde la maquilación de sus actividades computacionales, hasta la asesoría y soporte computacional a sus propios sistemas; por esta razón, se requiere de una especialización en la evaluación de estos servicios. La definición que se propone es la siguiente:

> *Es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad en* el servicio de asesoría o procesamiento externo de información *que proporciona* una empresa a otra. *Esto se lleva a cabo con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría* por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades *que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas.*

1.3.4.12 Auditoría ergonómica de sistemas computacionales

Uno de los aspectos menos analizados en el área de sistemas es la afectación que causan el mobiliario y los propios sistemas computacionales en los usuarios de computadoras; estos aspectos pueden llegar a influir en el bienestar, salud y rendimiento de los usuarios, razón por la cual se deben considerar mediante una auditoría especializada. Su definición es la siguiente:

> *Es la revisión técnica, específica y especializada que se realiza para* evaluar la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas computacionales en una empresa*. Esta revisión se realiza también con el propósito de evaluar la correcta adquisición y uso del mobi-*

liario, equipo y sistemas, a fin de proporcionar el bienestar, confort y comodidad que requieren los usuarios *de los sistemas de cómputo de la empresa, así como* evaluar la detección de los posibles problemas y sus repercusiones, y la determinación de las soluciones relacionadas con la salud física y bienestar de los usuarios de los sistemas *de la empresa.*

Las definiciones anteriores fueron presentadas de manera general, con el único propósito de identificar los tipos de auditorías de sistemas que serán tratados a lo largo de este libro. Más adelante se dará la profundidad que demanda cada una de estas auditorías.

1.4 Objetivos generales de la auditoría

A continuación, como complemento de los conceptos generales, se señalarán de manera muy general los objetivos que se pretende alcanzar con una auditoría, con la única intención de que el lector empiece a comprender las bases sobre las que descansa el desarrollo de una auditoría, cualquiera que ésta sea. Entre esos objetivos encontramos los siguientes:

- *Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.*
- *Hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa.*
- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los empleados y funcionarios de una institución, así como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.*
- *Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.*

Cabe aclarar que los objetivos antes enunciados son de carácter general; sin embargo, pueden adecuarse al tipo de auditoría que se pretenda realizar, siendo indispensable que antes de iniciar la evaluación de algún área primero se establezcan de manera precisa los objetivos que se pretende cubrir con esa auditoría, a fin de contar con su existencia, difusión y cumplimiento.

Debido a la importancia que tiene el objetivo en cada tipo de auditoría, en el siguiente capítulo se hace un enunciado específico de los principales objetivos de la propuesta de clasificación de auditoría que se mencionó en la sección 1.3 de este capítulo.

1.5 Marco esquemático de la auditoría de sistemas computacionales

Evaluación a:

- Hardware
  - Plataforma de hardware
  - Tarjeta madre
  - Procesadores
  - Dispositivos periféricos
  - Arquitectura del sistema
  - Instalaciones eléctricas, de datos y de telecomunicaciones
  - Innovaciones tecnológicas de hardware y periféricos
- Software
  - Plataforma del software
  - Sistema operativo
  - Lenguajes y programas de desarrollo
  - Programas, paqueterías de aplicación y bases de datos
  - Utilerías, bibliotecas y aplicaciones
  - Software de telecomunicación
  - Juegos y otros tipos de software
- Gestión informática
  - Actividad administrativa del área de sistemas
  - Operación del sistema de cómputo
  - Planeación y control de actividades
  - Presupuestos y gastos de los recursos informáticos
  - Gestión de la actividad informática
  - Capacitación y desarrollo del personal informático
  - Administración de estándares de operación, programación y desarrollo
- Información
  - Administración, seguridad y control de la información
  - Salvaguarda, protección y custodia de la información
  - Cumplimiento de las características de la información
- Diseño de sistemas
  - Metodologías de desarrollo de sistemas
  - Estándares de programación y desarrollo
  - Documentación de sistemas
- Bases de datos
  - Administración de bases de datos
  - Diseño de bases de datos

- Metodologías para el diseño y programación de bases de datos
- Seguridad, salvaguarda y protección de las bases de datos

Seguridad
- Seguridad del área de sistemas
- Seguridad física
- Seguridad lógica
- Seguridad de las instalaciones eléctricas, de datos y de telecomunicaciones
- Seguridad de la información, redes y bases de datos
- Administración y control de las bases de datos
- Seguridad del personal informático

Redes de cómputo
- Plataformas y configuración de las redes
- Protocolos de comunicaciones
- Sistemas operativos y software
- Administración de las redes de cómputo
- Administración de la seguridad de las redes
- Administración de las bases de datos de las redes

Especializadas
- Outsourcing
- Helpdesk
- Ergonomía en sistemas computacionales
- ISO-9000
- Internet/intranet
- Sistemas multimedia

Elementos fundamentales en el estudio de la auditoría

2

Estructura del capítulo:

Objetivos del capítulo

Mostrar los aspectos que intervienen de alguna manera en el desarrollo de una auditoría, analizando sus conceptos principales a través de un cuadro estructurado en el cual se indican los puntos básicos de esta materia. El propósito es que el lector conozca los elementos que fundamentan la existencia de la auditoría para que pueda identificarlos en los siguientes capítulos.

Introducción del capítulo

Los puntos que se tratan en este capítulo muestran, en forma general, los aspectos que se deben tomar en cuenta para entender los fundamentos de cualquier tipo de auditoría. Con esto se pretende establecer que la auditoría es una disciplina uniforme en sus cimientos, conceptos y aplicaciones, y que varía únicamente en cuanto al objetivo que se pretende alcanzar con su realización, así como en las herramientas que se utilizarán de acuerdo con la especialidad a evaluar.

2.1 Definición general de auditoría

En esta parte se presenta la propuesta de definición de auditoría, acompañada de su desglose correspondiente, con el propósito de dar un enfoque general sobre la conceptualización de esta importante disciplina de la actuación profesional.

> *Auditoría es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación.*

Del análisis de esta definición obtenemos los siguientes conceptos:

La auditoría es la revisión independiente [...]

Un requisito indispensable para llevar a cabo una auditoría, es que el auditor debe poseer una absoluta independencia mental, profesional y laboral, ya que esta soberanía de acción le permite actuar como un verdadero profesional al realizar cualquier tipo de evaluación. Es evidente que este libre albedrío le evitará tener cualquier tipo de obligación, preferencia, obediencia o algún otro compromiso con la empresa a la que audita.

Es precisamente en esta independencia donde radican la actuación profesional y la confiabilidad de un auditor.

[...] que realiza un auditor profesional [...]

La auditoría es una actividad muy especializada que puede ser ejecutada sólo por quienes están capacitados profesionalmente para ello. Sin embargo, es necesario que estos profesionales cuenten con los conocimientos, experiencia, actitudes y aptitudes necesarios para realizar este tipo de trabajo, a fin de cumplirlo tal y como lo demandan las empresas y la sociedad.

En México es requisito indispensable que el auditor especializado en la auditoría fiscal y contable cuente con el título y la cédula profesional vigentes, por lo cual debe estar avalado por colegios y asociaciones que respalden la calidad profesional que demanda esta actividad, además de poseer los conocimientos especializados que se requieren para ejercer esta función. Si alguien realiza una auditoría contable o fiscal y no cuenta con alguno de estos requisitos, no será válida la opinión o dictamen que emita.

[...] aplicando técnicas, métodos y procedimientos especializados, [...]

Cualquier profesional que tenga un título universitario puede actuar como auditor; sin embargo, si carece de los conocimientos especializados que demanda esta actividad, difícilmente podría realizarla con eficacia y eficiencia, ya que no conocería sus técnicas, métodos, procedimientos y herramientas especializadas y, en caso de conocerlas, tampoco podría utilizarlas con eficacia, aun contando con profundos conocimientos en las técnicas y herramientas especializadas de su profesión original.

[...] a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, [...]

La principal ocupación del auditor es evaluar las funciones, actividades, tareas y procedimientos que se realizan en cualquier empresa o área administrativa, con el fin de comprobar si éstas se cumplen de manera correcta. Para evaluar el grado de cumplimiento de dichas actividades, el auditor utiliza sus conocimientos, así como las herramientas especializadas en las áreas donde se aplica la auditoría.

[...] así como dictaminar sobre el resultado de dicha evaluación.

El resultado final de una auditoría es el informe de la misma, en donde el auditor, con absoluta libertad y profesionalismo, y totalmente fundamentado en la aplicación de sus técnicas, herramientas y conocimientos de auditoría, informa sobre los resultados obtenidos durante su revisión; para ello emite una opinión profesional e independiente, que plasma en un documento formal, llamado dictamen, en el cual asienta todas las desviaciones y los demás aspectos observados durante su evaluación, para que los interesados conozcan el estado que guardan las actividades y operaciones de la empresa o área auditada.

Éste es el objetivo final de la auditoría, emitir un dictamen profesional e independiente.

2.2 Objetivos particulares de cada tipo de auditoría

Aunque ya fueron señalados los objetivos generales de la auditoría, nos conviene repasarlos, ahora con la intención de compararlos con una nueva exposición de los objetivos específicos de cada uno de los tipos de auditoría que se proponen en este libro.

Concretamente, los objetivos generales de la auditoría, indicados en el punto 1.4 del capítulo anterior, son:

- *Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.*
- *Hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa.*
- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los empleados y funcionarios de una institución, así como de sus áreas y unidades administrativas.*
- *Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.*

Cabe aclarar que los objetivos que analizaremos a continuación parecerán repetitivos en algunos casos y en otros serán muy similares; sin embargo, la intención es presentarlos en cada tipo de auditoría tal y como son, aun a riesgo de parecer redundantes. El único propósito es que el lector compare los objetivos generales con los objetivos específicos de cada uno de los tipos de auditoría aquí propuestos.

2.2.1 Objetivos de la auditoría externa

La auditoría externa es aquella que se realiza con personal totalmente ajeno a la empresa auditada, con libertad absoluta de actuación y libre de cualquier injerencia por parte de la institución donde se practica; por lo tanto, sus objetivos son los siguientes:

- *Realizar una evaluación, de manera independiente, a una institución con la cual no se tengan ni empleo ni subordinación, con el fin emitir un dictamen externo sobre la razonabilidad de sus actividades, operaciones y resultados.*
- *Hacer una revisión independiente sobre el aspecto contable y las finanzas de las áreas de una empresa, emitiendo un dictamen autónomo.*
- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan las funciones de una institución, así como evaluar las actividades de sus áreas y unidades administrativas, utilizando un enfoque ajeno a la institución.*

2.2.2 Objetivos de la auditoría interna

Debido a que esta auditoría se lleva a cabo con personal que labora en la empresa y que depende estructuralmente de algún directivo de la misma, es de suma importancia que se establezcan y respeten los objetivos que se citan a continuación:

- *Realizar una evaluación independiente dentro de la institución donde se trabaja, contando con un mayor entendimiento de sus actividades y operaciones, con el fin de ayudar a evaluar la actuación de la gestión administrativa.*
- *Hacer una revisión interna del área contable, de las finanzas y del control interno de las áreas de una empresa, a fin de evaluar su funcionamiento desde un punto de vista interno.*
- *Evaluar internamente el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de cada uno de los integrantes de una institución, así como de sus áreas administrativas.*
- *Dictaminar en forma interna sobre las actividades, operaciones y funciones que se realizan en una empresa, contando con un mayor conocimiento de las actividades del personal que labora en ella, así como de sus funciones y tareas.*

2.2.3 Objetivos de la auditoría financiera

Esta auditoría está enfocada básicamente a evaluar la actuación financiera y contable de las empresas, así como sus resultados financieros. Sus objetivos son los siguientes:

- *Realizar una evaluación, de manera independiente, de las operaciones financieras de una institución, a fin de emitir un dictamen sobre la razonabilidad de sus registros, operaciones y resultados financieros.*
- *Hacer una revisión, desde un punto de vista autónomo, de las actividades financieras y de las operaciones y registros contables de las áreas de una empresa.*
- *Evaluar el cumplimiento de los planes, programas, políticas, lineamientos y normas que regulan las actividades financieras de una institución, así como de sus áreas presupuestales y unidades administrativas.*
- *Vigilar el ejercicio y cumplimiento de los planes, presupuestos y programas de inversión de una empresa, así como sus bienes e inventarios.*
- *Revisar los estados financieros que se presentan ante las autoridades fiscales y terceros, con el propósito de evaluar su correcta elaboración, los pagos de impuestos y utilidades de una empresa, así como emitir una opinión sobre el comportamiento de ésta.*

2.2.4 Objetivos de la auditoría administrativa

La finalidad de este tipo de auditoría es evaluar el comportamiento administrativo de las empresas; por tal razón, los objetivos a cumplir son los siguientes:

- *Realizar una evaluación, de manera independiente, de las actividades, operaciones, estructura organizacional y funciones de una institución, con el fin de emitir un dictamen sobre la razonabilidad de su gestión administrativa.*
- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la gestión directiva de las áreas y unidades administrativas de una institución.*
- *Evaluar la actividad administrativa de los directivos y demás empleados de una empresa, así como dictaminar sobre el cumplimiento de sus funciones y actividades.*
- *Analizar todo lo relacionado con la gestión administrativa de una empresa.*

2.2.5 Objetivos de la auditoría operativa

Esta auditoría es similar a la anterior, pero está enfocada exclusivamente a las operaciones de una empresa. Sus objetivos son los siguientes:

- *Realizar una evaluación, de manera independiente, de las actividades, operaciones, estructura organizacional y funciones de una institución, a fin de emitir un dictamen sobre la razonabilidad de sus operaciones fundamentales.*
- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la realización de las operaciones de una institución, así como evaluar sus áreas y unidades operacionales.*
- *Evaluar la actividad operativa de los directivos y demás empleados de una empresa.*
- *Evaluar los cambios y mejoras en los sistemas de operación, los métodos, procedimientos de trabajo y las técnicas específicas que regulan las operaciones y las actividades de los funcionarios y demás empleados de una empresa.*
- *Mejorar el uso de los recursos de una empresa en el desarrollo de sus operaciones y actividades*
- *Evaluar el volumen, frecuencia y periodicidad de las operaciones y actividades de las diferentes unidades administrativas de una empresa, en función de su objetivo institucional.*

2.2.6 Objetivos de la auditoría integral

La participación de grupos multidisciplinarios que serán capaces de hacer una evaluación total de todas las áreas de una empresa, con mayor profundidad y más completa, serán los aspectos fundamentales de esta auditoría, cuyos objetivos son los siguientes:

- *Realizar una evaluación global, multidisciplinaria e independiente sobre las actividades, operaciones, estructura organizacional y funciones de todas y cada una de las áreas y unidades de trabajo de una institución, con el fin de emitir un dictamen global sobre la razonabilidad de sus funciones y operaciones.*

- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan las áreas y unidades de trabajo de una empresa, así como de la correlación e integración de sus funciones y actividades.*
- *Dictaminar, en forma integral y multidisciplinaria, sobre los resultados e interrelación de las actividades de cada una de las áreas y unidades administrativas de una empresa, utilizando siempre las mismas herramientas de evaluación para hacer una valoración sistemática y emitir un dictamen veraz.*
- *Mejorar los sistemas de operación, los métodos y procedimientos de trabajo, las técnicas específicas y los controles que regulan las operaciones y actividades de todas las áreas de una institución, a través de una evaluación global y multidisciplinaria de las mismas.*
- *Aprovechar los recursos de las múltiples disciplinas de la auditoría, para hacer evaluaciones conjuntas de las operaciones y actividades de todas las unidades de trabajo de una empresa.*

2.2.7 Objetivos de la auditoría gubernamental

Esta auditoría es la responsable de evaluar las actividades gubernamentales, públicas y de gobierno, por lo tanto, sus objetivos son los siguientes:

- *Realizar una evaluación, de manera independiente, sobre las actividades, operaciones, estructura de organización y funciones de las empresas de la administración pública federal, a fin de emitir un dictamen sobre la razonabilidad de su gestión administrativa y del uso de los recursos públicos.*
- *Evaluar el adecuado cumplimiento de los planes globales de desarrollo, de los presupuestos y programas de inversión, y el uso correcto de los recursos públicos por parte de cada entidad de las administraciones públicas federal, estatal o municipal.*
- *Evaluar la actualización y correcta aplicación de las leyes, normas, políticas y procedimientos que regulan las actividades de una institución gubernamental, así como sus relaciones con otras dependencias y los ciudadanos.*
- *Dictaminar sobre los resultados de la gestión administrativa de directivos, empleados y trabajadores de cada una de las empresas y dependencias de las administraciones públicas federal, estatal y municipal, así como sobre el cumplimiento de sus actividades y funciones.*

2.2.8 Objetivos de la auditoría de sistemas

La evaluación a los sistemas computacionales, a la administración del centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

- *Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.*
- *Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.*
- *Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.*
- *Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.*
- *Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.*
- *Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora.*

La presentación de los objetivos anteriores tiene el único propósito de que el lector conozca y compare los fines básicos que se pretenden alcanzar en cada tipo propuesto de auditoría, y que los tenga presentes cuando elija los fundamentos básicos necesarios para hacer una revisión y con ello plantear los objetivos de la auditoría que requiera, buscando hacer una mejor evaluación del área que tenga que auditar.

2.3 Principales áreas, actividades y resultados que se auditan

Los siguientes puntos conforman una propuesta de las principales áreas, funciones, operaciones, resultados y actividades de una empresa o unidades administrativas que se pueden auditar; todo de acuerdo con el tipo de evaluación que se requiera. Al hacer esta propuesta se busca que el lector pueda identificar aquellas orientaciones sobresalientes que le servirán de guía para determinar las evaluaciones que deberá realizar cuando aplique una auditoría.

El interés de esta exposición es que el auditor cuente con un marco que le sirva de referencia para encauzar correctamente las formas de revisión, las técnicas, procedimientos y herramientas que puede utilizar en una evaluación, para que pueda valorar sus requerimientos a fin de emitir un dictamen confiable con los resultados de dichas revisiones.

Los puntos que a continuación se proponen se deben considerar como los puntos de partida para cualquier tipo de auditoría, mismos que se pueden ampliar de acuerdo con las necesidades específicas de la revisión que se vaya a realizar. Sin embargo, se sugiere que se tomen en cuenta los siguientes aspectos.

2.3.1 Evaluación de los estados de resultados financieros y operaciones contables

Uno de los usos tradicionales que se le ha dado a la auditoría es el de revisar el cumplimiento exacto y razonable de las normas contables que regulan todos los asuntos financieros de una empresa, así como revisar sus registros contables y el cumplimiento de sus operaciones conforme a los principios de contabilidad generalmente aceptados. Además, también se evalúa la correcta emisión de los resultados financieros alcanzados durante un periodo específico, verificando en todos los casos que todas estas actividades cumplan con las leyes, normas y regulaciones vigentes, tanto las emitidas por las autoridades correspondientes, como las de asociaciones de profesionales de este ramo, e incluso de la propia empresa en cuestión.

2.3.2 Evaluación de los objetivos, planes, programas y presupuestos

Es la auditoría que se realiza al establecimiento de los fines que se pretenden alcanzar en una empresa, a través de la elaboración y cumplimiento de sus objetivos y planes, ya sean generales, particulares, y a largo, mediano o corto plazo. En dicha evaluación se incluye la definición de las actividades, metas y eventos que se deben cumplir, así como la asignación de los recursos y tiempos programados para el desarrollo de esas actividades.

2.3.3 Evaluación de la estructura organizacional, funciones, perfil de puestos, líneas de autoridad y comunicaciones

Es la auditoría que se realiza a los aspectos organizacionales de una empresa y a sus unidades administrativas, incluyendo todo lo relacionado con la definición y cumplimiento de sus funciones, así como sus perfiles de puestos, la delimitación de sus líneas jerárquicas de autoridad y responsabilidad, sus canales formales de comunicación y todos aquellos componentes de su estructura organizacional dentro de los cuales se enmarcan todas sus actividades y tareas.

2.3.4 Evaluación de la administración de los recursos humanos de una empresa o del área auditada

Otro de los aspectos fundamentales que se debe contemplar dentro de una auditoría es todo lo relacionado con los recursos humanos de una empresa, revisión que se rea-

liza dentro de la llamada *auditoría laboral*. En esta evaluación se considera la selección, capacitación, adiestramiento y obligaciones de los patrones y trabajadores, el diseño de sus actividades, la definición de sus funciones y tareas, los contratos laborales, así como los aspectos sindicales, normas y reglamentos que regulan las relaciones laborales entre la empresa y el trabajador. Esta evaluación también se realiza a las prestaciones que reciben los trabajadores, así como a la administración de sus salarios, beneficios adicionales y todo lo relacionado con sus ingresos.

2.3.5 Evaluación de la administración de prestaciones, impuestos y obligaciones de una empresa, así como de sus funcionarios y personal en general

El objetivo principal de esta auditoría es hacer una revisión de la correcta determinación y cumplimiento de las obligaciones de una empresa, de sus funcionarios, empleados, proveedores y compradores, con el fin de verificar el cumplimiento del pago de sus impuestos y de sus obligaciones de carácter fiscal. También se verifica el cumplimiento de los otros tipos de imposiciones gubernamentales, estatales y municipales, ya sean de tipo social o relacionados con la seguridad de la comunidad.

2.3.6 Evaluación de las actividades y operaciones de una empresa, así como de sus funcionarios y personal en general

Esta auditoría está orientada a verificar el correcto desarrollo y ejecución de las operaciones, funciones y actividades de las áreas que integran una institución, así como a verificar que los funcionarios y empleados cumplan con dichas operaciones, funciones y actividades de acuerdo con las necesidades de la institución.

2.3.7 Evaluación de las normas, políticas, métodos y procedimientos de operación

Es la revisión del cumplimiento de las normas, políticas y lineamientos que regulan el desarrollo de las actividades de los funcionarios y empleados de una empresa, así como la evaluación de sus métodos de trabajo y procedimientos de operación, para determinar el buen desempeño de sus labores.

2.3.8 Evaluación de los bienes y activos de una empresa

Es la evaluación de la protección, custodia y forma de uso de los bienes muebles, inmuebles, equipos, y sistemas de las áreas de una empresa, las cuales estarán definidas por sus necesidades específicas de revisión o, en su caso, por las actividades especiales que demanda el tipo de activos a evaluar. Se incluyen las instalaciones, comunicaciones y protección de activos de la empresa.

2.3.9 Evaluación de otras áreas y actividades por auditar

Es la determinación específica y concreta de las áreas, actividades y/o eventos especiales que serán evaluados dentro de una empresa, mismos que estarán definidos por sus necesidades particulares de revisión o, en su caso, de sus operaciones que requieran ser evaluadas mediante una auditoría especial, no considerada dentro de los aspectos anteriores.

Aclaramos que las propuestas anteriores son únicamente enunciativas y su manifestación es sólo para que el lector pueda identificar los principales aspectos que debe examinar dentro de las actividades de cualquier tipo de auditoría. Insistimos, el propósito de estos puntos es que el lector pueda comprender la existencia e importancia de los aspectos ya mencionados, a fin de trasladarlos a la auditoría de sistemas computacionales, la cual trataremos en los siguientes capítulos.

Debemos señalar que los aspectos a evaluar serán establecidos de acuerdo con las necesidades concretas de la empresa y áreas en donde será ejecutada la auditoría, así como la experiencia, conocimientos y especialidad que debe tener el auditor que la realice.

2.4 Normas generales de auditoría

La profesión de auditoría se rige, al menos en el aspecto contable y financiero, por normas y criterios aceptados generalmente, los cuales son emitidos por asociaciones de profesionales quienes aportan experiencia, conocimientos y actualizaciones en esta materia, a fin de que los practicantes de esta profesión y similares conozcan estas normas y las cumplan en el desarrollo de algún tipo de auditoría, según la profesión que practiquen.

En la actualidad existen muchas asociaciones de profesionales dedicados a la contabilidad y la ingeniería financiera. Debido a esto, en casi todos los países existe alguna asociación o colegio de contadores, los cuales tienen entre sus principales funciones regular la actuación profesional de sus agremiados. Entre estas regulaciones se encuentran las normas aplicables a la auditoría financiera y contable.

A continuación citamos las normas generales de auditoría que son emitidas por asociaciones de contadores, mismas que consideran las actividades que debe cumplir el auditor. El propósito de señalar estas normas es que nos sirvan de referencia para tomar en cuenta los aspectos fundamentales del estudio de la auditoría como disciplina y deducir cómo sería su aplicación en las normas de auditoría de sistemas computacionales.

Debemos aclarar que aún no se sabe de asociaciones de auditores de sistemas, informática o disciplinas similares, mediante las cuales se regule la actuación de los auditores, y que los únicos intentos por normalizar sus acciones se dan tímidamente por las asociaciones de contadores y de licenciados en administración y ocasionalmente por asociaciones de auditores internos, por lo menos en México.

2.4.1 Normas generales de auditoría emitidas por el AICPA*

2.4.1.1 Normas generales

- *La auditoría debe ser realizada por personal que cuente con la capacitación técnica adecuada y la competencia para ejercer como auditor.*
- *El auditor debe conservar una actitud mental independiente en todos los aspectos.*
- *El auditor debe ser diligente en la presentación de los resultados de su auditoría.*

2.4.1.2 Normas para el trabajo

- *Para que una auditoría sea eficiente y eficaz, se debe planear y supervisar cabalmente.*
- *El control interno se debe entender en estructura y contenido a fin de aplicarlo en la planeación y determinación de la naturaleza, duración, extensión y profundidad de la realización de una auditoría.*
- *La evidencia que soporta el informe del auditor debe ser suficiente, competente y oportuna, esto se logra mediante las técnicas, métodos y procedimientos de auditoría.*

2.4.1.3 Normas de la información

- *El informe de la auditoría debe presentarse en estricto apego a las normas de auditoría y contabilidad generalmente aceptadas.*
- *En el informe de la auditoría se deben señalar las observaciones que se hayan detectado durante el periodo de evaluación, destacando aquellas desviaciones de los procedimientos normales de la operación de la empresa y de los principios generalmente aceptados.*
- *Los informes de auditorías financieras deberán contener la opinión razonada del auditor.*

2.4.2 Normas generales de auditoría emitidas por el IMCPAC**

Este instituto es el que agrupa a los contadores públicos de México y, como asociación de profesionales en esta materia, es el que ha emitido una serie de normas, principios y criterios relacionados con la auditoría, principalmente de carácter contable y financiera, con el propósito de homogeneizar la actuación de estos profesionales al realizar sus auditorías. Dichas normas se presentan a continuación.

Normas de auditoría

- *Normas personales*

* AICPA (American Institute Certified Public Accounting; Instituto Estadounidense de Contadores Públicos Certificados).
** IMCPAC (Instituto Mexicano de Contadores Públicos Asociación Civil).

- *Normas de ejecución del trabajo*
- *Normas de información*

Normas personales

- *Entrenamiento técnico y capacidad profesional*
- *Cuidado y diligencia profesional*
- *Independencia*

Normas de ejecución del trabajo

- *Planeación y supervisión*
- *Estudio y evaluación del control interno*
- *Obtención de evidencia suficiente y competente*

Normas de información

- *Declaración de la relación de estados o información financiera y expresión de opinión*
- Bases de opinión sobre estados financieros
- Vigencia

2.4.3 Normas para todos los auditores[1]

En la enciclopedia de la auditoría, William F. Messier propone que todos los auditores deben seguir las siguientes normas, mismas que presentamos sin hacer ningún comentario al respecto:

Independencia
Integridad profesional
Fiabilidad de los estados y registros
Mantenimiento del control interno
Obtención y evaluación de evidencia
Rango de conocimiento

- *Conocimiento completo*
- *Buen conocimiento*
- *Conocimiento adecuado*

Podríamos seguir citando más normas de auditoría emitidas por asociaciones, colegios o autores en la materia; sin embargo, para el propósito que se busca en este capítulo, sería inadecuado continuar con estas exposiciones a riesgo de parecer desactualizados en las citas de dichas normas. Por esta razón, hasta aquí dejamos los comentarios al respecto; sin embargo, a continuación proponemos normas generales de auditoría y sugerimos profundizar en su contenido, ya que así podremos analizar

los principales aspectos a utilizar en la emisión de las normas de auditoría, cualesquiera que sean las áreas donde se apliquen.

2.4.4 Normas generales

Las normas que se presentan a continuación pueden considerarse como las regulaciones formales que, como mínimo, debe considerar el auditor para desarrollar esta actividad profesional, cualquiera que sea su especialidad. Debido a la importancia de estas normas, se da una explicación breve y general de su aplicación.

2.4.4.1 Normas para la capacitación del auditor

Éstas son las normas relacionadas con la capacitación, adiestramiento y profesionalización de quienes trabajan en la auditoría de sistemas computacionales, debido a que con su adopción se pretende regular los conocimientos, habilidades y requerimientos técnicos de los profesionales que actúan en esta disciplina especializada. Dichas normas se agrupan en dos grandes aspectos:

- *Capacitación adecuada a las necesidades de auditoría*
- *Capacitación permanente del profesional dedicado a esta actividad*

2.4.4.2 Normas para la conducta observable del auditor

Debido a que la auditoría es una ocupación profesional que tiene un gran reconocimiento entre las empresas, trabajadores e incluso autoridades, su realización reclama una considerable responsabilidad, mucho prestigio y una gran capacidad laboral y moral por parte del auditor. Para que esto sea así, es necesario que se regule la intervención del auditor en este campo profesional, mediante una serie de normas que determinarán su actuación. Estas normas se pueden agrupar como sigue:

- *Para la independencia y actitud mental del auditor*
- *Para la actuación profesional del auditor*
- *Para la actividad de auditoría*

2.4.4.3 Normas para el desarrollo del trabajo del auditor

Para que la actuación profesional del auditor se realice de la mejor manera y con la eficacia que requieren las empresas y áreas de sistemas, es necesario que esta actividad sea regulada por una serie de normas, criterios y lineamientos que ayuden a uniformar estos trabajos. Para establecer, difundir y aplicar dichas normas, primero deben ser reguladas por algún organismo especializado, el cual previamente las estudia, explica y, ya debidamente comprobadas, las difunde y establece. Estas normas se pueden aplicar en los siguientes rubros:

- *En la planeación de las actividades de auditoría*
- *En la supervisión de las actividades del auditor*
- *En la aplicación del control interno*
- *En la aplicación de las herramientas, técnicas y procedimientos de auditoría*
- *En la obtención de las evidencias de la auditoría*

2.4.4.4 Normas para la emisión del informe de la auditoría

El producto final de una auditoría es la emisión de un informe, en el cual se reportan las incidencias encontradas durante la revisión, así como la opinión del auditor respecto a lo que evaluó; sin embargo, dicho informe debe ser regulado por algunos lineamientos, a fin de que su elaboración sea acorde con los aspectos profesionales que requiere esta disciplina. Estos lineamientos se aplican para los siguientes aspectos:

- *Para la presentación del informe de auditoría*
- *Para el dictamen y opinión del auditor*
- *Para la aplicación de las normas y principios de auditoría*

2.5 Métodos, técnicas, herramientas y procedimientos de auditoría

En esta parte de nuestro estudio sólo haremos mención de las principales herramientas que utiliza el auditor para llevar a cabo su trabajo, aclarando que en los capítulos 9, 10 y 11 de este libro analizaremos cada una de estas herramientas, enfocándolas concretamente hacia la auditoría de sistemas computacionales.

Estas técnicas, métodos y procedimientos de auditoría se ubicaran en tres grandes grupos, considerando a las herramientas tradicionales y otras herramientas específicas aplicables a los sistemas computacionales. En el siguiente cuadro se presentan esos tres grupos:

Instrumentos de recopilación de datos aplicables en la auditoría de sistemas

- *Entrevistas*
- *Cuestionario*
- *Encuestas*
- *Observación*
- *Inventarios*
- *Muestreo*
- *Experimentación*

Técnicas de evaluación aplicables en la auditoría de sistemas

- *Examen*
- *Inspección*

- *Confirmación*
- *Comparación*
- *Revisión documental*

Técnicas especiales para la auditoría de sistemas computacionales

- *Guías de evaluación*
- *Ponderación*
- *Simulación*
- *Evaluación*
- *Diagrama del círculo de sistemas*
- *Diagramas de sistemas*
- *Matriz de evaluación*
- *Programas de verificación*
- *Seguimiento de programación*

2.6 Estructuras de organización de las empresas y áreas dedicadas a la auditoría

Tomando en cuenta que en México existen muchas empresas y profesionales que se dedican a la auditoría, y debido a las propias características de esas empresas y/o áreas de auditores, a continuación se presenta una serie de propuestas de organización, bajo las cuales se puede clasificar la estructura de organización de las empresas y áreas de auditoría. Dichas propuestas se dividen en dos grupos.

El primero está determinado por las estructuras de aquellas empresas que se dedican a la *auditoría externa.* Estas estructuras se agrupan en tres grandes clasificaciones, según el tamaño de la empresa; claro está, todo será considerado de acuerdo con el número de sus ocupantes y actividades que deban realizar.

Para el segundo caso, la estructura de organización está considerada para aquellas empresas que cuentan con áreas de *auditoría interna*; en esta estructuración también se ubican tres tipos de áreas de auditoría interna dentro de las empresas, tomando en cuenta el tamaño de la institución y el número de empleados que haya en el área de auditoría interna.

2.6.1 Estructuras de organización de las empresas dedicadas a la auditoría externa

Para la presentación de esta clasificación de niveles ideales de estructuras de las empresas dedicadas a la auditoría externa, tomaremos el siguiente criterio de agrupación: *grandes empresas dedicadas a la auditoría, despachos o empresas medianas dedicadas a la auditoría y pequeños despachos o auditores independientes*. Sobre esta base se proponen estos niveles de puestos para adecuarse a las necesidades de la empresa auditora:

Grandes empresas dedicadas a la auditoría

- *Director o gerente general (al nivel de mando superior)*
- *Funcionarios de cuenta (por empresa o por área de atención)*
- *Gerentes o jefes de departamento o de área de atención*
- *Supervisores de auditoría*
- *Jefes de grupo o responsables de auditoría (Auditores Senior)*
- *Auditores asignados (Auditores Junior)*
- *Apoyo administrativo y secretarial*

Despachos o empresas medianas dedicadas a la auditoría

- *Gerente de auditoría*
- *Encargado de auditoría (Auditor Senior)*
- *Auditores Junior*
- *Apoyo secretarial*

Pequeños despachos o auditores independientes

- *Auditor Senior*
- *Auditor Junior*
- *Apoyo secretarial*

Es necesario volver a destacar que los niveles de estructura aquí propuestos son indicativos para la organización de cualquier empresa dedicada a la auditoría externa, en la condición de que esta estructuración puede adecuarse a las necesidades concretas de la propia institución, atendiendo los requerimientos de sus áreas, la especialidad de su personal, las necesidades de sus clientes o de cualquier otro tipo de criterio que le ayude a bien evaluar sus funciones, actividades u operaciones, según sus características y necesidades.

2.6.2. Estructuras de organización de las áreas de auditoría interna

De acuerdo con la estructura de organización, el tamaño de la empresa, las políticas y estilos de dirección de cada institución, la ubicación ideal de las áreas de auditoría interna tiene que ser a nivel de *staff* o asesoría, dependiendo y reportando directamente a los niveles de mayor jerarquía en la empresa, con subordinación de la dirección general o de una sola de las áreas de alta dirección. Es recomendable, de acuerdo con la estructura de organización de cada empresa, que el área de supeditación sea la administrativa, de contraloría o alguna similar en sus funciones. Sin embargo, nada impide que se pueda depender de cualquier otra área, siempre que sea del ámbito de alta dirección.

Tomando como criterio fundamental la clasificación dictaminada por Nacional Financiera sobre el tamaño de las empresas en México, encontramos que éstas se ubican en los siguientes cinco grupos, de acuerdo con su tamaño: *macroempresas, empresas*

grandes, empresas medianas, empresas pequeñas y microempresas. En apego a dicha clasificación, ubicaremos los niveles de puestos de la estructura de la auditoría interna como sigue:

Para auditorías internas de macroempresas y empresas grandes

- *Director o gerente al nivel de área funcional*
- *Gerentes o jefes de departamento, de área o de función a auditar*
- *Jefes de grupo o encargados (Auditores Senior)*
- *Auditores internos (Auditores Junior)*
- *Apoyo administrativo y secretarial*

Para auditorías internas de empresas medianas

- *Gerente de auditoría*
- *Auditor Senior*
- *Auditores Junior*
- *Apoyo secretarial*

Para auditorías internas de empresas pequeñas y microempresas

- *Auditor Senior*
- *Auditor Junior*
- *Apoyo secretarial*

También conviene aclarar que la propuesta de niveles de organización de auditoría interna puede ser modificada de acuerdo con las necesidades y características de la institución, a los requerimientos de atención de sus áreas, a su tamaño, giro y actividades, o por cualquier otro tipo de criterio que le permita hacer una evaluación adecuadamente.

3

Normas ético-morales que regulan la actuación del auditor

Estructura del capítulo:

Objetivos del capítulo

Presentar los conceptos fundamentales de conducta que ayudan a identificar la correcta actuación profesional, laboral, social y personal de un auditor, tomando en cuenta las principales directrices ético-morales, profesionales, sociales y personales que regulan su accionar ante las empresas, sus colegas de profesión y ante él mismo como especialista en la materia. El propósito es que el lector identifique los criterios y obligaciones fundamentales que debe cumplir el auditor en el campo ético, moral y profesional.

Introducción del capítulo

Es muy grande la responsabilidad que tiene el auditor ante la sociedad, sus colegas de profesión y las empresas, ya que el hecho de permitirle que revise profesionalmente los documentos, información, activos y operaciones de la empresa, representa la confianza que se le otorga como profesional especializado en la materia; más aún, cuando se acepta su opinión en el dictamen que emite, se da por sentada su calidad moral, profesional y ética. Por eso la sociedad, los funcionarios y empleados de las empresas casi siempre están convencidos de que la actuación de un auditor siempre está respaldada por una gran experiencia, sólidos conocimientos en auditoría y en la utilización de las herramientas de evaluación que corresponden a su área de revisión.

Dicha confianza no sólo se deriva de la experiencia, los conocimientos o la aplicación de técnicas, procedimientos y herramientas de evaluación del auditor, sino que se tiene la certidumbre de que actúa como un verdadero perito en su materia y de que está investido de una excelente ética profesional, laboral, jurídica, moral y personal que le hace confiable en la evaluación y los resultados que emite.

Dicha creencia siempre está respaldada porque un auditor cumple, o por lo menos se supone que debe cumplir, con una serie de preceptos, normas y obligaciones, tanto en los ámbitos ético y moral como en el social, jurídico, laboral y profesional que le obligan a sujetarse a las normas establecidas por la sociedad. Dichas normas le obligan a actuar como verdadero profesional de la auditoría. En ello estriba la confianza que se le tiene como auditor.

3.1 Marco conceptual de la ética

Para entender lo importante que es el estudio de esta materia, comenzaremos por identificar las definiciones y conceptos básicos que se han vertido alrededor de la ética, para después analizar las principales corrientes y autores del pensamiento filosófi-

co sobre esta parte esencial del comportamiento humano. Contando con este breve esbozo, ya estaremos en condiciones de identificar los principales valores y deberes éticos, criterios y responsabilidades, normas y obligaciones que el profesional de auditoría deberá respetar al ejercer su profesión.

3.1.1 Conceptos básicos relacionados con la ética

Como parte de este inciso vamos a señalar las principales definiciones de algunos temas relacionados con la ética, con el mero propósito de dar las bases conceptuales de esta materia.

Ético

"Del griego **eethikos** *de* éethos: *costumbre, carácter. Relativo a la moral."*[1]

Ética

"Relativo a la ética o moral, o que está de acuerdo con sus principios o su exigencia. Parte de la filosofía que estudia los fundamentos y las normas de la conducta humana. Dos son las corrientes principales: la que relaciona la ética con la naturaleza misma del hombre [...] la que no ve en las normas de conducta sociales más que unos convenios sociales reguladores de lo que considera bueno o malo, conveniente o nocivo."[2]

"Del griego **éthicos**: *Parte de la filosofía que trata de la moral y obligaciones de los hombres."*[3]

Moral

"Del latín **moralis** [...] *Ciencia que enseña las reglas que deben seguirse para hacer el bien y evitar el mal... Conjunto de facultades del espíritu [...]."*[4]

"Conjunto de principios y reglas que recomiendan lo bueno y rechazan lo malo [...] Grupo de facultades intelectuales que valora las acciones humanas [...] Juicio moral que no tiene que ver con lo jurídico [...] Que es decente, decoroso, honesto [...]."[5]

Social

"Que pertenece a, o se relaciona con las sociedades humanas [...] Sistema de organización social, política y económica que busca los beneficios de la colectividad y no los de los intereses individuales [...] Que pertenece a, o se relaciona con agrupaciones mercantiles o financieras [...] Que pertenece a, o se relaciona con las actividades que la gente organiza para convivir [...]."[6]

Con el análisis de los anteriores conceptos, vemos que la moral está relacionada con las normas de conducta de carácter social, jurídico, profesional y religioso que regulan la actuación del hombre en la sociedad, de acuerdo con los preceptos que se establecen conjuntamente para servir de guías en el accionar del hombre dentro de la misma sociedad.

Lo mismo ocurre con la actuación del profesional dedicado a la auditoría, ya que éste debe conducirse de acuerdo con las normas de conducta social, moral, religiosa, jurídica y profesional, las cuales regularán su actuación como profesional de la auditoría ante la sociedad, autoridades, empresas y empleados de estas últimas.

Sin embargo, la conceptualización de ética va más allá de estos conceptos, como lo señala Nicola Abbagnano en su diccionario de filosofía que dice:

"La ética es en general la ciencia de la conducta [...] y existen dos concepciones fundamentales de esta ciencia, a saber: 1. La que considera como ciencia del fin, al que debe dirigirse la conducta del hombre y de los medios para lograr tal fin y derivar tanto el fin como los medios de la naturaleza del hombre. 2. La que la considera como la ciencia del impulso de la conducta humana, e intenta determinarlo con vistas a dirigir o disciplinar la conducta misma."

"Estas dos concepciones se han entrelazado en formas diferentes, tanto en la antigüedad como en el mundo moderno[...] la primera, en efecto, habla el lenguaje ideal con el que el hombre se dirige por naturaleza [...] la segunda, en cambio, habla de los motivos y de las causas de la conducta humana, o también de las fuerzas que la determinan y pretenden atenerse al reconocimiento de los hechos."[7]

"[...]Gutiérrez Sáenz dice que 'la Ética estudia reflexivamente el fundamento de la conducta moral'. Esto quiere decir que el hombre desde el principio de su vida social (socialización) está sujeto todo el tiempo a seguir una serie de reglas, normas o leyes. Se crea entonces en el individuo una conciencia normativa que le indica cuáles son los caminos adecuados que lo conducirán ordenadamente y con la aceptación de sus congéneres a convivir y obtener los logros que se proponga, como son: la felicidad, la perpetuación, la autorrealización y otros más. Además, como señala Larroyo todas las normas se crean en contacto con los otros seres humanos, por lo que esa conciencia normativa es, en rigor, una conciencia social normativa."[8]

Atendiendo a lo anterior, la definición propuesta de ética profesional del auditor es la siguiente:

> *Es el conjunto de valores y principios éticos, morales y profesionales que permiten regular la actividad del profesional dedicado a la auditoría, con el fin de mejorar su actuación en las empresas que audita, así como establecer la responsabilidad que éste adquiere con el desarrollo de esta profesión.*

Sin embargo, la acepción de ética es mucho más amplia, según el autor y la corriente que se tomen en cuenta para su análisis y aplicación. Esta materia pretende regular el comportamiento y los deberes éticos y profesionales del auditor; de esta manera, encontramos que este campo de estudio es demasiado amplio y tiene muchas corrientes de pensamiento y autores, opuestos entre sí, y diversas formas de utilización. Debido a ello, a continuación le presentaremos las principales corrientes del pensamiento ético, sin profundizar en su análisis, ya que sólo queremos presentarle un

breve esbozo del tema, dejándole en absoluta libertad de profundizar sobre este apasionante e importante tema de carácter filosófico.

3.1.2 Principales corrientes éticas

Debido a que existen muchas corrientes de pensamiento respecto a las doctrinas ético-filosóficas, vamos a seguir las corrientes más características de esta materia, asumiendo de antemano que en este breve análisis podemos dejar sin mencionar otras corrientes muy importantes para algunos lectores; sin embargo, las que aquí se mencionan sólo serán a nivel de identificación, a fin de captar la esencia e importancia del estudio de la ética en la actuación profesional del auditor.

Las corrientes éticas que estudiaremos son las siguientes:

Doctrina ética griega
Doctrina ética aristotélica
Doctrina ética cristiana
Doctrina ética kantiana
Doctrina ética marxista
Doctrina ética existencialista
Doctrina ética pragmática

A continuación se hace un breve planteamiento del pensamiento filosófico de estas doctrinas, incluyendo las corrientes de cada una de ellas.

3.1.2.1 Doctrina ética griega

Esta doctrina se fundamenta en que pretende alcanzar el bien supremo como el objetivo fundamental del hombre, a través de una conducta virtuosa y moral. Dentro de esta doctrina encontramos las siguientes corrientes.

Sofismo

Derivado de **sofisma,** *"del griego* ***sóphisma****; habilidad, sabiduría",*[9] es la corriente filosófica que considera a la sabiduría y a la cultura como lo más importante en la vida. Desde el siglo V a.C., esta corriente estaba orientada a la permanente búsqueda de la verdad a través de la enseñanza, a fin de que el hombre pudiera encontrar la verdad y alcanzar la virtud a través de la sabiduría. También se identifica a los sofistas como los primeros educadores de la humanidad, en el sentido estricto de la educación, ya que enseñaban a los jóvenes por el puro hecho de enseñar, cobrando altos honorarios por ello. Entre sus principales representantes tenemos a.

Protágoras de Abdera (¿485-410 a.C?) Este autor consideraba que el hombre constituía el centro del universo "*el hombre es la medida de todas las cosas, de las que son en cuanto son y de las que no son en cuanto han dejado de ser*" (Estrada Parra, 1992; 122).

Calicles. La mayoría de los conocimientos de los griegos se basaba en la observación de los fenómenos naturales, siendo Calicles uno de los representantes de ese conocimiento al afirmar "*El pez grande devora al pequeño y el león hace trizas al ciervo y después se lo come; así el fuerte debe dominar al débil*", lo cual aplicaba a la sociedad de ese entonces, exponiendo leyes que desataban a quienes detentaban el poder para someter a los que carecían de él.

La influencia de ambos autores fue muy importante en esa época, ya que pretendían justificar el comportamiento de los poderosos a través del dominio de una clase pudiente sobre los demás, buscando a través de una moral empírica, basada en experiencias, la legalización de leyes para que se aceptaran y justificaran las acciones de los poderosos. Cabe agregar que al avanzar la sociedad, contrariamente a esa corriente, las leyes buscaron la protección del individuo, del débil o de los menos capaces, con lo cual, el rechazo de esta filosofía fue casi universal.

Eudemonismo

También formaba parte de la ética griega, el ***eudemonismo*** se deriva *de* ***ed,*** *bueno y* ***daimon****, demonio o espiritualidad. Doctrina moral que identifica la virtud con la alegría de hacer el bien*. Esta doctrina se refiere a los conceptos del bien y del mal, el concepto de virtud y la relación entre ésta y la felicidad. Sus principales representantes son Sócrates, Platón y Aristóteles.

Filosofía de Sócrates. En su filosofía jerarquiza los bienes, de los cuales el mayor anhelo o el fin supremo del hombre es la felicidad (Estrada Parra, 1992; 123). Por esta razón, ***eudemonía*** equivale, en griego, a felicidad. Sócrates, como filósofo, fue el promotor de esta corriente, la cual difundió a través del debate, de la ironía y la interrogación a sus interlocutores, a quienes conducía al conocimiento de sí mismos y de las ideas del bien y del mal, de la bondad y la virtud del alma, induciéndolos así a los temas relacionados con la felicidad, la sabiduría, el bien y los demás preceptos éticos que promulgaba.

El concepto del bien y del mal, esencia del pensamiento socrático, debería conducir al hombre a los principios morales y practicándolos llegaría a la felicidad*. El sabio es bueno, en cuanto a las intenciones que lo encauzan al saber*. Incluso uno de sus máximos fundamentos fue: *no hay hombres malos sino ignorantes*. Esto está muy relacionando con la bondad, la sabiduría, la virtud y la felicidad; así, quien maneja la bondad y la sabiduría puede llegar a ser virtuoso.

Otro de los conceptos importantes de su filosofía se refiere a la **virtud**; *"del latín* ***virtus****; Disposición constante del alma que nos inclina a obrar bien y evitar el mal."*[10] Para Sócrates, la sentencia *los hombres no son malos sino ignorantes*, indicaba que la maldad era la falta de conocimiento, pero del conocimiento del bien; por lo tanto, al poseer el bien, el hombre empezaba a ser virtuoso. La virtud proviene del saber; cuando se conoce la virtud se actúa conforme a ella y ya no es posible actuar al contrario. También consideraba que el bien supremo del hombre era la felicidad, pero para lo-

grarla debería practicar permanentemente la virtud, la cual sólo se alcanzaba por medio del saber.

Filosofía de Platón. Discípulo de Sócrates, Platón tomó al ser humano como la base fundamental de su filosofía, adoptando la idea del bien supremo como el fin último del hombre, complementada con el estudio de la sociedad como un enorme organismo, donde cada órgano (individuo) tiene suma importancia, de acuerdo con las clases sociales de esos individuos. Así, afirma que el cerebro debe estar representado por los filósofos, únicos capacitados para discernir sobre la justicia; por lo tanto, ellos deben gobernar. Los guerreros equivalen al corazón, órgano fundamental para la circulación de la sangre y portador de los sentimientos de la sociedad. Al pueblo se le concibe como las vísceras; sin las cuales no puede sobrevivir el organismo, pero no tiene la importancia del cerebro y el corazón.

Otra de las teorías de Platón es que lograr la felicidad es realizar el bien dentro de un mundo burdo, réplica de un mundo perfecto de ideas. En este último, los objetos son inmutables e incorruptibles y las ideas representan la perfección. Entre esas ideas inmutables está el bien supremo como la aspiración máxima del individuo, la cual sólo se alcanza a través de la sabiduría y la posibilidad de aspirar a la perfección, complementada con el dominio y organización de las pasiones y la necesidad de participar en el bien supremo. Alcanzar la felicidad es realizar en la vida las virtudes que acerquen más al individuo a los objetivos ideales; cuanto más se acerque la conducta a estos arquetipos, mayor será la felicidad.

Hedonismo

Del griego ***edos***; placer. *"Doctrina que persigue el placer como objetivo de vida. Identifica el bien con el placer y desea evitar el dolor."*[11] Es la doctrina que pretende alcanzar la felicidad a través del placer. Sus principales representantes son: **Epicuro** *y la doctrina moral de los estoicos*, **Zenón de Citium, Panacio de Rodas, Posidonio de Apamea, Epicteto, Séneca y Marco Aurelio.**

Epicuro (341-270 a.C.) Basaba la filosofía de su doctrina en la ruptura de los prejuicios que impiden alcanzar la felicidad mediante el disfrute legítimo del placer, pero no de carácter sexual o de cualquier otro carácter corporal, sino de elevación del espíritu. Por lo tanto, el objetivo fundamental del individuo es entender la elección de los valores y las condiciones para lograr placeres legítimos.

Estoicos. La esencia de esta filosofía moral es el *eclecticismo, "del griego* ***eklegein****, escoger. Método que consiste en reunir lo mejor de la doctrina de varios sistemas"*[12] el cual toma lo esencial de las demás corrientes filosóficas de los griegos y los romanos para adaptarlo a su propia corriente. Fundada en su primera época por ***Zenón de Citium***, esta filosofía se considera como una síntesis de las corrientes éticas grecolatinas, adoptando a la concepción de la naturaleza como su fundamento. En ésta hay una mayor preocupación por los problemas humanos y la moral establecida es producto de un convencionalismo humano, que repele la mera satisfacción del placer que excede a las normas jurídicas establecidas.

Similares conceptos aporta el pensamiento de ***Séneca***, quien recomendaba la práctica de la virtud para salvaguardar la vida humana; afirmaba que los mayores infortunios pueden resistirse si detrás de la conducta del hombre brilla la estrella de la virtud. ***Marco Aurelio***, en sus *soliloquios*, pretendió legar una serie de máximas para que el hombre pudiera realizar el bien, a pesar de los vicios, los males y las aflicciones.

3.1.2.2 Doctrina ética aristotélica

Esta doctrina moral ha tenido una notable influencia en el pensamiento moderno sobre la ética y la moral; su máximo representante es ***Aristóteles*** (384-322 a.C.), fundador de la doctrina peripatética y fundador del Liceo. Aristóteles fue discípulo de Platón y seguidor del pensamiento socrático, pero hay ciertas diferencias en sus corrientes filosóficas: *"Soy amigo de Platón pero soy más amigo de la verdad."*

En su obra *Aristóteles: Ética a Nicómaco*. Editorial Gredos, Madrid, afirmó que el fin último del hombre es la felicidad, aunque los fines del hombre son innumerables y de diversas categorías; así, cualquier actividad humana pretende alcanzar una meta. Por ejemplo, en la belleza de la construcción está el fin de la arquitectura; en la salud está el fin de la medicina, pero ante todo está la búsqueda de la felicidad.

Para Aristóteles, la felicidad es una meta tras la cual el hombre goza la totalidad del conocimiento propio, pero existen considerables contradicciones; por lo tanto, la felicidad es la lucha permanente por alcanzar los fines superiores. También afirmaba que el hombre busca como último fin su propio bien, su felicidad o su propia perfección, la cual sólo puede alcanzar a través de sus propias potencialidades.

También destacó la necesidad del completo desarrollo de las facultades humanas para practicar la virtud, y estableció como sus principales componentes a **la inteligencia** *(guía de la voluntad)*; **la inclinación a no cometer actos contrarios a la ética**; **la madurez** y **el justo medio** *(toda virtud se encuentra entre dos extremos: un exceso y un defecto, de entre los cuales debe ajustarse al medio más apropiado)*. Éstos son otros medios para alcanzar la virtud: **la templanza** *(entre el exceso del desenfreno y el defecto del embotamiento)* y **la liberalidad** *(en medio de la avaricia y el exceso de prodigalidad)*.

También afirmaba que todos los seres de este mundo están compuestos de *materia* y de *forma (hilemorfismo)*. En esta teoría, la sustancia del cuerpo (*materia* es el elemento individualizador y el alma la *forma*) es el elemento especificador. Todas las formas tienen la misma esencia y sólo se diferencian por la materia.

3.1.2.3 Doctrina ética cristiana

Su existencia se considera a partir de los cuatro evangelios reconocidos por la Iglesia católica: Marcos, Mateo, Lucas y Juan; esta filosofía ha sido una de las más difundidas y aceptadas en el mundo occidental. La ética cristiana toma como fundamento la representación de los máximos valores que emanan de Dios (Cristo), para que el hom-

bre intente alcanzar la perfección divina en este mundo *(la vida terrenal es temporal)*, obteniendo su recompensa en el cielo *(la verdadera vida está después de la muerte)*.

La base de esta doctrina es la búsqueda permanente de la virtud en el hombre, mediante las virtudes que predicó Jesús *(fe, esperanza y caridad)*, las cuales emanan de un poder superior y se citan en la epístola de San Pablo *"[...] virtud es una buena cualidad de nuestras almas, mediante la cual vivimos derechamente; cualidad de la que nadie puede abusar y que Dios produce a veces en nosotros sin nuestra intervención".*[13]

Esta doctrina afirma que los hombres son iguales ante Dios, sean pobres o ricos, hombres o mujeres, libres o esclavos, pecadores o santos, sacerdotes, etc., lo cual se sostiene en la tesis del amor entre los hombres y de que el perdón es la base del cristianismo.

Gutiérrez Sáenz sintetiza la filosofía cristiana en siete ideas capitales:[14]

***Dios**. El Creador y providente, que es amoroso y que le perdona todo al hombre. El máximo poder del que emanan todas las cosas del hombre y de su mundo.*

***El hombre**. El ser que actúa conforme a su albedrío para corresponder o no a los dones que Dios le brinda.*

***Cristo**. Encarnación de Dios, enviado a la tierra para la salvación de la humanidad, con el fin de que ésta imite su vida, obras y legados que dejó a través de sus discípulos.*

***Redención**. La salvación del hombre por medio del dolor, pobreza, sacrificio, muerte y resurrección de Cristo, con lo cual se da el perdón al hombre para su salvación permanente después de la muerte terrenal.*

***Iglesia**. Es la encargada de mantener, promulgar y unificar la proyección de Cristo, mediante la organización de los ideales del cristianismo.*

***El orden sobrenatural**. La vida terrenal es corta, mientras que la vida después de la muerte es eterna, y Cristo vino a salvar al hombre de las sombras, para que resurja en un nuevo mundo, siempre que sea virtuoso en la tierra.*

***La trascendencia**. El hombre se supera acercándose a Dios, que es el valor supremo. El objeto de la moral cristiana no es la felicidad sino el valor supremo, Dios. El hombre se realiza al acercarse a Dios.*

3.1.2.4 Doctrina ética kantiana

De la esencia de esta filosofía de **Emmanuel Kant** (1724-1804), destaca la diferencia que estableció entre una ley natural (aquella que no se da por el ser sino que éste sólo la interpreta y, por lo tanto, ésta es inquebrantable –**leyes naturales**–) y una norma social (la norma es una regla de conducta dictada por el hombre en su sociedad, la cual puede ser quebrantada en cualquier momento). Además, resalta la libertad del individuo para actuar de la manera que le parezca más conveniente (amoral, inmoral, moral y volitiva), a fin de elegir su conducta entre el **deber** y el **deber ser**. Claro está, enfatizaba Kant, en busca del valor moral sobre cualquier otra cosa.

Lo primordial de esta corriente es el fundamento de la moralidad, donde la conducta humana está ligada o subordinada a un **imperativo categórico,** el cual se subordina a los fundamentos morales que dicta la sociedad para alcanzar el nivel moral que rige el comportamiento del individuo (respeta a tus padres). También se tiene un **imperativo hipotético** que no tiene el mismo valor moral (si quieres dinero, trabaja), pero al cual también se subordina el individuo.

Kant también hizo énfasis en la importancia de los actos y sus relaciones con sus principales aplicaciones. Así encontramos como actos:[15]

***El acto intelectual**. Es el que pertenece al hombre para reproducir la voluntad divina, porque lo realiza con la inteligencia, entendida como la capacidad de seleccionar. Entre las múltiples posibilidades para lograr la verdad se encuentra el juicio, el cual viene a ser la diferencia específica entre la capacidad intelectual y la racional. Según Kant, el juicio está más allá del razonamiento, pués se combina con otras posibilidades de ampliar y demostrar una realidad verdadera o falsa.*

***El acto creador**. Es el que está vinculado con la estética y las grandes obras de arte que puede crear el hombre, como la literatura, la arquitectura, la música, la pintura, la escultura y todo lo que implica la jerarquía de la creación.*

***El acto volitivo**. Es el acto mediante el cual el hombre tiene la facultad de elegir, más allá del juicio, y que realiza bajo las reglas de conducta que la sociedad ha determinado. Éste es un acto de voluntad, no como juicio sino como una decisión íntima del ser humano.*

***El acto ético**. "El acto ético se efectúa en la sociedad, pero se determina y se soluciona en la intimidad del hombre; por lo tanto, la norma moral es interior aunque su manifestación sea exterior [...]."[16] El acto ético es unilateral e incoercible, debido a que beneficia o afecta al individuo que lo realiza y a su voluntad, aunque puede repercutir en las personas que le rodean, además de que no hay fuerza externa que exija su cumplimiento.*

***Los actos del deber**. Kant señala que estos actos pueden ser:*

***Acto amoral**. Porque carece de ética, ya que el individuo que lo realiza no actúa contra este acto, sino que desconoce el deber ser del mismo; por lo tanto, no actúa contra la moral sino que desconoce su significado.*

***Acto inmoral**. Aquí se tiene el conocimiento del acto inmoral y se actúa con pleno entendimiento contra la norma ética y la moral.*

***Acto moral**. El individuo actúa conforme al deber, haciendo que su voluntad se adecue a la norma; éste es un acto que se apega al deber que indica la propia norma.*

La esencia de la filosofía kantiana se encuentra concentrada en las obras: *Crítica de la razón pura* y *Crítica de la razón práctica*, *Fundamentos de metafísica de las costumbres* y *Metafísica de las costumbres*; en ellas, el filósofo destaca que la conducta del hombre deberá estar apegada a la moralidad en su sentido más puro, a través de la moral del de-

ber ser y por medio de los actos de voluntad del individuo, dándole a la ética el carácter de nobleza y altura moral en el hombre que busca la realización de sus ideales.

En su análisis a esta corriente ética, Gutiérrez Sáenz comenta:[17] *"1.- Fundamento de la moralidad, Kant critica los sistemas éticos anteriores a él [...] se basan empíricamente en ciertos objetos que consideramos como buenos y a los cuales debemos tender si es que queremos ser buenos. Contra esto se arguyen dos cosas: primero, nadie puede ponerse de acuerdo acerca del objeto efectivamente al que debemos tender. Unos creen que es la felicidad, otros dicen que es el placer, o las riquezas, etc*. [...] además, fundamentar la ética en un fin bueno cuya posesión nos perfeccione y nos haga felices [...]."

Aportaciones adicionales a esta corriente son: el ***racionalismo*** *(teoría filosófica basada en el predominio e independencia de la razón humana* —Descartes y Leibniz—. *Creencia en el poder absoluto de la razón frente a la fe),*[18] el ***apriorismo*** *(método sistemático del razonamiento a priori; el razonamiento de la causa a los efectos [...]),*[19] y el ***formalismo*** *(sistema metafísico que reconoce sólo el valor de la pura forma).*[20]

Un aspecto importante de la corriente kantiana es que da al hombre una autonomía completa, en cuanto a su deber ser, ya que el individuo realiza algún acto moral según su libre albedrío este acto será influido por motivaciones, coacciones o subordinaciones de carácter moral ajenas al individuo.

La filosofía de la ética kantiana tiene muchos estudiosos, los cuales no tan sólo han examinado esta corriente, sino que han tomado como sus antecedentes para el análisis al **empirismo psicológico** de **John Locke** (1632-1704) y **David Hume** (1711-1776), al **racionalismo intelectual** de **Gottfried Wilhelm Leibniz** (1646-1716) y **Christian Wolff** (1679-1754). También tenemos a **Johann Gottlieb Fichte** (1762-1814), **Friedrich Wilhelm Schelling** (1775-1854) y **Georg Wilhelm Friedrich Hegel** (1770-1831), quienes formaron parte de la ***escuela romántica alemana***.

3.1.2.5 Doctrina ética marxista

A través del materialismo histórico, la filosofía de la ética marxista difiere de las demás corrientes éticas, ya que considera que no existe sólo una moral sino diversas, según la clase social y la época en que vive el individuo; la principal diferencia con las otras doctrinas éticas se deriva del planteamiento materialista, en el cual la economía y los factores de producción están asociados a las diferencias morales de las clases sociales. Estas diferencias, según Marx, se establecen a través de las normas morales, con el único propósito de hacer formas para objetivar el dominio de las clases poderosas sobre las clases débiles.

Según Estrada Parra: *"Marx niega que existan principios éticos aplicables a cualquier sociedad, en tiempos y espacios absolutos. Las normas, señala, son producto de correlaciones de fuerzas económicas representadas en la lucha de clases."*[21]

El criterio del materialismo histórico, representado por Carl Marx (1818-1883) y Friedrich Engels (1820-1895), indica que las normas de conducta, dictadas por el

egoísmo de un grupo determinado, son falaces y niegan la libertad porque representan a la clase en el poder, la cual pretende engañar a la clase débil para así poder controlarla; tal es el caso de las normas religiosas y legales. De esta manera, las normas morales son producto de las relaciones socioeconómicas y tienen el propósito de mantener el dominio de las clases poderosas.

La ideología está muy presente en la ética marxista, la cual sostiene las siguientes tesis:

Lo que piensan los hombres es producto de la sociedad, entonces la conciencia se presenta como el lenguaje de la vida real, derivada de un resultado social.

La acepción primaria de ideología es negativa, en cuanto a que maneja ideas falsas y muchas veces falsificadoras de la realidad del hombre.

Los contenidos ideológicos de la conciencia, como la religión, la moral, la política, etcétera, carecen de una sustancia propia, de una historia y de un desarrollo que los sustenten.

Las formas ideológicas de la conciencia ocultan, desfiguran y suplantan, imaginativa o sustancialmente, la real existencia del hombre, ya que por medio de la alienación religiosa y económica de éste se busca mantener el dominio de la clase en el poder; esto se logra a través de la ***estäusserung*** *(exteriorización del hombre), en la cual se utiliza su fuerza de trabajo por medio de la* ***verässerung*** *(enajenación, expropiación de esa fuerza de trabajo), para así poder controlar a las masas, señalando lo que la gente debe desear y poseer para sentirse distinta y triunfadora. Y el hombre, como sociedad, no las cuestiona, sólo las acata.*

Para el marxismo, los *principios* de la ética del materialismo histórico señalan que:

La moral está condicionada por la sociedad y la lucha de clases.

El grupo en el poder dicta las reglas de acuerdo con las superestructuras (el ***materialismo,*** *que considera a la materia como infinita, eterna y autotransformable, y el* ***idealismo****, que considera a la divinidad como promotora del universo).*

La ética se modifica al cambiar los procesos de transformación de la sociedad por medio de la revolución de la lucha de clases.

El humanismo sólo se alcanzará cuando exista una sociedad sin clases.

Para **Gutiérrez Sáenz**, el ***materialismo dialéctico*** de **Marx** se concentra en los tres aspectos principales de su *cosmovisión*:

El materialismo*, donde "[...] lo primero es la materia, ella produce al espíritu y no al revés. Los que piensan al revés se llaman idealistas. Cualquier persona que crea en Dios también es tachada como idealista [...] La conciencia y el pensamiento, con ser inmateriales, no pasan de ser una propiedad, función y producto de la materia. [...] No hay seres espirituales independientes de la materia; por lo tanto, Dios, entendido como espíritu puro y creador del universo, no existe, sino que es una creación de la mente humana. Tampoco existe el alma espiritual e inmortal."*[22]

***La dialéctica**. De acuerdo con las leyes de Hegel, la tesis es la primera etapa de cualquier proceso evolutivo; la antítesis es cuando se manifiesta un sentido contrario con mayor énfasis a esa evolución, y la síntesis es la tercera etapa provocada por la conciliación de contrarios. Todos ellos son el motor de la historia, y se estudian para comprender los cambios del mundo. Lo anterior fue ampliado y profundamente explicado en el **Manifiesto del partido comunista**.*

***Alienación religiosa**. Una de las alienaciones más importantes que sufre el hombre es la religiosa: "[...] consiste en la idea mental de Dios a partir de lo mejor que tiene el hombre, para hipostasiar después dicha idea; es decir conferirle existencia real, y en seguida vivir sometido a la pseudolegislación originada de tal Dios, cuya existencia cree real y verdadera [...].* **La religión es el opio de los pueblos.**"[23] *Todo esto fue creado, según la ética marxista, con el único fin de lograr que el hombre viva de acuerdo al nivel que le corresponde como hombre, y se sigan manteniendo los tipos de explotaciones, opresiones y tiranías de la clase en el poder.*

***Alienación económica**. Viene a ser la explotación que sufre el hombre, por medio de la cual el trabajador es menospreciado en sus derechos y es obligado a vivir materialmente a un nivel infrahumano, ya que en el sistema capitalista, el trabajador sólo posee su fuerza de trabajo, por la cual recibe un salario de hambre y es confinado a la clase proletaria, mientras que el empresario, que se queda con el producto y fija el precio de éste, incluye la plusvalía o utilidad capitalista, la cual le va enriqueciendo para vivir en medio de lujos y derroches.*

La principal contribución del marxismo a la moral, es que el materialismo lucha por una sociedad sin clases, donde la conciencia del hombre se deriva de las relaciones sociales con una moral equitativa y fraterna, que sólo *se* alcanzará en un mundo sin diferencias de clases, y a través de la libertad que adquiere el individuo por la responsabilidad que tiene ante la sociedad sin clases, lo cual lo compromete con la causa social.

3.1.2.6 Doctrina ética existencialista

Nacida a consecuencia de las guerras mundiales, esta corriente filosófica se caracteriza por reflejar una situación política, cultural y social en crisis. Por esta razón, la población, y sobre todo la juventud, la adoptaron como una nueva forma de ética, ya que tenían una sensación generalizada de desamparo y buscaban afanosamente comprender cuál era la esencia de la vida, muchas veces sin lograrlo.

"Esta corriente sustenta que la realidad del hombre es su existencia y que no es necesario buscar una esencia más allá de esta vida, la cual es concreta, doliente, circunscrita y perfectamente establecida. Donde la conducta del hombre obedece a su angustia."[24]

El existencialismo tiene dos escuelas fundamentales; por un lado, el **existencialismo espiritualista**, iniciado por ***Sören Kierkegaard*** (1813-1855) autor del tratado, *Con-*

cepto de angustias y ***Miguel de Unamuno*** (1864-1936***)***, que tienden a buscar un valor superior (espiritual) que se acerca a lo religioso y que está más allá del ser concreto.

Esta corriente espiritualista se caracteriza por una búsqueda permanente de un ser supremo que está más allá de esta vida, con lo cual la permanente angustia del hombre es solucionada en parte con la fe en ese poder superior.

Por otro lado, en contraposición a la anterior, encontramos el **existencialismo materialista**, propuesto por ***Jean Paul Sartre*** (1905-1980) , el cual señala que no hay ninguna esperanza más allá de la materia.

Esta corriente metodista, se concentra en la existencia como lo único y lo primordial del individuo, que se refleja en una permanente angustia de éste por su existencia, a la cual no le encuentra ninguna solución, además de que tiene una libertad, casi absoluta, para encontrar el propósito de la vida, sin llegar a nada en concreto, sólo para vivir la existencia.

Para Sartre, los valores son relativos y de carácter subjetivo, por lo que el individuo crea su propio ser y su propia responsabilidad a través de su libertad. Por lo tanto, no hay valores morales que pueden ser universales, porque esto es contrario al hombre, ya que los seres humanos son responsables de sus propios actos al tomar sus propias decisiones. Consecuentemente, la moral, según Sartre, es subjetiva porque lo bueno es lo que cada cual elige; con base en esto, los valores morales impuestos por la sociedad no son propios de un individuo, por lo que éste no tiene la obligación de acatarlos.

El hombre es más que lo que él mismo sabe de sí, ya que alcanza niveles y estratos de acuerdo con su propia capacidad. Para el existencialismo, el hombre no es algo acabado sino algo único y particular que se nutre de los triunfos y derrotas que acumula a lo largo de su vida.

Entre las principales aportaciones del existencialismo están: ***el ser en sí*** *"[...] es el existir de un ser puro y simple, más sin intencionalidad, sin intimidad y, consiguientemente, sin posibilidad de que lo ajeno infunda también su realidad a lo propio"*,[25] y ***el ser para sí***, *que es el hombre que, como individuo, sufre y goza de una realidad en la cual él mismo se afirma y se transforma en todos los aspectos de la vida*.

3.1.2.7 Doctrina ética pragmática

El pragmatismo es una corriente en la cual la realización de los actos es impuesta sobre los ideales; donde la meditación y la concepción son más importantes si se apegan a la praxis (*conjunto de actividades que pueden transformar al mundo, como el conocimiento o los fenómenos [...]*), en relación con las corrientes del pensamiento ideal.

Al pragmatismo se le identifica con **pragmática,** *"del griego* ***pragma****, hecho, actividad; doctrina que se basa en el estudio de los hechos".*[26] El pensamiento filosófico de esta corriente se refiere a lo que éticamente es útil, es decir, la praxis es la aplicación real de la teoría moral en un mundo apegado estrictamente a las necesidades cotidianas del hombre, pues sus valores morales se derivan de las acciones realizadas por

el individuo en su familia, en la sociedad y en una determinada nación, y la voluntad de creer se da de acuerdo con las emociones personales.

En el pragmatismo, según ***William James*** (1842-1910), fundador de esta corriente filosófica, con la voluntad de creer emocionalmente, tanto en los valores como en la religión, se evita que se presente la ética como sistema, debido a que esos conceptos dependen de las emociones personales y están inmersos dentro de un mundo de sentimientos influidos por la utilidad que tengan los preceptos morales y económicos para el individuo, la familia y la sociedad; incluso para un país. Así, la conciencia es más una forma personal de entender los sentimientos, si éstos son de utilidad al individuo. Estos varían según la personalidad del individuo y la influencia económica cotidiana.

Entre los principales conceptos que se manejan en el pragmatismo se encuentran:

La verdad. Para James consiste en la relación de lo que es posible comprobar y que el hombre adopta como suyo, pues si no es así, esas ideas se consideran falsas. La verdad es parte de lo que las ciencias afirman, pero también de lo que proponen la conducta y el espíritu humano. Además, tanto para James como para **Charles Peirce** (1839-1914) y **John Deway** (1859-1952), la verdad se identifica como lo útil, principalmente con aquello que pueda contribuir al mejor desarrollo del ser humano y a la convivencia con los demás.

Lo bueno (como valor de la bondad y parte de la filosofía) es opuesto para el pragmatismo, ya que para esta doctrina, lo bueno es aquello que se inclina a la realidad objetiva del hombre y que favorece a la economía del individuo, de la familia, de la sociedad o de la nación; es decir, sólo es bueno aquello que tiene una aplicación económica e inmediata para el individuo, de la cual pueda obtener una consecuencia concreta, tangible y derivada de una experiencia expresa de sus tendencias prácticas y cotidianas. Incluso, para el **utilitarismo extremo**, lo bueno sólo es aquello que es útil de manera inmediata para el hombre, lo cual se deriva de frases tales como: *"no hay mejor amigo que una moneda en la bolsa"* y *"dime cuánto tienes y te diré cuánto vales"*. Estos conceptos han distorsionado los valores morales de las anteriores doctrinas éticas.

Influido por sus ideas de psicología, James proponía que no sólo es importante atender los problemas lógicos del hombre, sino también los de índole religiosa, emocional y moral, los cuales se pueden asociar con las experiencias directas de los individuos, tales como las sensaciones y las percepciones personales, a fin de encontrar una filosofía de la conciencia que derive en valores morales y religiosos, dentro de un empirismo radical.

La esencia de esta corriente ética pragmatista se concentra en que, para el hombre actual, es más fácil intentar acumular riquezas y vivir dentro de una economía boyante, sin importarle que para ello tenga que aplastar, manipular y/o explotar a sus semejantes; todo antes que renunciar a lo superfluo que le da el dinero al propio individuo, a su familia y a su país y, mucho menos, en reconocer los valores y derechos de los demás; sobre todo en lo relacionado con los valores éticos tradicionales y los derechos del individuo en la sociedad.

3.2 Principios de axiología y valores éticos

Para poder hablar de los valores del auditor de sistemas, lo primero es considerar las bases fundamentales de la ciencia que estudia la teoría filosófica de los valores; esto se profundiza mediante la *axiología*, cuyo significado es:

***Axiología** se deriva del griego **axios**,* valor *y **logia** (de **logos**),* tratado o teoría*, teoría del valor.*[27]

"Ciencia de los valores, en especial de los valores morales."[28]

La axiología entonces es la ciencia que trata de los valores de carácter moral que pretenden normar la conducta de los individuos ante la sociedad; es evidente que el auditor, como parte de una sociedad, debe considerar y acatar los valores ético-morales regulados mediante esta ciencia. Por ello, es necesario profundizar un poco sobre estos valores, antes de proponer las normas éticas que regularán la actuación del auditor de sistemas computacionales.

Aunque la definición de valor es la siguiente: *"del latín **valor-oris**, de **valore:*** valer. *Precio, costo o utilidad o valía"*,[29] desde el punto de vista filosófico estos conceptos adquieren otro significado, pues desde la antigüedad así se designaban los bienes de la cultura y los bienes vitales o espirituales del individuo, de los cuales no se concebía su existencia como entes aislados ni autónomos, sino como los atributos indispensables del ser. (Estrada Parra: 1992-1994.)

Según Estrada Parra, cuando cita a **Max Scheler,** señala que los valores son cualidades del orden material, aunque también son objetos ideales. Esto último fue explicado por **Hartmann.** Para **Aristóteles**, *la bondad, la belleza, la justicia, la verdad y la santidad* son entes que no son reales sino meramente ideales; aunque éstos se han considerado como los principales valores que dan las pautas del valor filosófico que pretende alcanzar el ser.

Las características de los valores son:[30]

***Objetividad**. Los valores existen en sí y por sí mismos, y no es necesaria su realización para que existan. Son independientes del sujeto que los obedece o destaca*.

***Dependencia**. Aunque los valores tienen existencia propia, están subordinados a la realidad, lo cual permite que el ser humano conozca su existencia. Además, a pesar de su intemporalidad, los valores son parte de la realidad*.

***Polaridad**. El valor siempre se presenta como una forma de perfección, y es una forma antagónica de la imperfección o la carencia. El valor verdadero se opone al falso, la belleza a la fealdad, la bondad a la maldad*.

***Cualidad**. Los valores no están relacionados con la cantidad sino con la cualidad; éstos no existen porque puedan aumentar o disminuir, sino porque el hombre se adecua o se acerca a ellos*.

Jerarquía. *Los valores se dan en un orden establecido, según su importancia, y este orden se modifica según quien los clasifica*.

Como complemento de esos conceptos, a continuación vamos a estudiar los principios y valores éticos iniciados por ***Max Scheler*** (1874-1928) y ***Nicolai Hartmann*** (1882-1950), también conocidos como **axiología de Scheler**; cuya tesis central es la materialidad y objetividad de los valores, oponiéndose al formalismo de Kant, *"[...] Según Scheler, los valores se conocen por medio de la intuición, y no son accesibles a la razón; ésta es ciega para los valores"*.[31]

Existen dos clases de intuiciones: **la intuición eidética** (de tipo racional), por medio de la cual se captan las esencias lógicas, por ejemplo los teoremas, y la **intuición emocional,** que capta otro tipo de objetos, las esencias analógicas, por ejemplo los valores.

Para Scheler, los valores son jerarquizados de acuerdo con esta propuesta:[32]

Valores de lo agradable y lo desagradable *(jerarquía de grado inferior). Son los que tienen relación inmediata con los sentidos y las sensaciones del placer contra el disgusto.*

Valores de lo vital y lo antivital *(jerarquía de grado medio inferior). Son aquellos cuya convergencia está encaminada a conservar y ampliar la vida en contra del aniquilamiento. Raúl Gutiérrez Sáenz cita esta jerarquía como valores de lo noble y de lo vulgar.*[33]

Valores espirituales y no espirituales *(jerarquía de grado superior). Son los que están más allá de los entes físicos, aunque sólo se perciben a través del hombre.*

Valores religiosos y profanos *(valores de grado superior). Son aquellos que se dan entre la tesis de lo santo y lo profano.*

También se puede citar la clasificación propuesta por **De Finance**, quien agrupa la jerarquía de los valores como sigue:[34]

Valores infrahumanos. *Son aquellos que perfeccionan al hombre en sus estratos inferiores: la fuerza, el placer, la salud, la agilidad, etcétera.*

Valores humanos inframorales. *Aquí se colocan todos los valores humanos:*

Valores económicos
Valores no-éticos
Valores estéticos
Valores sociales

Valores morales. *Son los valores que dependen exclusivamente del libre albedrío del individuo, en busca de la virtud y el nivel íntimo del comportamiento del individuo. Por ejemplo, entre éstos tenemos: la virtud, la prudencia, la justicia, la fortaleza y la templanza.*

Valores religiosos. *Considerados como el nivel superior, pues dependen de las potencias superiores al hombre. Por ejemplo, la santidad, la gracia, la caridad, etcétera.*

Según el criterio del mismo pensador, analizaremos las características de los valores:[35]

Son cualidades ideales, *pues existen en el espacio y en el tiempo, aunque no reales.*

Son alógicos, *no captables por la razón, sólo se perciben pero no son lógicos.*

Son contenidos a priori, *nacen de la comprensión de nuestra propia experiencia a través de la intuición.*

Son objetivos, *se dan independientemente de que sean conocidos o estimados.*

Son trascendentes, *como son cualidades ideales, trascienden a los demás.*

Son materiales, *tienen un contenido concreto que no se reduce a una pura forma o estructura universal, sino que se materializa en la esencia del ser.*

Se distinguen respecto al bien*, pues mientras el bien puede ser destruido, el valor permanece sin ser destruido.*

3.2.1 Principales valores y virtudes de José Armando Estrada Parra[36]

La veracidad

Es la capacidad que tiene el individuo para expresarse con acierto y honradez en la opinión que emite de un suceso, buscando acercarse siempre a la verdad de lo que narra o interpreta.

La comprensión

Es el conocimiento perfecto de las circunstancias de la persona cuyos problemas se desean entender, adentrándose en su vivencia.

La tolerancia

Es la capacidad para ser indulgente con la manera de pensar, sentir y actuar de los demás, aunque esta manera de pensar sea diferente a la nuestra, condescendiendo con ellos al saber escucharlos y comprenderlos.

La bondad

Aunque es de los valores que se consideran de mayor jerarquía, es de los más difíciles de explicar, aunque es fácil de entender intuitivamente. Calidad de lo bueno, indica el diccionario; pero representa la cualidad de no sólo actuar con bondad, sino de actuar además con bien.

El respeto

Es reconocer y considerar que todos los individuos tienen derechos, opiniones, criterios y privilegios, a fin de vivir en armonía y comprensión con nuestros semejantes.

La valentía

Entendida como arrojo, ánimo, es propiamente lo que se encuentra entre los extremos, por un lado el arrojo irreflexivo, temeridad y por otro la cobardía; esta virtud está acompañada de un control sobre los actos.

La templanza

Moderar los apetitos, las acciones, sentimientos y deseos, a fin de actuar con madurez y serenidad ante las circunstancias que se presentan. También se considera una de las virtudes cardinales del cristianismo.

La justicia

Es la constante y permanente voluntad de dar a cada quien lo que le corresponde, actuando con equidad e imparcialidad. También es una de las virtudes cardinales.

3.2.2 Principios y valores del auditor[37]

Los siguientes son los aspectos fundamentales que debe poseer el profesional que se quiera dedicar a la actividad de auditoría, a fin de que identifique y cumpla los requerimientos que le marca la sociedad para realizar esta función.

Honestidad

Se dice de quien actúa con veracidad, sinceridad, franqueza, honradez e imparcialidad en el cumplimiento de cualquier encomienda, actividad o trabajo. En el caso del auditor, es el cabal cumplimiento de cada una de estas cualidades, con lo cual proporciona la garantía de calidad profesional y moral que demandan de esta actividad las empresas y personas.

Integridad

La persona que posee esta cualidad es de principios sólidos y fundamentales y actúa en forma honorable, recta, valerosa y se apega a sus convicciones, cualesquiera que éstas sean, y las hace respetar; lo mismo sucede con el cumplimiento de los compromisos, trabajo y actividades que se le encomiendan. Está claro que el profesional que actúa como auditor debe poseer estas cualidades.

Cumplimiento

Se dice que una persona es cumplida y digna de confianza, cuando cumple escrupulosamente sus promesas, sus compromisos y respeta la esencia y letra de los convenios que contrae. Es obvio que el auditor que desea poseer esta cualidad debe actuar conforme se indica en este punto, ya que será lo que le ayudará a realizar cabalmente sus actividades.

Lealtad

Es la cualidad que caracteriza a quien es noble, recto, honesto y honrado con su familia, sus amigos, patrones, clientes y con su país, respetando sobre casi todas las cosas una adhesión y constancia con quienes le unen lazos de amistad, amor o profesionalismo. En el caso del auditor, además del cabal respeto a lo anterior, también se considera que es la fidelidad que guarda para con sus auditados, no utilizando ni revelando información que obtiene en forma confidencial de la empresa que audita. En el contex-

to profesional, también se entiende como la emisión de juicios independientes, profesionales y apegados a lo que detectó en su evaluación, evitando cualquier influencia indebida y conflicto de intereses.

Imparcialidad

Es cuando una persona, en este caso el auditor, busca actuar de manera equitativa en el cumplimiento de su trabajo o de cualquier acción que emprende, tratando de ser siempre justo, honesto y razonable en los juicios que emite, y evitando, tomar partido hacia algún lado en cualquier auditoría. Además, como profesional de la auditoría, siempre debe estar dispuesto a reconocer errores y a cambiar de posición, creencia y acciones cuando sea necesario, y debe procurar actuar siempre con un amplio compromiso de justicia, equidad, tolerancia y trato igual con los funcionarios y empleados que audite. Lo mismo se aplica a otros profesionales.

Respeto a los demás

Es la cualidad que caracteriza a quien demuestra consideración y estima por la dignidad, la intimidad y el derecho de autodeterminación de la gente, al actuar siempre de manera cortés, expedita y decente, y al proporcionarles lo que necesitan para la mejor toma de decisiones, sin avergonzarles ni degradarles. Esto es lo que debe hacer el auditor, independientemente del puesto y posición que representa para las empresas.

Ciudadano responsable

Se dice de la persona, en este caso del auditor, que está dispuesta a respetar y hacer cumplir las leyes, normas y reglamentos del país, al aceptar la responsabilidad y solidaridad, tanto en los derechos como en las obligaciones, que le imponen la sociedad, las empresas y sus conciudadanos. Esta persona respeta los principios y reglas que regulan las relaciones laborales, morales, comerciales, sociales y de cualquier otro tipo; también evita y, en su caso, protesta contra las injusticias.

Ver por los demás

Cuando una persona es atenta y amable en su trato, cuando es compartida, generosa y además tiene un amplio sentido de ayuda hacia sus semejantes, se dice que esa persona ve por los demás; ésta, específicamente, es una de las principales funciones que debe cumplir el auditor, ya que como su actividad fundamental es auditar (en este caso evaluar el trabajo de jefes y empleados), siempre estará en contacto con los demás, pero desde una posición de supervisión. Por esta razón debe tener un trato amable, cortés y justo con los que audita. Si es posible, debe ubicarse en el lugar de los demás para tratar de comprender sus reacciones.

Búsqueda de la excelencia

Es evidente que las personas de éxito, así como los auditores profesionales destacados, son aquellos que buscan la excelencia *(que sobresalen en mérito y bondad)* como

parte fundamental de su ser, cumpliendo indefectiblemente con la responsabilidad personal y profesional que requiere esta importante actividad. Estas personas procuran, en todas sus acciones, ser siempre diligentes, confiables, trabajadoras y comprometidas con el servicio que prestan a las empresas, realizando su trabajo, en este caso la evaluación de las áreas que auditan, lo mejor que pueden. También tienen un alto grado de competencia, capacitación y conocimientos relacionados con la auditoría, los cuales les ayudan a realizar con mayor efectividad y eficiencia su actividad profesional.

Responsabilidad

Se entiende como responsabilidad el hecho de aceptar el compromiso que implica la toma de decisiones y las consecuencias previstas por las acciones y omisiones en el cumplimiento del trabajo, de las actividades cotidianas y del desempeño profesional. En el caso específico del auditor, con la evaluación que realiza y con el dictamen que emite, adquiere el compromiso ineludible de una actuación profesional, aceptando plenamente las consecuencias de su actuación personal.

Confiabilidad

Ésta es una de las cualidades más buscadas en el profesional que se dedica a la auditoría, ya que se asume que su actuación está apegada a las normas y criterios que regulan esta profesión *(ánimo de hacer las cosas con rectitud)*. Por esta razón el auditado puede confiar en que el auditor aplicará las herramientas y métodos necesarios para realizar la auditoría y, derivado de ello, confía en la capacidad profesional de dicho auditor y acepta los juicios que emite.

Veracidad

Derivada de ***veraz*** *(el que dice o profesa la verdad),* se confiere veracidad a quien actúa con la suficiente honestidad, experiencia y conocimientos en su ramo, para emitir opiniones y juicios que estén avalados por una confianza en lo que dice, contando con que su actuación siempre será apegada a la verdad. En el caso del auditor, se refiere a la utilización de herramientas, métodos y procedimientos de auditoría, con los cuales puede obtener datos fidedignos, apegados a los sucesos verdaderos y con resultados reales, que le permiten hacer juicios fidedignos y confiables. Por esta razón, se le otorga al auditor, o a cualquier persona, la confianza de que está actuando con suma veracidad.

3.2.3 Principios y valores según alumnos de la UVM San Rafael

Alumnos de diversos semestres de la *Licenciatura en Sistemas de Computación Administrativa* del plantel San Rafael de la Universidad del Valle de México, realizaron en ésta una serie de encuestas sobre los valores y principios éticos y morales de los habitantes del D. F.,[38] cuyos resultados, de acuerdo con el universo y la muestra elegidos, pudieran hacerse extensivos hacia el comportamiento general de los mexicanos.

En estas aportaciones se mencionan únicamente los aspectos señalados por los alumnos, quedando a juicio del lector aceptarlos, rechazarlos y, en su caso, adaptarlos a las características propias del área y empresa que aplica la auditoría.

Integridad familiar

Es un gran sentimiento que aún se conserva entre los mexicanos, en el cual se le da el más alto valor a la integridad familiar, a la conservación y respeto hacia los vínculos familiares que nos unen a nuestros parientes. Es una tradición mediante la cual se conserva dicha unión de padres a hijos, e incluso se hace extensiva hacia los abuelos, tíos, sobrinos, primos y otros parientes. Éste se considera como uno de los valores fundamentales del pueblo mexicano. Este valor se conserva y se aprende por medio de la transmisión familiar, mediante la cual se heredan las costumbres y tradiciones que mantienen vigentes los lazos de unión familiar, base de los principios morales y éticos de la sociedad.

Creencia religiosa

Otro de los más altos valores que conservan los conciudadanos, es una firme creencia en la religión, principalmente en la católica, aunque también existen otras con muchos creyentes. Esto ayuda a establecer, difundir y preservar las normas y principios morales (básicamente de tipo religioso) que regulan la conducta del individuo ante la sociedad.

Ingenio

Es la capacidad generalizada de adaptarse fácilmente a los problemas cotidianos, mediante la cual se pueden resolver, o por lo menos sobrellevar, casi todas las situaciones conflictivas que se les presentan a las personas. También se dice de la capacidad de responder a los retos y frases dicharacheras de sus congéneres, que provocan hilaridad. Es una cualidad que aún se transmite, conserva y en mucho ayuda a realizar mejor el trabajo, cualquiera que éste sea.

Valor

Es la capacidad de afrontar con valentía, atrevimiento y dignidad las situaciones y problemas que se presentan cotidianamente. Esta cualidad ayuda a realizar cualquier actividad que se emprende. En el caso de los auditores, es la valentía para actuar en la evaluación y emisión de los resultados de su revisión.

Honradez

Es la actitud que hace que la persona proceda con rectitud e integridad ante los demás, y que sea incapaz de tomar algo que no le corresponde. En el caso del auditor, es uno de los requisitos fundamentales para su actuación profesional.

Responsabilidad

Es la plena aceptación para responder ante los demás acerca de las acciones, actividades y omisiones que se hacen, así como de las decisiones que se toman, aceptando sus consecuencias y beneficios. En el caso del auditor, se refiere a la plena aceptación de las acciones y actividades que realiza y de las decisiones que toma como parte de su actuación profesional.

Lealtad

Se dice de la cualidad que tiene aquel que es sincero, honrado y fiel con los demás y consigo mismo. Es decir, aquel que guarda fidelidad a una persona o a una cosa, y que actúa respetando los bienes y acciones de los demás. En el caso del auditor, es la fidelidad que guarda con sus auditados, respetando invariablemente la información, bienes y resultados que obtiene de una evaluación, sin utilizar para sí o para terceros los datos que obtiene en dicha evaluación.

Patriotismo

Es la procuración del bienestar y conservación de los valores nacionales, los cuales son vínculo de unión entre las naciones, los pueblos y los individuos.

Los anteriores son algunos de los muchos principios y valores que debe poseer el auditor dedicado al área de sistemas computacionales; sin embargo, el lector tiene plena libertad de aumentar, eliminar o modificar algunos de los aspectos antes expuestos. Lo importante es que capte la esencia de estas aportaciones en la actuación de un auditor profesional.

3.3 Criterios y responsabilidades del auditor

Los criterios y responsabilidades que analizaremos a continuación vienen a complementar los conceptos antes señalados. Estos criterios son presentados con el propósito de señalar al auditor el rumbo ético y moral que deberá seguir para cumplir y hacer respetar dichos criterios y responsabilidades, y para que norme su actuación profesional ante las empresas, la sociedad y sus colegas, esmerándose en el buen cumplimiento de esta actividad; no sólo cuando le sea encomendada una auditoría, sino también en su desempeño personal.

Está claro que la verdadera aplicación de estos criterios y responsabilidades estará relacionada íntimamente con las normas de cada institución en donde actúe el auditor, así como con la experiencia, conocimientos, aptitudes y ética de este último.

El estudio de estas regulaciones se puede agrupar en los siguientes aspectos fundamentales:

Criterios y responsabilidades del auditor en el aspecto ético-moral

Criterios y responsabilidades del auditor en el aspecto profesional-personal

Criterios y responsabilidades del auditor en el aspecto laboral

Criterios y responsabilidades del auditor en el aspecto de elementos de juicio

Criterios y responsabilidades del auditor en su respuesta ante las autoridades, leyes, normas y reglamentos

Criterios y responsabilidades del auditor en la presentación de resultados a terceros

Conviene destacar que en este inciso sólo se hace un breve análisis de los principales aspectos de estos criterios y responsabilidades de la disciplina de la auditoría; por esta razón, a continuación se hace un breve examen de cada uno de los asuntos que afectan el comportamiento del auditor.

3.3.1 Criterios y responsabilidades del auditor en el aspecto ético-moral

Los criterios y responsabilidades que a continuación se proponen, conciernen a los juicios de valor que regularán las actividades y convenios que se pacten entre dos individuos, *en este caso el auditor* y *el auditado,* en relación con la aplicación y observancia de las reglas y obligaciones que regularán los vínculos profesionales y personales entre ambos. También se señalan los principales *aspectos éticos y morales* que se presentan entre este profesional y el personal que es auditado, e incluso entre sus colegas.

Entre los criterios y responsabilidades del auditor se encuentran:

Los que son regulados por los códigos, leyes y reglamentos vigentes en México

Son los criterios, normas, reglamentos, condiciones y obligaciones que, establecidos por escrito en documentos formales, serán los lineamientos que regularán el ejercicio de las actividades públicas y privadas de los profesionales dedicados a la auditoría en México. Estos aspectos sirven para establecer los límites permisibles de actuación en las relaciones cotidianas de trabajo, sociales, jurídicas y profesionales del auditor. Estas relaciones deben ser reguladas y estar vigentes en las leyes nacionales.

Los que son regulados por las asociaciones y colegios de profesionales de la auditoría

Son los criterios, normas, condiciones, obligaciones y reglamentos emitidos, difundidos y sancionados por las asociaciones de profesionales y agrupaciones de personas dedicadas a una misma actividad profesional, en este caso a la auditoría. Estos criterios son acordados entre dichas agrupaciones con el propósito de regular las actividades, obligaciones y funciones del auditor.*

* En México existen varias asociaciones colegiadas de profesionales, las cuales regulan las actuaciones de sus agremiados y, en algunos casos, sólo los afiliados a estos colegios y asociaciones están facultados para actuar como auditores y emitir dictámenes válidos para las empresas y autoridades. Tal es el caso de los contadores públicos (IMCPAC) y los licenciados en administración (CONLA).

Los que son establecidos por los contratos pactados entre el cliente y la empresa auditora

Cuando se establecen contratos de trabajo entre una empresa y un auditor, generalmente se establecen los criterios, normas, reglamentos, condiciones y obligaciones que servirán para regular las actividades y funciones de este último. Asimismo, se establecen los honorarios del auditor y sus expectativas de trabajo.

Estos criterios también se aplican en el caso de los auditores internos, salvo que se complementan con los lineamientos internos de la empresa donde prestan sus servicios.

Las normas, lineamientos y políticas de la empresa auditada y de quien realiza la auditoría

Cada empresa tiene establecidos los criterios, condiciones y obligaciones que deben ser respetados por el personal que labora en ella; es decir, deben ser adoptados e invariablemente observados por el auditor y sus colaboradores, sin pretender cambiarlos o incumplirlos. Esto obedece a que son los aspectos vigentes que regulan la actuación de quienes colaboran con la empresa. Por lo tanto, es obligación del auditor vigilar que dichos criterios sean acatados por el personal que está siendo auditado y por sus propios colaboradores, ya que estos lineamientos son los aspectos fundamentales que regularán el desarrollo de las actividades, funciones y obligaciones de la propia institución.

Las normas de auditoría del IMCPAC[39]

El instituto que agrupa a los contadores públicos en México, emite periódicamente una serie de boletines para sus socios dedicados a la actividad de la auditoría, en los cuales indica los criterios, normas, reglamentos, condiciones y obligaciones que regulan el desarrollo de las actividades profesionales de dichos auditores en las evaluaciones contables de las empresas.

Específicamente, éstos tienen que cumplir las siguientes normas personales:

Entrenamiento técnico y capacidad profesional
Cuidado y diligencia profesional
Independencia

En estos lineamientos se establecen, en forma precisa, todas las condiciones de actuación y obligaciones personales que tienen estos profesionales para con la empresa auditada, con sus colegas y con las autoridades tributarias del país.*

Las normas de auditoría del CONLA[40]

En este colegio se agrupan los profesionales dedicados a la administración en México, y, al igual que el instituto señalado en el punto anterior, emite periódicamente una se-

* En México, los únicos autorizados a realizar auditorías contables, fiscales y financieras, son los contadores públicos titulados y asociados a los colegios de contadores del país.

rie de criterios, normas, reglamentos, condiciones y obligaciones que pretenden regular las actividades de los profesionales de la administración dedicados a la auditoría.

Además, mediante dichas publicaciones, contribuye a que sus asociados conozcan y se actualicen en las herramientas, procedimientos y actividades que les ayudarán a desarrollar mejor su trabajo, mismas que están obligados a seguir y utilizar para que sea aceptado su trabajo como verdaderos profesionales de esta actividad.

Dichos lineamientos son las condiciones fundamentales que regulan la actuación en la práctica de la auditoría administrativa; así como las obligaciones que tienen estos profesionales para con la empresa auditada, con sus colegas de profesión y con las autoridades del país.

Recientemente, se ha publicado y actualizado el *Código de Ética Profesional del Licenciado en Administración*, en el cual se regulan las labores que realizan los licenciados en administración, no sólo las del área de auditoría, sino en todas sus actividades de carácter profesional.

La ética profesional y moral del auditor

En razón del persistente ejercicio de su profesión, el auditor constantemente va acumulando experiencias, habilidades y conocimientos que le permiten perfeccionar sus criterios, normas, reglas de actuación y obligaciones, las cuales en mucho le ayudan a regular su actuación profesional ante las empresas que audita; con esto fortalece su ética personal y su conducta profesional en los trabajos que realiza para dichas empresas, ante las autoridades que le sancionan y ante sus colegas.

Las de la propia profesión de auditoría

Ya hemos señalado los criterios, normas, reglamentos, condiciones y obligaciones estipulados por las autoridades, asociaciones y empresas de México, los cuales determinan los lineamientos que regularán la actuación de estos profesionales ante sus clientes. Pero también existen otros lineamientos, generalmente no escritos, que ayudan a normalizar la actuación de los profesionales dedicados a la auditoría. Estos criterios regulan la conducta y los principios ético-morales que tratan de establecer los lineamientos de ética profesional, conducta personal y servicio profesional que deben observar los auditores.

3.3.2 Criterios y responsabilidades del auditor en el aspecto profesional-personal

Recomendamos que los criterios y responsabilidades que en seguida presentamos, también sean considerados como obligaciones morales y éticas por quienes se dediquen a la profesión de la auditoría, ya que son parte integral de las funciones cotidianas del auditor, aunque a veces no se encuentren formalmente establecidos ni estén señalados en algún escrito, ni contengan sanciones específicas para cuando no sean totalmente acatados.

Cabe destacar que el incumplimiento de estos aspectos por parte del auditor, le puede provocar consecuencias de tipo legal; sin embargo, en caso de incumplimiento de estos criterios y obligaciones, su principal sanción será de tipo profesional, moral y social, debido a que puede acarrearle desprestigio laboral y profesional ante sus colegas, ante las empresas, las autoridades y sus conciudadanos. Además, en muchos casos, esto evidencia la incapacidad de este profesional en la realización de sus funciones, entre muchas otras repercusiones de carácter profesional y personal que le puede acarrear tal incumplimiento.

Como en los casos anteriores, a continuación sólo se mencionan algunos de los lineamientos más sobresalientes de este punto, dejando al lector que, de acuerdo con su criterio, experiencia y necesidades específicas, establezca aquellos que sean útiles para su práctica de auditoría. Para nuestro caso citaremos los siguientes aspectos.

Tener la suficiente independencia mental y profesional para ejercer la profesión de auditor

El primer requisito que debe poseer quien se dedica a esta profesión, es que debe estar totalmente libre de cualquier tipo de influencia; es decir, debe ser autónomo en su actuación y no permitir ningún tipo de injerencia, ya sea de carácter interno o externo, evitando verse influido por obligaciones laborales, convicciones morales, prejuicios personales, aspectos religiosos, deseos insanos, normas de conducta equivocadas o por cualquier otro tipo de influencia que le impida actuar con una absoluta independencia mental, tanto en el plano personal como en el profesional.

Si un auditor actúa sin tener la suficiente libertad de acción y se deja influir, ya sea en lo personal, profesional o laboral, su intervención y su responsabilidad serán muy pobres y sus alcances y resultados estarán muy limitados. Además, su evaluación será muy deficiente, limitada y poco ética. Por esta razón, no cumplirá cabalmente con el cometido que se le encomienda.

Contar con la calificación, habilidad, aptitud y experiencia profesional en auditoría

El auditor es un profesional especializado que debe tener un amplio cúmulo de conocimientos, métodos, herramientas y técnicas específicas de auditoría, a fin de que pueda realizar su trabajo con eficiencia y eficacia.

Sin embargo, además de lo anterior, este profesional debe poseer otras características personales que son representativas del auditor, tales como la constancia, la honradez, el valor, la confianza en sí mismo, la tenacidad, la capacidad analítica y otras peculiaridades de personalidad que en mucho le ayudarán a incrementar sus habilidades naturales para desempeñarse como un buen auditor. Además, debe contar con la suficiente experiencia profesional para el buen desempeño de su trabajo; también debe contar con la calificación profesional que le otorgue el grado de auditor. El ideal sería que el auditor, como profesional, cuente con todas estas cualidades.

Manejar adecuadamente las relaciones personales, profesionales y laborales entre él y el auditado

Actuar como auditor no es una tarea fácil y muchas veces resulta una labor muy ingrata y poco gratificante, debido a que éste revisa el trabajo de los demás y aplica su criterio para evaluar su adecuado cumplimiento, cosa que no es del agrado de muchos. Por ello, a veces sus relaciones con los auditados no son siempre gratas, tornándose ásperas, poco cordiales y a veces agresivas y problemáticas, razón por la cual tiene que aprender a sobrellevar las situaciones que se le presenten cotidianamente en su trabajo.

Por otro lado, también se llega a dar el caso de que, por lo que representa el auditor, los auditados dan ciertas muestras de amistad, frecuentemente poco sinceras, cuyo único objetivo es evitar o minimizar los problemas que se pudieran presentar con la auditoría. Con estas actitudes, el auditado busca influir en el ánimo del auditor poco avezado en estos trabajos. Incluso, en no pocos casos, con estas acciones se puede desvirtuar su trabajo, tanto por la agresión que siente, la cual puede influir en su ánimo, como por la simpatía que le despiertan sus auditados, la cual puede ocasionar cierta parcialidad.

Utilizar la misma metodología y procedimientos de evaluación establecidos por los responsables de la gestión de la auditoría

Como profesional de la auditoría, el auditor debe utilizar invariablemente la misma metodología, procedimientos, herramientas y técnicas que se hayan establecido para la revisión de las áreas, resultados, operaciones y actividades que se quieran evaluar, de tal manera que en todos los casos sean obtenidos resultados confiables con los mismos métodos de evaluación.

Los resultados que obtiene el auditor que modifica los medios utilizados para obtener pruebas y documentos que avalen una revisión, no son éticos, ni profesionales, ni válidos, ni mucho menos confiables; tampoco es válido alterar los parámetros de evaluación entre una revisión y otra. Lo mismo sucede con los criterios erróneos de valoración y análisis con los que se emiten los resultados finales de una auditoría.

No modificar, ocultar o destruir evidencias en la evaluación

Los resultados que obtiene el auditor forman evidencias palpables sobre las cuales éste se apoya para emitir su dictamen; por esa razón, tales evidencias deben ser reales, jamás pueden ser inventadas, modificadas, destruidas, ocultadas o alteradas, aunque sirvan para testimoniar defectos o para realzar virtudes de los auditados.

Es una obligación ineludible del auditor respetar y salvaguardar esa información. En algunos casos, el incumplimiento de estos conceptos ocasiona delitos sancionables de carácter laboral e inclusive legal.

Ser discreto, confiable y profesional con la información y los resultados de la evaluación

En el cotidiano desempeño de sus actividades, el auditor obtiene información privilegiada utilizando métodos, procedimientos y técnicas de revisión; dicha información le

ayuda a valorar sus resultados, y únicamente le pertenece a la empresa auditada. Por esta razón, es su obligación profesional, personal y moral respetar la confidencialidad de dicha información y jamás difundirla, así como tampoco difundir los resultados obtenidos de la auditoría. Tampoco puede utilizarla para su provecho, ni el de terceros. En algunos casos, difundir información confidencial conlleva sanciones de carácter laboral y legal.

Una de las principales exigencias del auditor, es que debe ser discreto en todos los sentidos y siempre debe mantener la confianza que se le otorga como profesional de esta actividad, ya que cuando una empresa le proporciona información y documentación, está confiando en su discreción.

Actuar con equidad, imparcialidad, razonabilidad y profesionalismo

La **equidad** *es una virtud que trata de igualar la justicia, ponderación y emisión de juicios*; la **imparcialidad** *es el tratar de evitar la preferencia injusta sobre algo* y la **razonabilidad** *es la capacidad del individuo para discurrir y emitir un juicio*; en el caso del auditor, cobran suma importancia estas virtudes, debido a que, por su actividad, está comprometido a actuar de manera **ecuánime** *(igualdad de ánimo),* **imparcial** *(sin cargo hacia algún lado)* y **razonada** *(fundada en el razonamiento)*.

El auditor no puede realizar una revisión si carece de alguna de estas virtudes, ya que en la aplicación correcta de cada una de ellas es en donde se fundamenta su actuación profesional. Además, al permitirle revisar las actividades de una empresa, ésta confía en que su actuación profesional estará avalada por estos aspectos.

Emitir dictámenes profesionales, independientes y razonables

Debido a que la consecuencia final de una auditoría es la emisión del dictamen de ésta, para el caso de este profesional, estos criterios y obligaciones adquieren una importancia mayúscula, ya que su emisión es la opinión fundamentada, lo más objetivamente posible, en los resultados obtenidos durante la evaluación del cumplimiento de las actividades, funciones y operaciones del área auditada.

Por esa razón, se espera que el auditor emita un dictamen profesional sobre los aspectos revisados, el cual deberá ser consecuencia de un juicio razonado, independiente y libre de influencias, y deberá ser hecho con los métodos, técnicas y herramientas adecuadas.

3.3.3 Criterios y responsabilidades del auditor en el aspecto estrictamente laboral

Dentro de un plano netamente laboral, el auditor también debe cumplir con ciertos criterios y obligaciones que regulan su actuación como profesional de esta materia, acatándolos de acuerdo con su nivel de participación en la auditoría, con su rango de autoridad y con la responsabilidad que adquiere al ser contratado por una institución.

Al igual que en los casos anteriores, usted tiene la absoluta libertad de aceptar, modificar o refutar las sugerencias de criterios y obligaciones que presentamos a continuación, siempre y cuando en la definición de éstas busque regular el aspecto laboral de los auditores.

Cumplir con los planes, programas, contratos y presupuestos acordados

Sin importar que el auditor sea empleado de la empresa auditada o que sea independiente, es su obligación cumplir y respetar los planes, presupuestos y programas de trabajo que le sean asignados para realizar su labor.

Es su obligación saber respetar y hacer cumplir las indicaciones recibidas como subordinado, o las concertadas en caso de ser un auditor independiente.

Aplicar los métodos, técnicas y procedimientos de evaluación debidamente avalados

Como profesional de la auditoría, ya sea subordinado o independiente, el auditor debe saber aplicar una serie de métodos, procedimientos, herramientas, técnicas y guías de evaluación que le permitirán obtener resultados acertados en cualquier revisión que realice, siempre y cuando estas herramientas hayan sido previamente diseñadas, ya que ello le permitirá realizar su trabajo con eficiencia y eficacia. Además, contar con el diseño previo de tales herramientas y utilizarlas correctamente, aunado a sus conocimientos y experiencia en otras auditorías, le ayudará a obtener los mejores resultados en la evaluación.

También diremos que es obligación del auditor utilizar estas herramientas en la realización de una auditoría.

Revisar y profundizar sobre los puntos relevantes de las áreas que serán auditadas

De acuerdo con los planes y programas de auditoría, el auditor debe hacer una profunda revisión de todos los aspectos que considere relevantes en las áreas y actividades que vaya a evaluar, ya sea porque ha elegido previamente algunos puntos específicos para analizarlos, o simple y sencillamente porque, como resultado de alguna evaluación preliminar, necesita verificar con más detalle algunos de los aspectos importantes de dichas áreas.

Es necesario reiterar que *no es elección del auditor profundizar en los aspectos relevantes, es su obligación*; también es su obligación revisar aquellos que supuestamente no son importantes.

Elaborar las evaluaciones, dictámenes e informes conforme a las normas y lineamientos que regulan el desarrollo de las auditorías

Ya hemos destacado, en los aspectos *ético-moral y profesional-personal*, la importancia que tiene que el auditor cumpla con los criterios y obligaciones establecidos en

cuanto a la forma de realizar su evaluación y la manera de emitir su dictamen, destacando que su emisión esta regulada por leyes, asociaciones y por el propio auditor. Entonces, podemos decir que en los criterios y responsabilidades en el aspecto laboral del auditor debe ocurrir lo mismo, ya que también es su obligación profesional, laboral y ética apegarse a las normas y lineamientos que regulen el desarrollo de una auditoría. Esto, a la vez que es una obligación, es una garantía para el auditado, en el sentido de que el auditor siempre utilizará los mismos criterios en su evaluación y emisión de informes.

Esto es lo que da el soporte necesario para confiar en que el trabajo del auditor se desarrolla eficientemente.

Acatar las normas disciplinarias y de conducta de la empresa de auditoría externa, así como las de la empresa auditada

Ya se mencionó en un inciso anterior que los criterios, normas, condiciones, obligaciones y reglamentos establecidos dentro la empresa auditada tienen que ser estrictamente respetados, tanto por el auditor que realiza la auditoría como por cada uno de sus colaboradores y por el personal que es auditado, ya que éstas son las normas de conducta que regularán invariablemente las actividades, funciones y obligaciones entre este profesional y la institución, no sólo en el aspecto laboral, sino también en el disciplinario.

Un auditor nunca debe romper las normas de conducta y medidas disciplinarias establecidas en la institución auditada; siempre deberá acatarlas.

Capacitar y adiestrar al personal subalterno

A la vez que es una obligación laboral, también es conveniente capacitar constantemente a los auditores, tanto para provecho del auditor como para beneficio de la empresa que lo contrata; es decir, es una exigencia profesional y moral proporcionar la capacitación necesaria a los auditores, a fin de que éstos se desempeñen óptimamente en su trabajo. Entre más preparado y profesional sea el personal que realiza una auditoría, más eficientes y confiables serán los resultados de las evaluaciones.

Además, con la capacitación de los auditores se contribuye a la mayor eficiencia y eficacia en la realización de este tipo de trabajos, ya que esto no sólo ayuda a solventar la responsabilidad patronal ante los trabajadores, sino que al mismo patrón le permite tener una mayor competitividad en el ejercicio de esta profesión, lo cual es muy provechoso ya que puede contar con personal altamente capacitado para cumplir con las actividades tan especializadas que demanda esta profesión. Igual o mayor beneficio obtiene quien actúa como jefe, ya que así será más descansada la conducción del trabajo, debido a que puede contar con auditores capacitados. Otra razón para capacitar a los auditores es que esto beneficia profesionalmente a las empresas auditadas, ya que entre más capacitado esté el auditor, la revisión que realice será más profesional, más profunda y con mayor competencia, lo cual es una garantía de calidad.

3.3.4 Criterios y responsabilidades del auditor en el aspecto de elementos de juicio

Juicio *es la facultad de analizar y comprender las cosas para compararlas entre sí o mediante algún otro parámetro válido y, como resultado de ello, emitir una opinión*. Para el caso de la auditoría esto es de suma importancia, ya que el encargo fundamental de un auditor es **emitir un juicio**, en este caso **dictamen**, sobre los aspectos que evalúa. Por esa razón, es importante identificar los criterios y obligaciones que normarán el desempeño de este profesional para estar en condiciones de emitir un juicio, opinión y/o dictamen.

Verificar la autenticidad de hechos, fenómenos y evidencias encontradas

Es requisito indispensable que el auditor evalúe concienzudamente los hechos, fenómenos y/o evidencias que haya encontrado durante su revisión, con el propósito de emitir un dictamen válido, independiente y confiable sólo después de haber hecho una verdadera comprobación de las pruebas encontradas, verificando siempre las evidencias y hechos obtenidos hasta agotar todos los posibles aspectos que repercutan en el fenómeno en estudio.

Sería poco ético por parte del auditor, a la vez que falto de profesionalismo e inmoral, apoyarse en datos falsos o de dudosa veracidad para emitir un dictamen, opinión o juicio, pero sería menos ético emitirlo sin tener la suficiente evidencia, tanto en sentido positivo como en negativo.

Apegarse a las normas y lineamientos básicos de auditoría emitidos por asociaciones y colegios de profesionales,así como a los de la propia empresa que se esté auditando

Para que los resultados de una auditoría sean confiables, tienen que existir ciertos estándares, métodos y técnicas de aplicación uniforme, mismos que son normados por las asociaciones y colegios de profesionales e incluso por las mismas empresas que se dedican a la auditoría, con el único propósito de que se apliquen de manera igual en el desarrollo de cualquier auditoría; lo mismo ocurre con los procedimientos y lineamientos que se utilizan para la ejecución de una evaluación.

Por esta razón, las asociaciones de profesionales de la auditoría, previo consenso entre sus asociados, emiten periódicamente las normas, criterios, obligaciones y lineamientos de aplicación obligatoria que regulan y fundamentan la actuación del auditor. Con esto, dichas asociaciones buscan que los juicios que emitan sus asociados sean confiables, además de que se sigan los mismos parámetros de evaluación. Claro está, sin coartar la libertad de acción del auditor ni intervenir en su independencia profesional ni personal.

Aplicar de manera uniforme los métodos, técnicas, procedimientos, herramientas y criterios de evaluación

Al igual que en el punto anterior, para emitir un buen juicio sobre lo auditado, es necesario que el auditor verifique las evidencias encontradas, esto sólo se puede garan-

tizar a través de una aplicación uniforme de los métodos, técnicas, procedimientos y criterios de evaluación, los cuales tienen que ser usados de la misma manera en todas las actividades, resultados y operaciones que se evalúen en una auditoría.

Es repetitivo, pero no está de más mencionar que utilizar las mismas herramientas de evaluación en todos los aspectos que comprende la auditoría es resguardo de un buen análisis de los hechos, fenómenos y evidencias, con lo cual se puede garantizar la veracidad y confiabilidad en la evaluación, así como en la emisión del dictamen sobre los resultados obtenidos.

Evaluar en forma independiente, libre de influencias, presiones y prejuicios

El trabajo del auditor sólo es válido y confiable si emite un dictamen confiable y veraz, el cual sea resultado de una evaluación profesional, libre de cualquier influencia y presión, tanto de carácter interno *(de la empresa, área o personal auditado)* como externo *(de autoridades, terceros o de sus jefes)*. Es decir, a la hora de emitir un dictamen, su juicio debe ser absolutamente independiente.

Se mencionó en los incisos anteriores y se reitera en este punto que el objetivo final del auditor es emitir un juicio razonado, apoyado en las evidencias que encontró en su revisión y en la verificación de todos los aspectos que intervinieron en la producción de su dictamen. Sin embargo, dicho juicio también debe estar libre de cualquier tipo de influencia para no minimizar las deficiencias localizadas.

3.3.5 Criterios y responsabilidades del auditor en su respuesta ante las autoridades, leyes, normas y reglamentos

A lo largo de este capítulo se ha comentado muchas veces que el producto terminal de una auditoría es la emisión de un dictamen, en el cual se presenta la opinión fundamentada de un profesional respecto a:

Los resultados que obtuvo en una revisión que realizó durante cierto periodo

La observancia y realización de las actividades de una institución

El adecuado cumplimiento de las operaciones que se desarrollan en las áreas de una institución y el correcto cumplimiento de las funciones de sus funcionarios y empleados

Sin embargo, la responsabilidad del auditor va más allá de emitir un dictamen, ya que el resultado de éste también puede llegar a otros interesados, aparte de la empresa, quienes pueden utilizarlo para efectuar acciones de carácter laboral e incluso acciones de tipo legal y/o penal.

Por esta razón, el dictamen del auditor debe estar bien fundamentado, apoyado en evidencias y plasmado con la mayor veracidad, debe contener la valoración de todo lo contemplando durante la revisión y debe estar totalmente apoyado en técnicas, métodos y procedimientos reconocidos para hacer una auditoría. Esto es lo que le dará vigencia y confiabilidad al trabajo del auditor.

Pero además de lo anterior, la actuación de este profesional puede tener resultados marginales; esto pasaría en caso de que encontrara delitos, faltas e infracciones en perjuicio de la empresa y sus empleados, de las leyes, las normas y los reglamentos vigentes, los cuales tendría que dar a conocer debidamente fundamentados. Igual pudiera darse el caso de que los resultados de su actuación como auditor tuvieran que ser verificados, rectificados o ratificados como parte de alguna acción de carácter legal.

También puede darse el caso de que el propio auditor incurra en un trabajo no honesto, poco profesional y sin la integridad que se requiere en este tipo de trabajos; en ese caso, el auditor sería responsable de cometer esos delitos y su actuación profesional y laboral tendría que ser evaluada.

Por esas razones, cobran vigencia los criterios y obligaciones que a continuación se analizan.

CIVILES por delitos e infracciones debidos a negligencia, impericia, abuso de confianza o dolo, tanto en los resultados encontrados como en la realización de la auditoría misma

En el dictamen de auditoría, el auditor puede establecer las posibles infracciones, delitos y transgresiones que llegara a detectar por parte de ejecutivos o empleados en perjuicio de los bienes de la empresa o de terceros. Por esta razón, las observaciones que reporte siempre deben estar perfectamente asentadas y formalmente comprobadas, ya que puede darse el caso de que tenga que presentar dichas observaciones como evidencias de los hechos reportados. Incluso se pueden aprovechar los resultados de este documento para corroborar la comisión y existencia de algún ilícito.

Por otro lado, y derivado del resultado de la emisión del informe, también se pueden fundamentar acusaciones en contra del auditor que realizó la auditoría, ya sean por supuestas o verdaderas acciones de negligencia profesional, impericia en el desempeño de las actividades encomendadas, abuso de confianza, actuación con dolo o cualquier otra infracción que el auditor cometa en detrimento de la institución a la que está auditando. Entonces, si se llegara a dar alguno de estos casos, este pseudoprofesional tendría que responder ante la empresa auditada y ante las autoridades correspondientes, por lo que se podrían establecer multas e infracciones de tipo laboral, civil e incluso de carácter legal.

FISCALES por los delitos e infracciones de carácter fiscal que se descubran o realicen

Los auditores financieros, contables y fiscales, principalmente, deben cumplir con ciertos requisitos de carácter legal y laboral para ejercer su profesión, debido a que, bajo el amparo de sus asociaciones o por mandato de las propias autoridades hacendarias, se les confiere la facultad de emitir un dictamen formal sobre los resultados financieros de una institución, el cual es válido y plenamente reconocido por los interesados y

las autoridades correspondientes. Con dicho dictamen se avala la situación financiera de la empresa auditada y la opinión del auditor es considerada como válida y formal, siempre que cumpla con los requisitos que establece el IMCPAC.

De ahí nace la importancia que tiene su actuación como auditor, debido a que en su dictamen puede plasmar la correcta situación financiera de la empresa o, en su caso, determinar la infracción en los aspectos fiscales de la institución. Además, ante las autoridades y terceros interesados, el juicio que el auditor emita como resultado de su auditoría es válido.

Es evidente que, como ya hemos señalado, se pueden fincar responsabilidades fiscales, civiles, laborales y penales como resultado del dictamen financiero del auditor. Por otro lado, el propio auditor puede llegar a cometer delitos de carácter fiscal y de otro tipo, derivados de su actuación como auditor. He ahí la importancia de cumplir con lo señalado por estos criterios y obligaciones.

PENALES por delitos de fraude, robo, abuso de confianza, encubrimiento, revelación del secreto y responsabilidad profesionales por parte del auditado y del propio auditor

La afectación a los bienes patrimoniales de una empresa puede ser alguno de los resultados de un dictamen de auditoría, debido a que con la aplicación de exámenes y métodos de revisión a los resultados, las operaciones y actividades de dicha empresa, se pueden evidenciar deficiencias en el manejo de los bienes institucionales, lo cual sería delito penal en caso de que sean voluntarias, o negligencias en caso de ser involuntarias; este caso puede tener como consecuencia responsabilidad civil, pero también puede convertirse en penal.

Por eso el dictamen del auditor es tan importante, ya que con él se pueden evidenciar delitos de carácter penal, tales como fraudes a los bienes de la institución, robos en todos los sentidos, abuso de confianza, encubrimiento de acciones fraudulentas, revelación de secretos profesionales y otros delitos de similar afectación patrimonial, los cuales son cometidos tanto por el personal auditado como por el propio auditor al no reportarlos.

JUDICIALES por los resultados de la auditoría y por la actuación del auditor

Como consecuencia del juicio emitido por el auditor, también se pueden descubrir ilícitos de carácter judicial, delitos en que pueden incurrir los ejecutivos y empleados de la institución auditada, así como delitos de terceras personas involucradas con la empresa. Tales delitos pueden plasmarse en el dictamen, siempre y cuando el propio auditor los fundamente y corrobore de la manera adecuada.

Parece repetitivo señalar que el resultado del informe de auditoría puede ser suficiente evidencia para comprobar delitos de carácter judicial o, cuando menos, sirven de apoyo para establecer suposiciones fundamentadas de infracciones e ilícitos de es-

te tipo, siempre y cuando estén soportados por las técnicas, métodos y procedimientos debidamente fundamentados por el auditor.

LABORALES Por las faltas detectadas al reglamento interno de la institución, así como a la Ley Federal del Trabajo.

Además de que las situaciones determinadas por el auditor pudieran ser consideradas como delitos de tipo penal, fiscal, civil o judicial, según los resultados de su evaluación a las actividades y operaciones que se realizan en la empresa, también se pueden determinar otro tipo de deficiencias, no tan graves, pero que pueden provocar algunas infracciones que afectan a la Ley Federal del Trabajo y sus reglamentos, a la Secretaría del Trabajo, a los trabajadores y a la propia institución que se audita. Por ética profesional, el auditor debe asentar tales delitos en su informe, aunque aparentemente esas infracciones sean consideradas como aspectos internos de la empresa que está auditando; no olvidemos que, de alguna manera, las desviaciones reportadas de este tipo pueden ser producto de algún incumplimiento de ciertas obligaciones hacia los trabajadores.

3.3.6 Criterios y responsabilidades del auditor en la presentación de resultados a terceros

Igual que se mencionó en el caso anterior, el producto fundamental de una auditoría es la emisión de un informe, en el cual se presenta la opinión fundamentada del auditor respecto a la revisión que ha realizado a los resultados obtenidos en un periodo, al desarrollo de las actividades y operaciones de las áreas de una institución y al cumplimiento de las funciones y tareas de sus funcionarios y empleados, entre otras muchas cosas que se esperan del dictamen.

Aunado a lo anterior, es necesario establecer que una auditoría no se puede dar al azar ni generarse por sí sola, sino que tiene un origen, ya sea que la empresa demande una revisión de sus propias actividades y resultados, por requerimiento de las autoridades correspondientes, como seguimiento a un programa periódico de evaluación o por encargo de terceras personas, sean dueños, socios, proveedores u otras personas que tengan alguna injerencia en la gestión administrativa de la empresa.

Sin embargo, la responsabilidad del auditor es emitir un dictamen para los responsables de la administración de la empresa, a fin de que estos funcionarios puedan utilizar el resultado de su trabajo. Dicho dictamen también puede servir para otros interesados, ajenos a la compañía, sólo si tienen alguna injerencia en la gestión administrativa de la institución y están autorizados para ver tales resultados. Por esa razón, el dictamen del auditor debe estar bien fundamentado, apoyado en evidencias y debe ser veraz en todo lo contemplado durante la revisión, ya que también servirá para las siguientes personas.

Accionistas e inversionistas de la empresa auditada

Los resultados de la auditoría son requeridos y turnados a los accionistas, dueños e inversionistas de la empresa para su análisis, quienes los utilizan para determinar el cum-

plimiento de los objetivos y actividades de su empresa, así como para evaluar los resultados que se han alcanzado durante un periodo y para establecer las acciones necesarias respecto a la marcha de la empresa, de sus funcionarios y empleados. El resultado de esta evaluación se puede presentar en forma parcial acerca de una actividad o acción específica, o también puede ser presentado como resultado de una evaluación global.

Funcionarios, empleados y trabajadores de la empresa auditada

Cuando el dictamen se hace llegar a los funcionarios, los empleados y trabajadores de la empresa, en la parte que les corresponde de acuerdo con sus áreas de trabajo y con las actividades que desempeñan, es para que cada uno conozca el resultado de una evaluación objetiva de su actuación real en el cumplimiento de sus obligaciones. En estos casos, los informes se les proporcionarán de acuerdo con su nivel de participación en las actividades de la corporación y con el grado de confidencialidad establecido en la institución.

Acreedores y proveedores de la empresa auditada

Por lo general, la realización del informe de auditoría para los proveedores y acreedores de la empresa se da bajo condiciones especiales, considerando características especiales respecto a su contenido, profundidad y alcances, y con la condicionante de que sólo se puede informar hasta donde la empresa auditada lo estime conveniente y hasta donde los accionistas lo permitan. Jamás se hará sin el consentimiento de éstos.

La empresa auditada tiene la facultad de negarse a proporcionar los resultados de una auditoría a los acreedores y proveedores, ya que sólo está obligada a turnárselos cuando existe un mandato judicial; de otra manera, por ningún motivo ningún acreedor u otra institución podrá obligar a la empresa a que le permita revisar los resultados de su auditoría, mucho menos a sancionarle con sus resultados.

Autoridades hacendarias, municipales, estatales y federales

El informe de auditoría es requerido y turnado a las autoridades que, dentro de su ámbito territorial, regulan la actuación fiscal de las empresas. Por lo general, estas auditorías son de carácter impositivo y se orientan a aspectos concretos definidos por las leyes, normas y reglamentos de la administración pública. En algunos casos, dichos aspectos tienen que ver con las instituciones de salud y del trabajo, pero la revisión sólo se realiza bajo requerimiento de carácter legal.

En este caso no es elección de las empresas permitir la auditoría, sino que están obligadas por la ley y forzosamente deberán permitir que se lleve a cabo la evaluación de sus registros contables, de la emisión de sus resultados financieros y de la correcta información y pago de los impuestos correspondientes y, si es el caso, de sus sistemas computacionales y bases de datos. También están obligadas a permitir que el auditor externo informe a esas autoridades sobre el resultado de la auditoría.

3.4 Normas profesionales del auditor

En los puntos anteriores ya fueron destacados los *criterios y responsabilidades* que regulan la actuación profesional de los auditores, estableciendo en cada caso aquellos aspectos sobresalientes de su actuación, los cuales se pueden considerar de aplicación general y de acatamiento obligatorio para estos profesionales. Sin embargo, a continuación vamos a estudiar normas que son obligatorias para un auditor, las cuales en muchos casos sí están reguladas y su incumplimiento conlleva una sanción. Para nuestro caso, dichas normas y lineamientos serán analizados desde un plano exclusivamente de aplicación profesional.

Cabe señalar que estas *normas profesionales del auditor* se apoyan en la experiencia profesional de este autor en el ramo de auditoría, así como en lo determinado por el ***Instituto Mexicano de Contadores Públicos, A.C.*** (IMCPAC) y por el ***Colegio Nacional de Licenciados en Administración, A.C.*** (CONLA), además de otros autores indicados en el capítulo II de este libro. Este autor complementa este conocimiento con lo aprendido en años de impartir esta materia en aulas universitarias, lo cual ha permitido establecer las normas mínimas que pueden regular la actuación de este tipo de profesionales; estas normas las podemos agrupar de la manera siguiente:

- Normas permanentes de carácter profesional
- Normas de carácter social
- Normas de comportamiento ético-moral

Tenemos que aclarar que en algunos casos, amigo lector, le parecerán similares y reiterativos algunos de los aspectos que a continuación presentamos; sin embargo, aunque en muchos casos sí son muy similares en cuanto a su contenido y tratamiento, lo que pretendemos es dar a conocer y reafirmar el entendimiento de los elementos indispensables que tomaremos en cuenta para regular las normas de actuación profesional de un auditor, en cualquier rama en donde se lleve a cabo una auditoría.

También conviene mencionar que algunos de estos lineamientos no están escritos ni pueden ser sancionados, pero de alguna manera existen, se conocen en el ambiente laboral y deben ser acatados por los profesionales de la auditoría; pero también tenemos aquellos que están normados y regulados por organismos que sí contemplan sanciones en caso de incumplimiento. Ambos aspectos se analizarán a continuación.

3.4.1 Normas permanentes de carácter profesional

Las normas permanentes de carácter profesional son aquellas que debe cumplir invariablemente el profesional dedicado a la actividad de la auditoría de sistemas computacionales; el auditor no debe admitir bajo ninguna circunstancia variación alguna respecto a la aplicación y cumplimiento de dichas normas. Esto se debe a que es obligación profesional *(deber ético, moral y profesional)* del propio auditor y del personal

que colabora con él, hacer una cabal observancia de dichas normas a fin de mantener su prestigio y credibilidad en las empresas donde realice su evaluación. Entre los casos más relevantes encontramos los siguientes:

Emitir una opinión responsable y profesional respaldada en evidencias comprobadas

Una auditoría solamente es válida cuando está debidamente fundamentada por técnicas, métodos y procedimientos de carácter profesional que han sido previamente aprobados y comprobados; estos métodos son un soporte para que el auditor, apoyado en su experiencia y conocimientos de la materia, emita una opinión confiable y de tipo profesional.

La opinión fundamentada del auditor le hace confiable en los juicios que emite.

Mantener una disciplina profesional

Al igual que en cualquier profesión e incluso en algunas de las actividades laborales, sociales y cotidianas de la vida, un profesional de la auditoría también debe mantener una actuación permanentemente profesional por encima de cualquier cosa, tanto en el aspecto laboral como el personal, lo cual sólo se logra con constancia, voluntad y una férrea disciplina.

Parecería jactancioso destacar que el auditor realiza una actividad preponderante para las empresas que audita, pero los funcionarios y empleados de esas instituciones esperan que su actuación, como experto, siempre sea profesional. También se espera lo mismo de su actuación cotidiana; como persona, se presume que siempre actuará con disciplina.

Para ser buen auditor, no sólo hay que trabajar como tal, sino también hay que parecerlo.

Guardar el secreto profesional

Debido a que el auditor está en contacto con información confidencial de la empresa que audita, es su obligación no sólo profesional sino también ética y moral, que en todos los casos mantenga el secreto profesional, tanto de la información que le es confiada como de los resultados de su evaluación. Por ningún motivo debe dar a conocer la información que le fue confiada.

El auditor es como un confesor, no de almas sino de empresas.

Tener independencia mental

También se debe considerar que para ser auditor no sólo hay que trabajar en ello, sino tener una aptitud, competencia y disposición profesional de tipo muy especial, caracterizada por una actitud mental independiente que siempre debe estar libre de cualquier influencia. Además, el auditor debe tener los suficientes conocimientos, habilidades y

experiencia para saber evitar las influencia de cualquier género, así como las amenazas y los aspectos sentimentales que encontrará en la realización de su trabajo.

Para ser auditor hay que ser independiente de pensamiento, palabra y actuación.

Contar con responsabilidad profesional

Si se considera que *no es lo mismo ser un profesional que trabaja en la auditoría que ser un profesional de la auditoría*, es evidente que no sólo hay que laborar como auditor para sobrevivir, sino que hay que actuar y pensar como verdadero profesional de la auditoría; lo anterior se refleja en la forma de aceptar la responsabilidad que se tiene para cumplir con las actividades de una auditoría; ésta no sólo es una norma y obligación profesional, sino que es un requisito ético, moral y personal para actuar como auditor.

No sólo hay que laborar como auditor, también hay que aceptar la responsabilidad que esto implica.

Capacitación y adiestramiento permanentes

Como en toda actividad profesional, el auditor también requiere de una constante capacitación profesional, laboral y técnica, para que adquiera nuevos conocimientos de métodos, procedimientos y herramientas de evaluación que le ayuden a desempeñar mejor su trabajo. La capacitación puede ser de carácter formal o informal, de tipo académico, laboral o personal. Lo importante es que estos profesionales se capaciten constantemente para realizar mejor su actividad profesional.

Para el auditor, la capacitación es la herramienta fundamental para el buen desempeño de su actividad profesional.

Hacer una planeación de la auditoría y de los programas de evaluación

Para realizar un buen trabajo de auditoría, es necesario que para cualquier tipo de auditoría que practique, el auditor se apoye en una previa planeación de todas las actividades, herramientas y recursos que deba utilizar, incluyendo los planes, programas y presupuestos, no sólo de los recursos a utilizar, sino también de las técnicas, métodos y procedimientos de auditoría. Es evidente que esta actividad es producto de normas y obligaciones de tipo profesional; permanentes, por cierto.

La planeación de la auditoría es la herramienta indispensable para un buen desarrollo y cumplimiento profesional de la misma.

Hacer la presentación del dictamen por escrito, así como la aclaración de diferencias

El informe que presente el auditor debe ser lo más confiable posible, con lenguaje claro, bien estructurado y debe contener todos los aspectos fundamentales que apoyan su opinión como profesional, evitando en todos los casos la subjetividad en lo evalua-

do; la mejor forma de lograrlo es presentar este informe por escrito, a fin de no dejar dudas sobre lo que se está informando. Además, no basta con presentarlo por escrito, también es un requisito normado y una obligación profesional que el contenido del informe esté comentado con los involucrados en la revisión y, si es el caso, deben estar aclaradas las posibles divergencias y dudas que surjan entre el auditor y el auditado. Esto le dará al auditor su carácter profesional.

El informe de auditoría es un documento legal que no debe ser ocultado a los auditados ni ser presentado a sus espaldas, sino que les debe ser presentado con pleno conocimiento de su contenido.

3.4.2 Normas de carácter social

El auditor, como todo profesional y cualquier ciudadano, vive en una sociedad en la cual desempeña su actividad profesional y a la cual sirve con su trabajo. Dicha sociedad se rige por una serie de normas y obligaciones, muchas de ellas no escritas, pero sí aceptadas por los integrantes de esa comunidad.

Para entenderlo mejor, nos conviene identificar los conceptos que fundamentan estas normas.

Social

"Perteneciente o relativo a la sociedad humana, o las relaciones entre las clases sociales [...]. Se dice del individuo perteneciente a ella."[41]

Sociedad

"Del latín **societas.** *Estado de los hombres o de los animales que viven sometidos a las leyes comunes [...]. Reunión de varias personas sometidas a una misma regla [...]. Asociación de varias personas con el fin de proporcionarles alguna utilidad [...]."*[42]

Estas definiciones son las que regulan la actuación del auditor dentro de su ambiente social y laboral.

El análisis de estas normas se realizará de la manera siguiente.

Acatar las normas y obligaciones de carácter social

Con base en las definiciones anteriores, al convivir con un grupo de personas dentro de un núcleo de la sociedad, el auditor debe regir su conducta con las normas y lineamientos que regulan la actuación de cualquier profesional. Estas normas y obligaciones sociales, que por lo general no están establecidas por escrito, son las que determinan la actuación de este tipo de profesionales y en general de toda la sociedad.

Respetar a las autoridades, leyes, normas y reglamentos

Dentro de las enseñanzas de carácter social que desde pequeños se nos inculcan en la familia y en la sociedad, se encuentra el aprendizaje del civismo, por medio del cual

se nos enseña a respetar y acatar, entre otras cosas, lo determinado por la normas, leyes y reglamentos que regulan el comportamiento de las personas que cohabitan dentro de un conglomerado social; también se nos inculca el respeto a las autoridades y disposiciones sociales.

Es requisito de carácter social que el auditor sepa respetar y hacer cumplir las disposiciones y normas emanadas de las autoridades que regulan su actividad profesional, tanto en su actuación con las empresas que audita como con las personas que trata en la realización de una auditoría.

Evitar y prevenir sobornos, componendas y dádivas

Es requisito indispensable, sin admitir ninguna variación al respecto, que el auditor prevenga y evite cualquier tipo de soborno, componenda o dádiva que pudieran resultar de su actividad profesional; estos términos se definen como sigue.

Sobornar

"Corromper a alguien con dinero, regalos u otro medio para conseguir algo de él."[43]

"Del latín **Sobornare***. Excitar, incitar, corromper. Corromper a uno con dádivas para conseguir de él una cosa."*[44]

Componenda

"[...] Chanchullo, solución indigna."[45]

Ser leal con los auditados

Un requisito indispensable para el auditor, también de comportamiento social, ético, profesional y moral, es que debe ser leal con las empresas que audita y con el personal que labora dentro de ellas. No es válido ni profesional ser desleal con quienes se audita. Además, cumplir con esta obligación, en mucho le ayuda a fundamentar sus relaciones con las empresas, con sus colegas y con la sociedad en general.

Contar con una opinión profesional y defenderla

Al emitir el informe de una auditoría y plasmar su opinión en un dictamen, el auditor demuestra a la sociedad que tiene una opinión personal, la cual fundamenta en la aplicación de sus técnicas, métodos y procedimientos de auditoría, misma que defiende por medio de su opinión profesional, la cual está cimentada por las evidencias que obtiene al realizar su trabajo; eso es lo que espera la colectividad de este profesional.

Por esta razón, la comunidad le confiere al auditor una gran calidad moral, social y profesional, ya que da por hecho que su actuación está apegada a una estricta ética profesional y personal, la cual demuestra con la opinión que emite y defiende.

Emitir un dictamen con firma profesional

La sociedad, las autoridades y los responsables de las empresas auditadas reclaman que el informe que emite el auditor esté respaldado por una firma profesional, ya sea la de una empresa que avale su actuación o la del propio auditor. Este profesional debe estar avalado y certificado por las autoridades y asociaciones de profesionales del ramo para ejercer esta actividad.

Contar con apoyo didáctico y normativo vigente

Para ejercer la profesión de auditor, también es requisito contar con el apoyo didáctico y normativo que esté vigente en esta actividad, ya que la sociedad, las empresas y sus ejecutivos y empleados reclaman que al realizar esta actividad, el auditor cuente con la capacitación y conocimientos más adelantados y vigentes de su profesión.

3.4.3 Normas de comportamiento ético-moral

Aunque ya fueron señaladas como las obligaciones y responsabilidades de carácter ético y moral que debe cumplir el auditor, a continuación vamos a analizar, desde la óptica del aspecto profesional, la normas de conducta que como profesional debe acatar el auditor, dentro de un estricto sentido ético y moral; dichas normas son las siguientes.

Ser incorruptible e insobornable

Ya señalamos en las normas de carácter social que es requisito indispensable, sin admitir ninguna variación al respecto, que el auditor sea insobornable e incorruptible y que no haya ninguna duda respecto a su actuación en la evaluación que está realizando. Esta cualidad moral, más que norma y obligación, es la que da la confianza en la actuación de un profesional de la auditoría.

Alterar en algo el informe de la auditoría para minimizar, no informar o modificar lo encontrado en una evaluación no es una actitud ética del auditor, mucho menos moral ni profesional. Si esta actitud se deriva de sobornos, corruptelas y componendas para alterar su opinión, este pseudoauditor carece de calidad profesional. Igual si obedece a otro tipo de intereses ajenos a los fines de la auditoría.

Ser imparcial en los juicios que emite como auditor

Para ser un buen profesional en esta rama, entre otras muchas características, se debe ser imparcial, esto con el propósito de poder emitir un juicio acertado y ecuánime respecto a lo que se está evaluando. El cumplimiento de esta cualidad o norma ético-moral es lo que le da validez y vigencia a la profesión de auditor, debido a que, al emitir un dictamen, éste se hace libre de cualquier presión e influencia y sin ningún sesgo ni parcialidad; el auditor sólo debe informar de lo que realmente observó. Además, de-

be fundamentar su opinión en las evidencias y pruebas que obtuvo con los métodos, técnicas y herramientas de auditoría que utilizó. Esto no sólo es una norma ético-moral, sino profesional y laboral.

Contar con un juicio sereno, ético y moral

También fue señalado en los elementos de juicio que el objetivo final de una evaluación es emitir un dictamen sobre los aspectos que se están evaluando a la luz de las técnicas que utilice el auditor.

Por esta razón, es importante identificar los elementos señalados en ese punto y los criterios y obligaciones de carácter ético y moral que adquiere este profesional al emitir un dictamen, mismo que fundamenta en un juicio sereno, el cual apoya con las evidencias de que dispone y con las pruebas obtenidas con sus herramientas de evaluación..

Acatar y hacer cumplir las normas morales y éticas

Parece reiterativo decir que el auditor debe acatar y hacer cumplir las normas ético-morales que regulan su actuación como profesional, lo cual se aplica invariablemente a su actuación tanto en el ámbito profesional, como en el ámbito personal y social.

Esto es lo que esperan de su actuación los funcionarios y empleados de las empresas que audita, sus colegas, las asociaciones a las que pertenezca y la comunidad en general. Todos esperan que su actuación como auditor se apegue invariablemente a un estricto cumplimiento de las normas morales y éticas que regulan a la sociedad.

Control interno

4

Estructura del capítulo:

Objetivos del capítulo

Estudiar los conceptos y características fundamentales del control interno en las empresas, a fin de identificar e interpretar sus aplicaciones principales en el plano administrativo y así poder satisfacer, con eficiencia y eficacia, las necesidades de evaluación, razonabilidad y oportunidad en la protección y seguridad de los bienes de una institución; también para saber cómo se desarrollan las actividades, operaciones y resultados financieros que se obtienen en las áreas de dicha institución.

Todo ello con el propósito de presentar al lector los aspectos fundamentales del control interno, con el fin de que entienda la importancia de este elemento básico de la auditoría tradicional y reflexione sobre lo fundamental de su aplicación en la auditoría de sistemas de información, así como sobre su importancia en la práctica de cada uno de los tipos de auditoría que se estudiarán.

Introducción del capítulo

El control interno nace por la necesidad de evaluar y satisfacer la ***eficiencia, eficacia*, *razonabilidad, oportunidad y confiabilidad*** en la protección, salvaguarda y seguridad de los bienes de una empresa, así como para ayudar a controlar el desarrollo de sus actividades, operaciones y resultados financieros que se espera obtener en el desempeño de las funciones y operaciones de toda la empresa.

Dicho *control interno* se adopta a partir de la clara definición de los objetivos institucionales de las empresas, con el fin de evaluar el cumplimiento adecuado de sus funciones, actividades y operaciones, para que esto les permita tener una administración eficiente. También se contempla todo lo relacionado con la estructura de organización, las funciones, los niveles de autoridad y la responsabilidad de la empresa, así como la definición de los métodos y procedimientos necesarios para el desempeño de sus actividades, y el registro de las operaciones contables y la emisión de los resultados financieros de la empresa.

Gómez Morfín cita la siguiente definición de control interno:

"Es el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para la:

- *Protección de los activos*
- *Obtención de información correcta y oportuna*
- *Promoción de la eficiencia de operación*
- *Adhesión a las políticas prescritas por la dirección."*

J. Manuel Lazcano y Enrique Rivas Z. *señalan lo siguiente:*

"Para el logro de estos objetivos, el control interno descansa en los elementos de organización, procedimientos, personal y supervisión."[1]

El propósito fundamental de la aplicación del control interno es que las empresas puedan satisfacer sus necesidades de seguridad y protección de sus activos; con su aplicación, también pueden lograr la ejecución adecuada de sus actividades y el cumplimiento de las normas y políticas que regulan las funciones de directivos y empleados. Partiendo de estas consideraciones, a continuación se analiza el control interno en forma general, y en el siguiente capítulo se analizará su aplicación específica en el área de informática.

4.1 Conceptos y definiciones de control

Para entender el funcionamiento del control interno en el área de informática, lo primero es analizar los conceptos y definiciones de control, después su ciclo de aplicación e importancia en las empresas; finalmente, la aplicación del control interno en las empresas. Una vez hecho este análisis, podremos entender cómo se aplica el control interno en el área de sistemas.

Por esta razón, iniciaremos nuestro estudio con los conceptos fundamentales.

4.1.1 Definiciones de control

El *control* es una de las fases del *proceso administrativo* y se encarga de evaluar que los resultados obtenidos durante el ejercicio se hayan cumplido de acuerdo con los planes y programas previamente determinados, a fin de retroalimentar sobre el cumplimiento adecuado de las funciones y actividades que se reportan como las desviaciones encontradas; todo ello para incrementar la eficiencia y eficacia de una institución. Las siguientes son algunas de las definiciones de control:

"Inspección, vigilancia que se ejerce sobre personas o cosas [...] Conjunto de operaciones encaminadas a comprobar el funcionamiento, productividad, etc., de algún mecanismo [...]."[2]

"Control es verificar que todo ocurra de acuerdo a las reglas establecidas y las órdenes impartidas [...]."[3]

"Dentro del concepto de sistemas, el control es definido como un medio de obtener mayor flexibilidad operativa y como un medio de evitar el planteamiento de operaciones cuando las variables sean desconocidas [...]."[4]

"El control consiste en obligar a los acontecimientos a ajustar un plan."[5]

"El control es la fase del proceso administrativo que debe mantener la actividad organizacional dentro de los límites permisibles, de acuerdo con las expectativas. El control organizacional está irremediablemente relacionado con la planeación. Los planes son el marco de referencia dentro del cual funciona el proceso de control [...] La palabra control tiene varios significados: [...] verificar, regular, comparar con un estándar, ejercer autoridad sobre (dirigir u ordenar), limitar o restringir [...] Cuando menos tres líneas relativas quedan claras de su definición: 1) limitar o restringir, 2) dirigir u ordenar, y 3) regular. [...]."[6]

4.1.2 Objetivos del control

Para comprender la importancia del control en las empresas, lo primero es entender cuáles son los objetivos que se pretenden satisfacer con su adopción, aunque éstos sean muy variados y específicos de acuerdo con el tipo de institución donde se establezcan y a las características específicas de la misma. A continuación se proponen, de manera general, los siguientes objetivos del control:

- *Se adopta para poder establecer estándares, medir su cumplimiento y evaluar el alcance real de los planes y programas, comparado con lo realmente alcanzado.*
- *Con su adopción se ayuda en la protección y salvaguarda de los bienes y activos de las empresas.*
- *Con su adopción se contribuye a la planeación y evaluación correctas del cumplimiento de las funciones, actividades y operaciones de las empresas.*
- *Ayuda permanentemente a la buena marcha de la empresa, pues retroalimenta la trayectoria de la misma.*
- *Junto a la planeación, el control es una parte indispensable en las actividades de dirección de cualquier empresa.*

4.1.3 Elementos del control

Para empezar, debemos saber cuáles son los elementos fundamentales del control, a fin de identificar la forma de utilizar el control interno en las empresas y así poder aplicar ese conocimiento al control interno en sistemas, y más concretamente a las aplicaciones específicas de auditoría de sistemas computacionales.

Para los autores **Kast** y **Rosenzweig,** en su tratado *Administración en las organizaciones*, los elementos básicos del control son más que una simple función que responde a los cambios del medio ambiente, debido a que también nos sirven para retroalimentar a lo que está cambiando; su aportación es la siguiente:

"Los elementos básicos del control:

1. *Una característica medible y controlable para la que se conocen estándares*
2. *Un medio (instrumento censor) para medir las características*

3. *Un medio para comparar los resultados reales con los estándares y evaluar las diferencias*
4. *Un medio para efectuar cambios en el sistema a fin de ajustarlos a las necesidades."*[7]

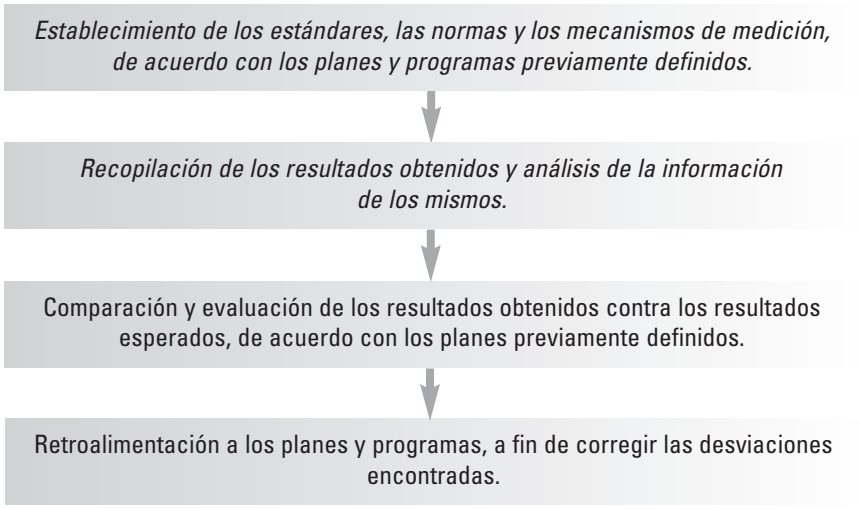
W. H. Harper, en su tratado *Contabilidad de empresas*, manifiesta que los factores fundamentales del control, los cuales también llamamos elementos de control, son los siguientes:

"Factores fundamentales del control [...]

- *El plan*
- *La comparación entre los hechos reales y el plan*
- *La acción para rectificar las divergencias*

La falta de cualquiera de estos elementos esenciales [...] no existe el control."[8]

Podríamos continuar con el análisis de dichos elementos, sin embargo nos conviene aclarar que para este libro vamos a tomar los siguientes aspectos como elementos del control:



4.1.3.1 Establecimiento de normas, estándares y mecanismos de medición, de acuerdo con los planes y programas previamente definidos

Para su adopción en las empresas, lo primero es identificar cuáles son las necesidades de medición establecidas en los planes, programas, funciones, actividades, operacio-

nes o en cualquier otra acción que se desea evaluar; el propósito es diseñar aquellas normas, estándares y mecanismos que serán utilizados en la medición de lo que se espera alcanzar. Todo ello de acuerdo con los planes y programas previamente establecidos en la empresa.

Lo anterior vendría a ser el diseño de las herramientas y de los instrumentos de auditoría, los cuales servirán para evaluar los aspectos deseados. El diseño de dichos instrumentos se analizará de manera concreta en capítulos posteriores.

4.1.3.2 Recopilación de los resultados obtenidos y análisis de la información de los mismos

Con los instrumentos de evaluación previamente diseñados, se hace la recopilación de los resultados de los planes, programas, operaciones y actividades, así como de los beneficios obtenidos (en esto ayudan las herramientas de auditoría, a recopilar la información de los resultados alcanzados).

Con la obtención de esta información se efectúa el análisis de esos resultados, ya sea en forma estadística, de análisis de variaciones, de razones financieras, de experiencia y observaciones personales, o de cualquier otro medio de análisis que permita obtener conclusiones válidas.

De hecho, esto sería la aplicación de una auditoría, el reporte de observaciones y la previa elaboración del informe de la misma.

4.1.3.3 Comparación y evaluación de los resultados obtenidos contra los resultados esperados, de acuerdo con los planes previamente definidos

El siguiente paso es realizar un concienzudo análisis de lo que realmente se alcanzó de los planes, programas, actividades, funciones, etcétera, en comparación con lo que se esperaba desarrollar de los mismos. El único propósito es valorar los alcances reales que se han obtenido; evidentemente, de acuerdo con los instrumentos de medición previamente establecidos.

Éste sería el informe de auditoría, ya que informa lo alcanzado en relación con lo esperado.

4.1.3.4 Retroalimentación a los planes y programas, a fin de corregir las desviaciones encontradas

Con este último análisis se estará en condiciones de saber si se cumplió con lo inicialmente esperado, así como de retroalimentar con los resultados, ya sea para conservar o mejorar los planes y programas con los cuales se alcanzó el objetivo, o para modificarlos y corregirlos cuando no se obtengan buenos resultados.

Como podemos observar, con los elementos del control se busca evaluar, mediante estándares y mecanismos de medición previamente establecidos, el resultado de planes y programas inicialmente determinados, a fin de retroalimentar o, en su caso, corregir las desviaciones que se lleguen a detectar; lo importante de esta función es que sirve para volver a alimentar (retroalimentar) la realización adecuada de esos planes y programas.

4.1.4 Utilidad del control

El control en las instituciones tiene una razón de ser, de acuerdo con los planes y programas de cada empresa, ya que inicialmente nos permite establecer los estándares que nos ayudarán a obtener la información necesaria para evaluar el cumplimiento adecuado de los planes y programas previamente definidos; más tarde, con la información recopilada, nos ayuda a comparar lo que se alcanzó realmente contra lo esperado; por último, esta evaluación nos sirve para retroalimentar con mejoras y correcciones los planes y programas que servirán de base para el futuro.

Con base en el análisis anterior, podemos concentrar la utilidad del control en los siguientes conceptos:

- Permite diseñar y establecer las normas, estándares y criterios de medición para poder evaluar el cumplimiento de planes y programas.
- Ayuda a evaluar el cumplimiento y desempeño de las funciones, actividades y tareas de los integrantes de una empresa, comparando lo alcanzado contra lo esperado.
- Permite medir la eficiencia y eficacia en el cumplimiento de las operaciones de una empresa, al comparar lo realmente alcanzado contra lo esperado.
- Contribuye a la detección de fallas y desviaciones, así como a la corrección de errores en el desempeño de las actividades y operaciones de una empresa.
- Ayuda a modificar los planes y programas como consecuencia de la valoración de los resultados.
- Retroalimenta la planeación y programación de las empresas.

Éstas son algunas de las muchas utilidades que puede tener el establecimiento del control en las empresas; dichas utilidades se pueden ampliar conforme a las características y necesidades de cada institución.

4.1.5 Características del control

Para que el control en las empresas sea verdaderamente efectivo, es obligatorio considerar algunas de sus características fundamentales al momento de establecerlo.

Entre algunas de esas características encontramos:

Oportuno

Esta característica es la esencia del control, debido a que es la presentación a tiempo de los resultados obtenidos con su aplicación; es importante evaluar dichos resultados en el momento que se requieran, no antes porque se desconocerían sus verdaderos alcances, ni después puesto que ya no servirían para nada.

Cuantificable

Para que verdaderamente se puedan comparar los resultados alcanzados contra los esperados, es necesario que sean medibles en unidades representativas de algún valor numérico para así poder cuantificar, porcentual o numéricamente lo que se haya alcanzado.

Calificable

Así como los valores de comparación deben ser numéricos para su cuantificación, en auditoría en sistemas computacionales, se dan casos de evaluaciones que no necesariamente deben ser de tipo numérico, ya que, en algunos casos específicos, en su lugar se pueden sustituir estas unidades de valor por conceptos de calidad o por medidas de cualidad; mismas que son de carácter subjetivo, pero pueden ser aplicados para evaluar el cumplimiento, pero relativos a la calidad; siempre y cuando en la evaluación sean utilizados de manera uniforme tanto para planear como para medir los resultados.*

Confiable

Para que el control sea útil, debe señalar resultados correctos sin desviaciones ni alteraciones y sin errores de ningún tipo, a fin de que se pueda confiar en que dichos resultados siempre son valorados con los mismos parámetros.

Estándares y normas de evaluación

Al medir los resultados alcanzados, éstos deberán compararse de acuerdo con los estándares y normas previamente establecidos, a fin de contemplar las mismas unidades para planear y controlar; con esto se logra una estandarización que permite valorar adecuadamente los alcances obtenidos.

* La medición de valores en auditoría, cualesquiera que sean sus ramas, necesariamente utiliza dos escalas de medición: **Los valores cuantificables o numéricos**, caracterizados por la utilización de cualesquiera escala de valor numérico, en donde a éstos se les asigna un cierto valor numérico que se utiliza para calificar y comparar contra otros valores esperados (también numéricos); los cuales sirven de referencia para medir y evaluar el cumplimiento (también se conocen como escalas de valores objetivas) y, **los Valores calificables**, caracterizados por utilizar escalas de medición no numéricas, en donde se califica por medios de apreciación subjetiva, no necesariamente en valores, como ejemplo estos pueden ser: excelente, deficiente, cumplió, adecuado, cumplido, etc (que se asignan por apreciación); sin embargo, con éstos calificativos se pueden medir el cumplimiento de lo realizado contra lo esperado, aunque no necesariamente se utilicen escalas numéricas que se puedan contar o medir.

4.1.6 Ciclo de aplicación del control

Para que el control sea aplicado correctamente en las instituciones, debe satisfacer un ciclo adecuado que va desde el establecimiento en planes y programas iniciales hasta su culminación en la retroalimentación. Podemos establecerlo concretamente de acuerdo con diferentes puntos de vista.

Kast y Rosenzweig, cuando citan a Marvin A. Mundel,[9] señalan los pasos del ciclo de control, los cuales se presentan en los puntos siguientes así como en la figura 4.1:

1. Determina objetivos y estrategias
2. Planea programas
3. Determina cargas de trabajo
4. Asigna los recursos requeridos a las cargas de trabajo
5. Adquiere/delega autoridad para utilizar recursos
6. Desempeña el trabajo
7. Compara el desempeño con el plan
8. Compara los objetivos alcanzados con los objetivos deseados
9. Compara el programa alcanzado con el programa planeado

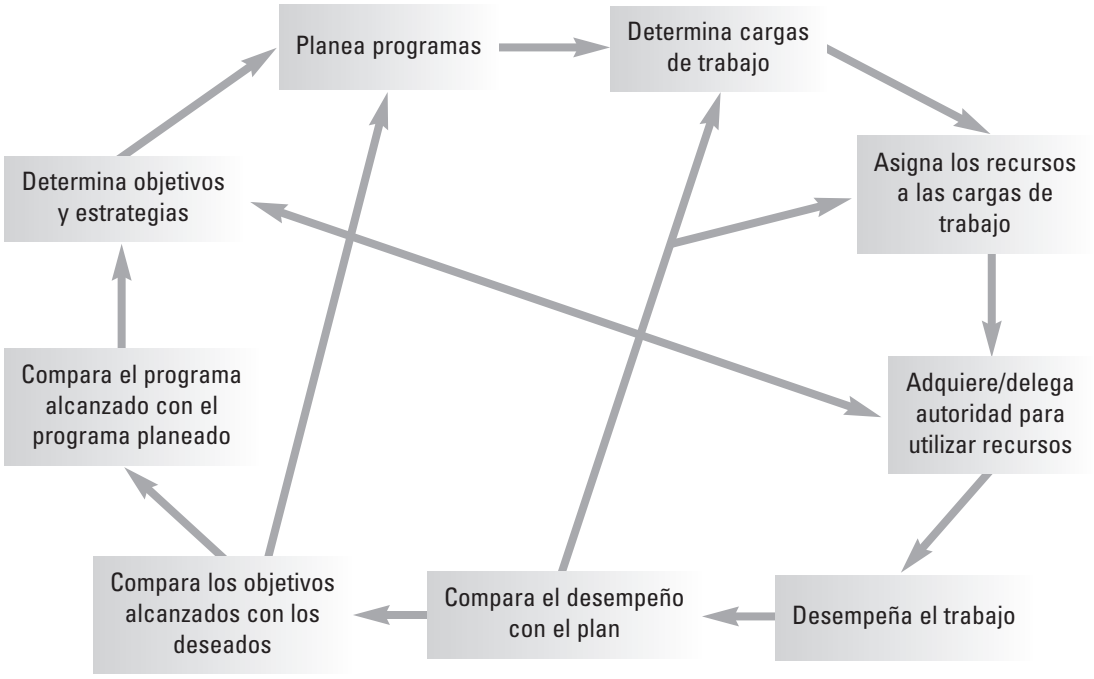


Figura 4.1 *Ciclo del control*

Una vez hecho el análisis de los conceptos anteriores y del cuadro complementario, podemos observar la utilidad del ciclo del control, el cual está perfectamente definido para su adopción en las empresas, ya que con su establecimiento se pueden cumplir sus objetivos. Además, se complementa con una estrecha interrelación entre varios de sus elementos, lo cual por sí solo refleja la importancia del establecimiento del control en las empresas; sin embargo, para complementar ese cuadro, a continuación se propone un ciclo de vida similar, sólo que estará más enfocado hacia la importancia del control en las empresas para la retroalimentación de planes y programas.

4.1.7 El control como sistema

De acuerdo con la teoría general de sistemas, entenderemos como sistema lo siguiente*: "Conjunto de elementos interrelacionados que pretenden satisfacer un fin"*, el cual está compuesto por un ciclo fundamental de comportamiento que consiste en insumos de entrada, proceso y resultados en salidas, pero complementado con una retroalimentación que le hace corregir las posibles desviaciones encontradas (vea la figura 4.2).

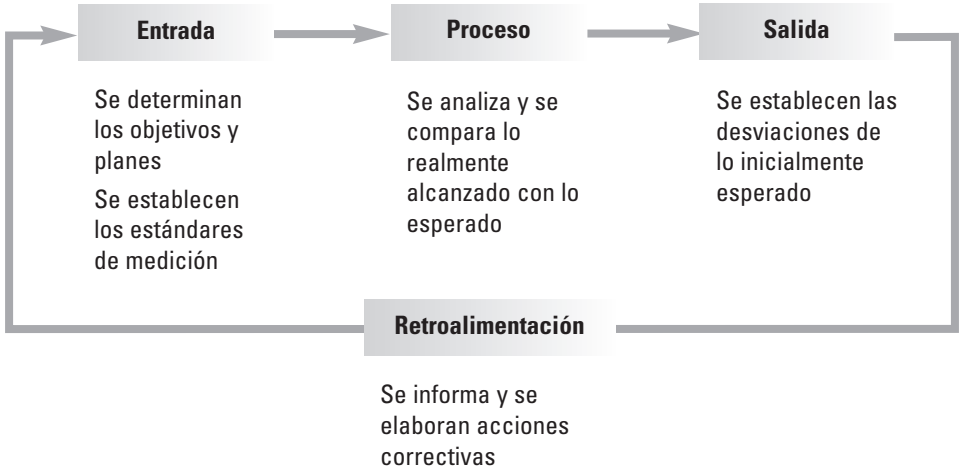


Figura 4.2 *El control como sistema*

Es evidente que el control, analizado como un sistema, nos permite identificar un comportamiento similar a los sistemas. El comportamiento de sus componentes se define de la siguiente manera:

- *Como* ***elementos de entrada (insumos),*** *nos referimos a la planeación de objetivos, programas, presupuestos y todos los aspectos que se espera alcanzar, incluyendo los estándares que permitirán determinar los aspectos y formas de*

evaluar tales resultados ; también se toma como insumo a la propia recopilación de datos.

- *Como **procesamiento,** vemos que al contar con los anteriores elementos de entrada podemos hacer el análisis de esa información, a fin de comparar lo realmente alcanzado contra lo que se esperaba obtener; esto nos permite evaluar el cumplimiento de lo señalado en los insumos.*
- *Como **resultados,** nos referimos a las conclusiones que se obtuvieron del procesamiento de la información anterior, lo cual permitirá obtener como salida el análisis del resultado de lo alcanzado contra lo esperado; con estos productos se realizará la información del comportamiento observado de la operación.*
- *La **retroalimentación** cierra el ciclo del control como sistema. Ésta consiste en informar de los resultados de la evaluación, a fin de tomar las medidas necesarias para corregir las posibles desviaciones, si es que las hubo, o en su caso, para realizar una mejor planeación en la fase de insumos.*

Este ciclo del control como sistema puede adaptarse a cualquier tipo de actividad; además, dentro de un plano netamente administrativo, es la base fundamental de la planeación y control de cualquier actividad en las empresas.

4.2 Conceptos y definiciones del control interno

El control interno es la adopción de una serie de medidas que se establecen en las empresas, con el propósito de contar con instrumentos tendientes a salvaguardar la integridad de los bienes institucionales y así ayudar a la administración y cumplimiento correctos de las actividades y operaciones de las empresas. Con la implantación de tales medidas se pueden conseguir los siguientes beneficios:

- *Proteger y salvaguardar los bienes de la empresa y a su personal.*
- *Prevenir y, en su caso, descubrir la presencia de fraudes, robos y acciones dolosas.*
- *Obtener la información contable, financiera y administrativa de manera confiable y oportuna.*
- *Promover el desarrollo correcto de las funciones, operaciones y actividades de la empresa.*

4.2.1 Definiciones de control interno

Para entender cómo funciona el control interno en las empresas es conveniente conocer los marcos conceptuales de este término. A continuación se presentan las aportaciones de algunos autores al respecto:

José Antonio Echenique

"El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus ac-

tividades, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración."[10]

HOLMES R. ARTHUR
"El control interno es una función de la gerencia que tiene por objeto salvaguardar y preservar los bienes de la empresa, evitar desembolsos indebidos de fondos, y ofrecer la seguridad de que no se contraen obligaciones sin autorización."[11]

L. HALL
"El control interno comprende la organización sistemática del trabajo administrativo y de los procedimientos de rutina, con el objeto de prevenir el fraude, los errores y los trabajos inútiles mediante el efecto disuasivo de los controles ejercidos."[12]

El control interno es especialmente importante en las empresas, debido a que proporciona el grado de confiabilidad que se requiere para:

- *Proteger los activos.*
- *Asegurar la validez de la información.*
- *Promover la eficiencia en las operaciones.*
- *Estimular y asegurar el cumplimiento de las políticas y directrices emanadas de la dirección.*

Para el diseño e implantación del sistema de control interno, se cuenta con el apoyo de las siguientes técnicas:

- *Ejecución del cuestionario de control.*
- *Análisis del flujo de transacciones.*
- *Realización de pruebas de cumplimiento.*
- *Resultados.*
- *Medidas de corrección.*[13]

Una vez hecho el análisis de las anteriores aportaciones, podemos inferir su definición:

El control interno es el establecimiento de los mecanismos y estándares de control que se adoptan en las empresas, a fin de ayudarse en la administración correcta de sus recursos, en la satisfacción de sus necesidades de seguridad, en la salvaguarda y protección de los activos institucionales, en la ejecución adecuada de sus funciones, actividades y operaciones, y en el registro correcto de sus operaciones contables y reportes de resultados financieros; todo ello para el mejor cumplimiento del objetivo institucional.

Como complemento, ahora podemos señalar esta definición de control interno con los siguientes beneficios que se obtienen con su establecimiento:

- *Salvaguardar los activos de la empresa.*
- *Determinar los métodos y procedimientos necesarios para el buen desarrollo de sus funciones y actividades.*

- *Establecer la elaboración correcta de los registros contables y de los resultados financieros.*
- *Contribuir con la dirección de la empresa en la implantación y cumplimiento de las normas, políticas y lineamientos que regularán su actuación.*

4.2.2 Objetivos del control interno

Tomando en cuenta que el **control interno** busca *contribuir en la seguridad y protección de los bienes de la empresa, en la obtención de información correcta y oportuna, en la promoción de la eficacia de la operación y en la dirección adecuada de la empresa*, se puede establecer que su principal prioridad es la ayuda que proporciona al buen funcionamiento de la institución y a la salvaguarda de su patrimonio. Sin embargo, hace falta una información adecuada para comprobar si se satisfacen esas prioridades.

Además, el control interno también sirve para evaluar el desarrollo correcto de las actividades de las empresas, así como la aceptación y cumplimiento adecuados de las normas y políticas que regulan sus actividades.

Con base en lo anterior, se pueden establecer los siguientes puntos como los objetivos fundamentales del control interno:

- *Establecer la seguridad y protección de los activos de la empresa.*
- *Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa.*
- *Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.*
- *Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.*
- *Implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.*

Continuando con el mismo esquema de exposición de esta obra, en los siguientes puntos se analizan por separado cada uno de estos objetivos.

4.2.2.1 Establecer la seguridad y protección de los activos de la empresa

Mediante la identificación y adopción de este objetivo en las empresas, se pretende establecer las pautas que sirvan para proteger y manejar adecuadamente los recursos financieros, bienes muebles e inmuebles, equipos y demás recursos que se les hayan asignado a dichas empresas o a sus áreas de trabajo.

Con la implantación del control interno se pretende vigilar que se cumpla con la protección y seguridad de los bienes y activos de la empresa, estableciendo todas las medidas, planes, programas, métodos, técnicas y funciones que permitan administrar adecuadamente sus activos.

Otra de las funciones básicas del control interno es vigilar y evaluar la adquisición, utilización, protección, custodia y resguardo correctos de aquellos bienes que permitirán valorar su óptimo aprovechamiento en la empresa, lo cual dicho sea de paso, también es el objetivo fundamental de una auditoría.

4.2.2.2 Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa

Para estar en condiciones de proteger los bienes de la empresa, lo primero que se debe hacer es verificar que los activos estén correctamente registrados, debidamente cuantificados y saber dónde están ubicados; esto se logra a través de una inscripción contable adecuada de las transacciones comerciales de la empresa y del registro oportuno de sus movimientos financieros. El propósito es que con dichos registros se puedan elaborar los estados de resultados de la empresa, en los cuales se refleje el comportamiento de sus bienes y activos, así como las utilidades que obtiene la misma con sus operaciones y actividades.

Para satisfacer este objetivo se busca, por medio del control interno, promover la confiabilidad, oportunidad y veracidad de todas las actividades comerciales y financieras que se realizan en la institución, a fin de verificar el registro correcto de sus transacciones contables, y así poder evaluar la emisión de sus resultados financieros, así como valorar las utilidades o el déficit que se obtenga durante un periodo determinado. En esto estriba la importancia del control interno.

Lo anterior es algo de lo que busca satisfacerse con el establecimiento del control interno en las empresas.

4.2.2.3 Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa

Otro de los objetivos básicos del control interno es contribuir a la mejor realización de las operaciones, actividades y tareas que se tienen asignadas en una institución, en sus áreas específicas o en determinadas unidades administrativas; esto únicamente se logra cuando se cuenta con la verificación y evaluación correctas del cumplimiento de las actividades de la institución, así como de sus funciones y tareas. Además, con ello se incrementan la eficiencia y eficacia en la realización de dichas actividades.

4.2.2.4 Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa

Para que se realicen fielmente las actividades de una empresa, se debe vigilar que se cumplan de manera adecuada las disposiciones, reglamentos y normas que regulan el

desarrollo de tales actividades, además de tener que cumplir con los métodos, técnicas y procedimientos previamente determinados.

Precisamente otro de los objetivos básicos del control interno es supervisar que se cumplan las normas, las políticas y los procedimientos que determinan la realización correcta de las funciones, actividades y tareas de una empresa.

4.2.2.5 Implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa

El siguiente objetivo fundamental del control interno es contribuir a la implantación y aplicación correctas de los métodos, técnicas y procedimientos que ayuden a evaluar y, en su caso, retroalimentar la realización adecuada de las funciones, actividades y tareas encomendadas a las áreas de una empresa.

En este punto, con el control interno también se busca evaluar el cumplimiento y apego a los métodos, técnicas y procedimientos que permitan desarrollar eficientemente las tareas que se tienen encomendadas dentro de una empresa.

Con la presentación de los objetivos anteriores sólo se busca ejemplificar los aspectos básicos que se deben considerar al implantar el control interno en una empresa, así como en alguna de sus áreas o en cualquier unidad administrativa. El propósito es que se tome en cuenta dicho control para su aplicación real en la institución, en el entendimiento de que dichos objetivos se pueden diseñar y adaptar de acuerdo con las necesidades concretas de la propia empresa.

Tampoco se debe perder de vista que el control interno busca verificar, evaluar y, en su caso, retroalimentar la protección de los activos de la empresa, el registro adecuado de sus operaciones contables y la emisión de sus resultados financieros, así como evaluar sus funciones, actividades y tareas. Esto se logra por medio de la implantación de los elementos del control antes señalados.

4.2.3 Importancia del control interno para la auditoría

Todas las empresas, sean públicas, privadas, de participación estatal, paraestatales o mixtas, deben contar con instrumentos adecuados de control que les permitan llevar su administración con eficiencia y eficacia. Por esta razón es tan importante contar con un control interno en la empresa, para satisfacer sus expectativas en cuanto a la salvaguarda y custodia de sus bienes, a la promoción de la confiabilidad, oportunidad y veracidad de sus registros contables y la emisión de su información financiera, a la implantación correcta de los métodos, técnicas y procedimientos que le permitan desarrollar adecuadamente sus actividades, tareas y funciones, así como al establecimiento y cumplimiento de las normas, políticas y procedimientos que regulan sus actividades. Lo mismo para empresas de giros comerciales, de servicios o de cualquier

otro giro, sin importar que sean pequeñas, medianas, o grandes empresas o consorcios. En todos los casos se deberá establecer el control interno.

El establecimiento de un sistema de control interno facilita a las autoridades de la empresa la evaluación y supervisión y, en su caso, la corrección de los planes, presupuestos y programas que determinarán el rumbo a seguir en la institución, de acuerdo con la misión, visión y objetivos de ésta. Con sólo cumplir lo anterior se justificaría la importancia del control interno.

Sin embargo, se puede agregar que la utilidad del control interno se distingue por el establecimiento y vigilancia del cumplimiento de reglas, métodos y procedimientos que se determinan para mantener la integridad y seguridad de los bienes de la empresa, así como para el manejo adecuado de los datos, para la confiabilidad en los registros y archivos contables, para la emisión de resultados financieros y para la definición de normas, lineamientos, procedimientos y reglas de actuación para el desarrollo de las actividades de la empresa. Además, con el control interno se establecen un conjunto de medidas y reglas concretas, la mayoría de carácter contable, que definen concretamente los alcances y limitaciones de actuación de los funcionarios y empleados de la institución.

Es precisamente en esas consideraciones donde se fundamenta la importancia de la auditoría, debido a que por medio del control interno se determinan las actividades, acciones y demás elementos que permiten satisfacer las necesidades de las instituciones. Además, recordemos que de la definición de la auditoría se desprende lo siguiente: *es la revisión de las funciones, acciones, operaciones o de cualquier actividad de una entidad administrativa*. Por esta razón, se evalúan la existencia y el cumplimiento del control interno en la empresa, así como la forma en que se aplica; también se evalúa su utilidad en la salvaguarda y protección de archivos y en el desarrollo de las actividades de la empresa, además de la existencia de los elementos que integran el señalado control interno. Es evidente que la importancia del control interno se fundamenta en la evaluación de lo que se determina por medio de él.

Por otro lado, en el ambiente contable se ha establecido que el estudio y la evaluación del control interno se utilizan para determinar el tipo, el alcance y la oportunidad de las empresas públicas, privadas, paraestatales o mixtas. Incluso, de acuerdo con las normas de auditoría, existen tres métodos para evaluar el estudio del control interno:

Método de cuestionario, en el cual se evalúan, por medio de cuestionarios, los procesos, rutinas y medidas básicas de la empresa, tanto las fundamentales y las principales como las secundarias con las que se llevan a cabo las actividades de la empresa.*

* En la teoría de la organización, las funciones de una empresa se clasifican en: **funciones básicas** o **sustantivas**, aquellas que se realizan para satisfacer el objetivo fundamental de la empresa; las **funciones** de apoyo, que son aquellas que se realizan para apoyar la realización de las primeras y las **funciones complementarias**, cuya existencia ayuda a realizar mejor las primeras funciones, pero su ausencia no repercute, en ningún caso, en el cumplimiento de las funciones básicas. Criterios que se pueden aplicar a las normas de auditoría relacionadas con la evaluación del control interno.

Método gráfico, en el cual se hace la evaluación de los mismos aspectos, pero mediante esquemas, gráficas, cuadros, flujos de operación y demás aspectos esquemáticos que ayudan a entender visualmente este control interno.

Método mixto, que es la combinación de los dos anteriores, ya que interroga por medio de cuestionarios y complementa los procesos, rutinas y procedimientos de la empresa por medio de gráficas, cuadros y diagramas.

La aplicación de esta evaluación y el estudio del control interno serán suficientes por sí mismos para destacar la importancia de este control en la auditoría, lo cual se hace extensivo a la auditoría de sistemas computacionales.

4.3 Elementos del control interno

Ya hemos analizado al principio de este capítulo que los elementos básicos del control son:

- *Establecimiento de estándares y mecanismos de medición*
- *Recopilación de los resultados obtenidos y análisis de la información*
- *Comparación y evaluación de los resultados alcanzados*
- *Retroalimentación a los planes y programas*

Sin embargo, estos elementos básicos del control han sido transformados, por medio de la aplicación contable y administrativa, en control interno y se han considerado los siguientes elementos para ser utilizados en las empresas:[14]

Elementos de organización

Dirección
Coordinación
Asignación de responsabilidades

Elementos de procedimientos

Planeación y sistematización
Registros y formas
Informes

Elementos de personal

Entrenamiento
Eficiencia y eficacia
Moralidad
Retribución

Elementos de supervisión

Revisión para precisar
Pérdidas y deficiencias

Mejores métodos
Mejores formas de control
Operaciones más eficientes
Mejor uso de los recursos físicos y humanos

La transformación de estos elementos se fundamenta en el *Boletín E-02* del Instituto Mexicano de Contadores Públicos, A.C., el cual señala lo siguiente acerca del control interno:

"El estudio y evaluación del control interno se efectúa con el objeto de cumplir con la norma de ejecución del trabajo que requiere que: el auditor debe efectuar un estudio y evaluación adecuados del control interno existente, que le sirvan de base para determinar el grado de confianza que va a depositar en él; asimismo, que le permitan determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría."[15]

Con el propósito de entender el funcionamiento del control interno en las áreas de informática, y transportar dicho entendimiento a su importancia en la auditoría de sistemas computacionales, a continuación se estudian los elementos del control interno, las partes que lo integran y sus características fundamentales.

4.3.1 Elementos de organización

Con la aplicación de este primer elemento del control interno se pretende entender la cohesión que se requiere entre las áreas y unidades administrativas de una empresa, así como la coherencia entre sus recursos, funciones y actividades para el cumplimiento adecuado de los objetivos encomendados a la misma; esto se logra mediante un diseño eficiente de estructura de organización. Dentro de este elemento se consideran también los siguientes subelementos.

Dirección

La dirección es uno de los elementos básicos para cualquier institución, debido a que es una parte fundamental para cumplir el objetivo institucional, ya que a través de la acción de dirigir se coordina el desarrollo de las actividades y la integración de los recursos humanos con los recursos materiales y económicos. También es la función que determina, supervisa y evalúa el cumplimiento de otras funciones, tareas y actividades en las demás áreas de la empresa.

En el control interno, la dirección es el elemento fundamental de la organización, ya que contribuye a la cohesión y coherencia de la estructura de organización y ayuda a supervisar el desarrollo de las funciones, actividades y tareas que se realizan para cumplir el objetivo institucional.

Coordinación

La coordinación es otro de los elementos fundamentales de cualquier institución, debido a que con dicha función los recursos humanos obtienen la armonía y la congruen-

cia que necesitan para la realización de sus actividades, contando con el apoyo de los otros recursos de la empresa; incluye la distribución ordenada de las tareas, métodos y procedimientos necesarios para cumplir el objetivo institucional.

En relación con su implantación en la empresa, esta actividad contribuye a la realización correcta de las funciones y actividades que tiene encomendadas la institución, lo cual se logra a través de la armonía, congruencia y distribución ordenada de los recursos disponibles para proteger los activos de dicha institución, así como a través del registro apropiado de sus operaciones, de la realización eficiente de sus actividades y de la emisión correcta de sus resultados financieros.

Asignación de responsabilidades

La asignación de responsabilidades representa la garantía de que las funciones, actividades y responsabilidades están correctamente delimitadas entre las áreas y los empleados de la empresa y de que éstos se comprenden en forma clara, concreta y correcta; además, también representa la delegación de autoridad y responsabilidad que tienen los encargados de realizarlas. Con lo anterior se busca la mayor eficiencia y eficacia en el cumplimiento de los objetivos institucionales.

Esta función contribuye a la distribución adecuada de las actividades y cargas de trabajo entre los integrantes de la empresa, a fin de lograr que el desarrollo de sus operaciones sea más eficiente y eficaz y que se cumpla con el objetivo de dicha empresa.

4.3.2. Elementos de procedimientos

Con este segundo elemento del control interno se pretende dar congruencia, continuidad y secuencia al desarrollo de las actividades y tareas que se tienen que realizar en la institución para el cumplimiento de sus objetivos. Su importancia radica en que se busca contribuir en la eficiencia y eficacia de las actividades de la empresa, por medio de una sucesión lógica, cronológica y congruente de sus actividades de trabajo, comúnmente llamadas métodos y procedimientos de operación. Esto sólo se alcanza mediante los siguientes subelementos.

Planeación y sistematización

La adopción de este subelemento permite diseñar aquellos métodos, técnicas y herramientas que servirán para desarrollar eficientemente todas las actividades y operaciones que se tienen encomendadas en la empresa y en sus áreas, con el propósito de satisfacer el objetivo institucional.

Su importancia radica en que además de establecer los métodos, técnicas y procedimientos para la ejecución correcta de las actividades de una empresa, también se establecen las normas, políticas y lineamentos que permitirán uniformar el desarrollo de sus actividades y funciones.

Cabe señalar que el cumplimiento adecuado de este subelemento del control interno también contribuye a la asignación precisa de actividades y tareas de cada uno de los recursos de la empresa.

Registros y formas

Esta parte del control interno se refiere al establecimiento de los instrumentos que permitirán registrar, de manera uniforme, todas las transacciones y actividades, así como los resultados obtenidos con el desarrollo de las operaciones de la institución, a la vez que permiten mantener los antecedentes históricos sobre ellos y, en muchos casos, permiten elaborar estadísticas sobre el registro, desarrollo y cumplimiento de las operaciones de la empresa, a fin de mantener un control eficiente sobre sus resultados.

En el control interno es de suma importancia establecer estos elementos, debido a que, además de servir de antecedentes estadísticos sobre el cumplimiento de las tareas, actividades y transacciones de la empresa, también se puede estandarizar el registro de esas operaciones, lo cual permite su uniformidad. Además, los registros y las formas permiten evaluar documentalmente los resultados alcanzados en comparación con lo planeado, y así estar en condiciones de retroalimentar a la empresa con dichos resultados para el mejor desempeño de sus actividades.

Informe

Es la presentación formal de los registros, estadísticas y resultados obtenidos durante un periodo determinado, el cual está dentro de un plan previamente definido para cumplir con las actividades de una institución. El principal propósito es presentar el resultado obtenido, a fin de comparar lo realmente logrado con lo que se esperaba obtener durante dicho periodo; así se puede evaluar el cumplimiento de los objetivos de la institución y, en su caso, retroalimentar sus actividades para su mejor realización.

La importancia que tienen los informes para el control interno radica en que, al establecer las formas y métodos de registros de las actividades, operaciones y resultados de la empresa, se pueden evaluar sus resultados finales y se puede medir el cumplimiento de los objetivos previamente determinados por dicha empresa.

4.3.3 Elementos de personal

El tercer elemento de importancia para establecer el control interno es el relacionado con los recursos humanos de una institución, ya que con estos recursos se realizan todas las funciones, actividades y operaciones dentro de la propia empresa; evidentemente, con el apoyo de los demás recursos de que dispone para sus operaciones.

La adopción de este elemento es de suma importancia para las empresas, ya que su utilización permite unificar y estandarizar el cumplimiento de las funciones de sus directivos, empleados, trabajadores, proveedores, socios, asesores y de todos los individuos que participan en el desarrollo de las actividades de las mismas.

Para entender la relevancia que tiene este elemento del control interno en la protección de los recursos de la empresa, en el registro y emisión de resultados y en la realización adecuada de sus actividades, es necesario establecer que el recurso más importante para cualquier institución es el humano, ya que es con el que se realizan

todas las actividades, funciones y tareas de la institución. Por esta razón, vamos a estudiar sus subelementos.

Entrenamiento

El entrenamiento se refiere a la capacitación, adiestramiento y preparación que se proporciona a los recursos humanos de una empresa, con el propósito de que éstos puedan desarrollar e incrementar sus conocimientos, habilidades, aptitudes y experiencias para el mejor desempeño de las funciones y tareas que les encomienda dicha empresa.

La importancia de este elemento es que con él se pueden determinar y adecuar las necesidades específicas de capacitación, adiestramiento y preparación del personal a través de cursos, seminarios, enseñanzas programadas, autocapacitación y otras herramientas, con lo cual se contribuye al mejor cumplimiento de sus funciones y actividades.

Eficiencia y eficacia

Este subelemento del control interno permite medir y evaluar el rendimiento adecuado de los recursos humanos de una empresa, a través de la explotación de las habilidades, conocimientos y aptitudes del personal para ejercer las funciones y actividades necesarias para alcanzar el objetivo de la institución. Para entender la importancia de este punto es necesario conocer los siguientes conceptos:

EFICIENTE:

"Que realiza la función para la que se destina. Competente, capaz [...]."[16]

EFICAZ:

"Eficiente, operativo. Se dice de la persona que lleva a cabo un proyecto, y de la cosa que contribuye a su realización."[17]

Una vez visto el significado de los conceptos anteriores, es fácil entender por qué es de suma importancia para las empresas utilizar este subelemento, ya que con su aplicación se contribuirá en gran medida al desempeño correcto de sus funciones, actividades y operaciones; tanto en lo eficaz como en lo eficiente.

Moralidad

"[...] la conformidad de los actos de alguien de acuerdo a sus principios..."[18]

La moralidad en el control interno es la actuación de los trabajadores de acuerdo con los principios y normas que regulan su conducta dentro de la empresa, así como en la sociedad.

El establecimiento de este subelemento garantiza la actuación adecuada de los recursos humanos en la realización de sus funciones y actividades a fin de cumplir con los objetivos de la empresa. La importancia de este subelemento es que, a nivel de directivos, empleados, trabajadores, proveedores, asesores, clientes y de cualquier otra

persona que tenga contacto con la empresa, uniforma la actuación correcta de estos recursos humanos en beneficio de la propia institución.*

Retribución

Desde sus primeros tratados de administración, F. Taylor y H. Fayol han señalado la importancia de la equidad en la retribución del ingreso comparado con la carga de trabajo que se realiza. Éste es uno de los aspectos fundamentales para conservar al trabajador dentro de la empresa, y al mismo tiempo sirve para que el empleado aporte su mejor esfuerzo, conocimientos, habilidades y aptitudes para el desarrollo correcto de sus actividades.

Este subelemento es de suma importancia para que los recursos humanos de una empresa realicen las funciones y actividades que les fueron encomendadas; además, con su establecimiento se regularán las relaciones laborales entre la empresa, como persona moral, y el trabajador, como persona física, procurando la equidad entre el trabajo del empleado y su retribución. Además, esta relación mantendrá la equidad en las prestaciones que recibe el trabajador y las obligaciones de la empresa.

4.3.4 Elementos de supervisión

El último elemento del control interno es la revisión de las actividades que se realizan en la empresa, lo cual se realiza a través de la inspección, supervisión y evaluación del cumplimiento de las funciones y actividades de todos sus recursos.

La supervisión, entendida como la evaluación permanente que se realiza a las actividades encomendadas a los recursos humanos de una empresa, es la otra parte que complementa el desarrollo correcto de las funciones de la entidad, ya que este elemento pretende revisar y evaluar los resultados obtenidos durante un periodo para compararlos con lo inicialmente planeado.

Se podría asegurar que este último elemento del control interno es el que fundamenta la existencia de las auditorías, ya que, como se indicó al principio de este capítulo, el control tiene cuatro elementos fundamentales:

- *El diseño de los instrumentos de evaluación.*
- *La recopilación de los resultados obtenidos.*
- *La evaluación de los resultados obtenidos.*
- *La retroalimentación de la empresa para la mejor planeación de sus actividades.*

Estos elementos fundamentan la existencia de la supervisión, ya que la entidad o persona que ejerce esta actividad en la empresa hace una constante revisión de los resultados de sus subordinados y también de los registros donde se asientan sus operaciones. Con esta evaluación se estará en condiciones de retroalimentar a una empresa para la ejecución correcta de sus actividades.

* En el capítulo 3 fueron tratados todos los aspectos relacionados con la ética, moral y valores del auditor; éstos también pueden aplicarse a estos recursos humanos.

4.3.4.1 Revisión para precisar

Es la acción de obtener información, analizarla y evaluarla, a fin de precisar si el cumplimiento de las actividades, planes y funciones de la empresa ha sido el adecuado, lo cual se logra únicamente por medio de la supervisión constante de las actividades y resultados.

4.3.4.2 Pérdidas y deficiencias

El control interno contribuye, por medio de la supervisión, a que en las empresas y sus áreas no existan pérdidas de los bienes y activos, así como para detectar las irregularidades en la protección, el cumplimiento y la realización correcta de las funciones de dichas empresas.

4.3.4.3 Mejores métodos

Para realizar de manera adecuada los planes, actividades, funciones y resultados de las empresas, es necesario que, por medio de la supervisión, se haga una evaluación constante de su cumplimiento, lo cual sólo se logra con mejores métodos de trabajo, resultado de la retroalimentación del control interno en las empresas.

4.3.4.4 Mejores formas de control

Entre más se aplica la supervisión en las actividades de una empresa, también se van mejorando las formas de evaluar el desempeño de los planes, programas y actividades, con lo cual se puede retroalimentar su cumplimiento. Es evidente que esto se obtiene con una aplicación adecuada de la supervisión, lo cual permite determinar las mejores formas de control en todas las funciones de una empresa.

4.3.4.5 Operaciones más eficientes

A medida que se mejoran las formas de control con el establecimiento del control interno en las empresas, también se mejorarán sus resultados por medio de la supervisión, lo cual ayuda a realizar mejor sus operaciones.

4.3.4.6 Mejor uso de los recursos físicos y humanos

La implantación del control interno en las empresas, además de satisfacer todos los aspectos antes señalados, se complementa con la supervisión para obtener el mejor aprovechamiento de los recursos tanto humanos como físicos; además contribuye al logro de mejores resultados en el cumplimiento de las funciones de éstos.

De los puntos antes estudiados se desprende la importancia de estos elementos del control interno, ya que su principal función es revisar y evaluar la protección de los activos de la empresa, así como su uso adecuado; además, sirven para analizar el re-

gistro y emisión correctos de sus resultados financieros. Asimismo, con estos elementos se evalúa el cumplimiento de las actividades de una empresa, de acuerdo con lo determinado en los planes, programas, métodos, procedimientos y técnicas. Igual ocurre con las normas, políticas y lineamientos que regulan la actuación de los recursos de la empresa. Es evidente que esta finalidad del control interno también se cumple, o complementa, cuando se realiza una auditoría.

4.4 Estándares de control

Para complementar la conceptualización del control interno en las empresas, ahora nos conviene señalar algunos de los principales estándares que se pueden utilizar en la medición del control y del control interno de las instituciones, con el fin de ayudar a la eficiencia y eficacia en el desarrollo de las actividades normales de éstas. A continuación encontramos los siguientes estándares.

4.4.1 Estándares físicos

Son aquellos estándares que se pueden apreciar mediante algunas medidas de dimensión de tipo tangible, tales como: extensión, longitud, magnitud, tamaño, volumen, calibre, etcétera; también se incluyen los valores monetarios, sólo que a éstos los analizaremos en los siguientes estándares.

En el control interno, los estándares físicos pueden agruparse de la siguiente manera:

4.4.1.1 Estándares físicos de medición

Son los que se establecen para medir y contar superficies, volúmenes, pesos, distancias y cualquier otro tipo de medidas de carácter físico, los cuales se pueden diseñar para comparar con otras medidas previas. Por ejemplo, medir los metros de construcción, apreciar el volumen (litros) de líquidos producidos en una jornada, contar las toneladas producidas de cereales o cualquier otro parámetro que se pueda calcular, de acuerdo con el establecimiento de medidas universalmente establecidas.

4.4.1.2 Estándares físicos de comparación

Estos estándares se establecen como proporciones y ordenadores matemáticos que sirven para comparar entre una dimensión y otra, tales como las operaciones aritméticas, los registros contables, las mediciones estadísticas y otros factores de medida utilizados para comparar. Entre ellos encontramos:

- *Los operadores matemáticos:* sumando (+); sustraendo (–); igual a... (=); mayor que... (>) menor que... (<), etcétera.
- *Las ecuaciones de cualquier grado que sirven para comparar entre un resultado y otro.*
- *La aplicación de las reglas contables y razones financieras, etcétera.*

4.4.1.3 Estándares físicos de acumulación

Son aquellos medidores que permiten hacer mediciones que indican acumulación de algo, tales como la acumulación de intereses, estándares de producción y otros estándares de aplicación similar.

4.4.2 Estándares de costos

Son mediciones de tipo monetario que permiten hacer una estimación del costo (*valor que se le da a un trabajo*); estos estándares pueden ser contados por cualquier medio, considerando en ello el valor que se le da, en aspectos numerarios, a cualquier actividad; por ejemplo, las transacciones del mercado y las operaciones de una empresa.

Entre los principales estándares de costos podemos destacar los siguientes:

4.4.2.1 Estándares de costos fijos

Se refieren a aquellas partes de los costos que no varían con el nivel de producción y que, se produzca o no, de todos modos se tienen que realizar; estos costos fijos siempre están directamente implicados en cualquier operación; por ejemplo, la renta de un local, la energía eléctrica que se consume, el costo de empleados administrativos, etcétera.

4.4.2.2 Estándares de costos variables

Son aquellos costos que se asignan a los resultados de la operación de cualquier negocio, los cuales están directamente relacionados con el volumen de producción de los bienes o servicios de la empresa; estos costos se pueden agrupar en los siguientes grupos.

Costos de materias primas

Costos variables que se acumulan en función al volumen de materias primas utilizadas en la producción de bienes o servicios.

Costos de producción

Son los costos que están directamente involucrados en la producción de algún bien o servicios que no sean materias primas ni ventas, tales como combustibles, refacciones de las máquinas, costo de suministros de operación, etcétera.

Costos de venta

Para llevar los bienes y servicios de la institución al mercado de consumidores, es necesario realizar una serie de gastos que se conocen como costos de venta, los cuales se harán en función al volumen de ventas y se utilizarán en la venta y distribución de dichos bienes a manera de comisiones, gastos de publicidad, gastos de entrega, etcétera.

Costos de mano de obra

Los principales costos que se tienen en las empresas son los relacionados con el personal que labora en ellas, entre los cuales se destacan la mano de obra administrativa, la mano de obra de producción, los costos de la fuerza de venta, etcétera.

Otros costos

En las empresas existen muchos tipos de costos, por lo cual es necesario señalar que dichos costos pueden agruparse según las características propias de cada institución y según sus diferentes maneras clasificación, pero invariablemente deben ser tomados en cuenta.

4.4.3 Estándares de capital

Son aquellos estándares que se adoptan en las empresas para el manejo y control de los llamados bienes de capital, ya sea capital de trabajo, capital contable, capital financiero o cualquier otro tipo de estándar que incide en el capital que se maneja en las empresas.

A continuación tenemos algunos ejemplos de estos indicadores de capital.

4.4.3.1 Estándares económicos

Son todos aquellos indicadores de capital que se manifiestan de acuerdo con la evaluación de la economía de una empresa y que son dictaminados por los estándares económicos generalmente aceptados dentro de una sociedad comercial.

4.4.3.2 Razones financieras

Son los valores comparados que se establecen por medio del análisis de los resultados financieros de una empresa, los cuales se utilizan con el propósito de evaluar el adecuado funcionamiento de sus actividades financieras, en concordancia plena con sus requisitos contables.

4.4.3.3 Estándares de rendimiento de capital

Son los estándares que se adoptan en las instituciones para medir el rendimiento del capital puesto a su disposición, con los cuales se establecen los beneficios derivados del uso de dicho capital. Entre estos estándares encontramos las tasas de rendimiento, los indicadores de rentabilidad, la Tasa Interna de Retorno (TIR), los flujos de efectivo, etcétera.

4.4.3.4 Inventarios

Es la acumulación de capital de trabajo y bienes de la empresa, los cuales están a su disposición para la producción de bienes y servicios; entre estos estándares podemos

citar la inversión fija en maquinaria, en equipos de transporte, en muebles e inmuebles, en inventarios de materias primas y de productos terminados, etcétera.

4.4.4 Estándares de ingresos y egresos

Son los valores monetarios que se asignan a los ingresos (*entradas*) y egresos (*salidas*) que tiene una empresa como parte fundamental de sus actividades de trabajo; por lo general, están expresados en numerario y sirven para evaluar el grado de cumplimiento de los planes y programas de carácter monetario. Dichos estándares se presentan a continuación:

4.4.4.1 Estándares de ingresos

Aquí se agrupan todos los estándares que se derivan de las captaciones que tiene la empresa, ya sean por la ventas de sus bienes y servicios, por sus resultados financieros e intereses, por sus venta de acciones, bonos, empréstitos, etc., los cuales permitirán, junto con los egresos, valorar sus resultados financieros.

4.4.4.2 Estándares de egresos

Los estándares que aquí se agrupan están relacionados con las erogaciones que tiene una institución para su mantenimiento, tales como gastos de producción, costos de mano de obra, pagos de préstamos, intereses y utilidades, etcétera.

4.4.5 Estándares no tangibles

Los estándares que hemos analizado anteriormente se relacionan con elementos físicos que de alguna manera pueden ser contados; sin embargo, para el control interno de las empresas también se pueden utilizar otros tipos de estándares que no necesariamente deben ser tangibles ni numerales, los cuales, aunque no se puedan cuantificar, sí se deben identificar y tomar en cuenta.

Está claro que existen muchos de estos estándares y la mayoría pudieran ser considerados de tipo subjetivo, ya que son difíciles de expresar en mediciones físicas y monetarias; sin embargo existen y son muy utilizados en las empresas para evaluar el cumplimiento de sus actividades y operaciones.

Por lo general, estos estándares son representaciones que se dan a las cualidades de las cosas. A continuación citaremos algunos ejemplos de dichas representaciones:

- *Bueno (aquel que hace bien las cosas)*
- *Satisfactoriamente (que satisface los requerimientos)*
- *Bondadoso (el que tiene bondad)*
- *Adecuado (acomodado de una cosa a otra)*

- *Valeroso (aquel que tiene valor para alguien o algo)*
- *Brillante (el que sobresale de los demás)*

Como se observa en los ejemplos anteriores, sería muy difícil cuantificar estos estándares en forma correcta, salvo que se vuelvan a calificar; por ejemplo, en el caso de bueno tendríamos *muy bueno, poco bueno, nada bueno*; en el caso de satisfactorio tendríamos*, altamente satisfactorio, cumplió satisfactoriamente, poco satisfactorio, poco insatisfactorio*, altamente insatisfactorio, etcétera.

Su utilización para el control interno es muy importante, aunque para muchos no tiene gran validez su aplicación; sin embargo, en las empresas, y en el informe de auditoría, su empleo es constante. Para prueba de ello, basta con citar el inicio de la opinión de algunos auditores:

"[...] en mi opinión cumple satisfactoriamente con los [...]"

Como es fácil de observar, en este tipo de estándares la cuantificación y los valores que se les da a estos conceptos solamente estarán medidos por su cualidad y calificación subjetiva.

4.4.6 Estándares de control estadístico

Estos estándares son de los más difundidos y de mayor aceptación en la utilización del control interno en las empresas, ya que permiten establecer, medir y evaluar, al amparo de razones matemáticas, estadísticas, y en algunos casos integrales y diferenciales, los resultados alcanzados en las empresas.

En este punto se indica la existencia de dichos estándares ya que serán utilizados de alguna manera durante el desarrollo de este libro, en el entendimiento de que son parte fundamental del mismo.

4.4.7 Estándares de auditoría

Los estándares que se comentan en esta parte son la esencia de este libro, ya que a lo largo del mismo se presentan como las herramientas, métodos, técnicas y procedimientos de auditoría y, en sí, de los elementos de control que se utilizan durante todo este punto.

Por esta razón, ya no será comentado ninguno de estos tipos de estándares y sólo se mencionará su existencia para complemento de este punto, ya que posteriormente se analizarán con el enfoque y aplicación que corresponden a la auditoría de los sistemas informáticos.

4.4.8 Normas de evaluación[19]

El maestro Rodríguez Valencia analiza los estándares de control bajo otro criterio, relacionando los estándares de evaluación con normas que contribuyen al establecimiento de los parámetros de evaluación que se requieren para el establecimiento del

control interno necesario para realizar una auditoría; sin embargo, las normas que a continuación se indican, en algunos casos parecerán repetitivas en comparación con las antes expuestas, pero la intención de darlas a conocer en este apartado es complementar algunos estándares que se pueden considerar para hacer la medición de resultados que se necesitan en el control; dichas normas son las siguientes.

4.4.8.1 Normas cuantitativas

Son aquellas que permiten dar una cuantía medible en cifras significativas, con las cuales se establecerán parámetros válidos para medir resultados. A continuación presentamos las siguientes normas sin hacer ningún comentario al respecto, ya que son fáciles de comprender.

- *Normas físicas*
- *Normas de costos*
- *Normas de capital*
- *Normas de ingresos*
- *Normas de programas*
- *Normas de productividad*
- *Normas de posición en el mercado*

4.4.8.2 Normas cualitativas

Estas normas se establecen de forma no tan objetiva, y sirven de parámetros cualitativos (que denotan una cualidad que se atribuye a algo); asimismo, ayudan a medir ciertos aspectos no cuantificables en unidades físicas, pero sí medibles en otros parámetros no numerarios.

Al igual que las anteriores, mencionaremos esta lista de normas sin ningún comentario.

- *Normas de publicidad*
- *Normas de desarrollo de personal*
- *Normas de información*
- *Normas de hegemonía del producto*
- *Normas de actitudes de los empleados*

4.4.8.3 Normas materiales

Estas normas se refieren a los criterios que permiten evaluar aspectos fundamentales en el desempeño de las actividades de una empresa, los cuales pueden ayudarnos a establecer estándares de evaluación útiles en el control; estas normas están divididas en dos grandes grupos:

Normas de desempeño

Son aquellas que permiten medir los resultados alcanzados con una operación normal de una empresa; dichas normas son las siguientes.

- *Normas de cantidad*
- *Normas de calidad*
- *Normas de costos*
- *Normas de tiempo*

Normas complementarias

Estas normas se establecen para apoyar la evaluación de las normas de desempeño, con ello se complementan los estándares de medición de las primeras; entre estas normas encontramos las siguientes:

- *Normas de factores físicos*
- *Normas de comportamiento*
- *Normas de función*
- *Normas de políticas*

4.4.9 Otras normas y estándares

Actualmente existen muchos tipos de estándares que buscan utilizarse para evaluar el cumplimiento de lo alcanzado en relación con lo esperado, por eso a continuación se indican algunos de estos ejemplos:

4.4.9.1 Estándares del IEEE

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) fue formado a principios de los 80 para desarrollar estándares para las tecnologías emergentes en muchas de las ramas de la ingeniería; para el caso específico del área de sistemas computacionales y en especial para que los equipos de redes de diferentes fabricantes pudieran trabajar juntos e integrarse sin problemas, se formó el comité de la serie IEEE 802, el cual está relacionado con el Modelo ISO (Organización Internacional de Estándares) de la OSI, específicamente su desarrollo es el siguiente:*

- *En el año de 1982 se publicó un borrador de los estándares para redes CSMA/CS y Token Bus.*
- *En 1983 se publicó el estándar 802.3, que describe una red de banda base CSMA/CD similar a Ethernet. Desde entonces se le han hecho algunos anexos dependiendo del tipo de medio físico que se utilice. Estos anexos incluyen redes como:*
  - *10BASE-2. Red de banda base que opera con cable coaxial delgado a 10 Mbps.*
  - *1BASE-5. Red de banda base que opera con cable trenzado a 1 Mbps.*

* En la sección 12.7, "Auditoría a los sistemas de redes", se amplían conceptos sobre estos puntos.

- *10BASE-T. Red de banda base que opera con cable trenzado a 10 Mpbs.*
- *10BROAD-36. Red de banda base que opera con cable coaxial grueso a 10 Mbps.*

- *El siguiente estándar publicado fue el 802.4 que describe una red con paso de token, orientada a transmisiones tanto de banda amplia como de banda base.*
- *El tercer estándar fue el 802.5, se basó en las especificaciones de la red IBM de Token-Ring. Éste define una red Token-Ring con cable trenzado cubierto con transmisión de datos de 1 a 4 Mbps. Se le han hecho mejoras al estándar para incluir entre otras cosas una tasa de operación de 16 Mbps.*

4.4.9.2 Normas de la serie ISO-9000

La ISO elaboró las normas de la serie ISO 9000 para la gestión y el aseguramiento de la calidad y la primera edición de las normas fue en 1987. Posteriormente, en 1994 se hizo una revisión de las normas y se espera una próxima revisión para el año 2000.

La serie ISO 9000 se compone de las siguientes normas:[20]

- *ISO 9000: incluye directrices para la selección y uso de las normas de la serie.*
- *ISO 9001: da los requerimientos exigibles a la organización para el aseguramiento de la calidad en las actividades de diseño, desarrollo, producción, instalación, inspección y servicio posventa.*
- *ISO 9002: determina los requerimientos exigibles para el aseguramiento de la calidad en las actividades de producción, instalación y servicio posventa.*
- *ISO 9003: establece los requerimientos exigibles para el aseguramiento de la calidad sólo en las actividades de inspección y ensayos finales.*
- *ISO 9004: es una guía para la gestión de la calidad y elementos del sistema de calidad.*

Las normas complementarias de la serie son:

- *ISO 8402: es una recopilación del vocabulario utilizado en las normas de la serie.*
- *ISO 10011-1/2/3: establecen criterios de auditorías, de calificación de los auditores y de gestión de programas de auditorías, respectivamente.*
- *ISO 100013: es una guía para la elaboración del manual de calidad para la organización.*
- *De todas las normas de la serie, las únicas certificables son la 9001, 9002 y 9003.*

4.4.9.3 Estándares de educación

La educación, en cualquiera de sus niveles, demanda de constantes evaluaciones de su cumplimiento en el desempeño de sus maestros, los resultados de sus educandos, los planes y programas y muchos otros componentes de la educación que son susceptibles de evaluar; entre algunos de los componentes medulares de la evaluación curricular, como ejemplo común en todos los estándares, señalamos los siguientes aspectos.

- ***Conocimientos:*** *conceptos, ideas, datos, divergencias, principios, teorías, tecnología, paradigmas, leyes.*
- ***Valores, actitudes y virtudes humanas:*** *ética, dignidad, solidaridad, igualdad, integridad, autocontrol, responsabilidad, socialización.*
- ***Diseños curriculares:*** *Componentes, perfiles de egresados, objetivos, mapas curriculares, programas analíticos y detallados, evaluación y otros componentes que señalan las características de una educación primaria, secundaria, media superior, estudios universitarios o de posgrado.*
- ***Destrezas y competencias:*** *vida, reflexión, pensamiento, comunicación, estudio, investigación, adaptación, trabajo, tecnología, integración, teorización.*
- ***Estudio y trabajo:*** *calidad total, compromiso, dedicación, servicio, producción, tecnología, empleabilidad, economía y desarrollo global.*
- ***Diversidad cultural:*** *etnicidad, raza, edad y género, procedencia, status socioeconómico, tipo de familia, excepcionalidad, escolaridad.*
- ***Prevención:*** *salud, higiene, conservación de recursos, violencia, drogas, alcohol y armas.*

Estándares y normas de calidad

En estos casos es donde se diseñan estándares y normas por medio de los cuales se busca apreciar los cumplimientos en cuanto a la calidad esperada en relación con la calidad realmente alcanzada; éstos pueden ser muchos tipos de estándares de medición y muy variados aspectos, por esa razón sólo se menciona su existencia y aplicación.

Normas Oficiales Mexicanas

Se han diseñado una serie de normas mexicanas que buscan estandarizar la realización de evaluaciones en muchos aspectos, de entre los cuales se destaca la lista de NOM correspondiente al año 2000:[21]

- *PROY-NOM-152-SCT1-1999, PROYECTO de Norma Oficial Mexicana sobre Interfaz digital a redes públicas (Interfaz digital a 2,048 Kbit/s).*
- *PROY-NOM-151-SCT1-1999, PROYECTO de Norma Oficial Mexicana sobre Interfaz a redes públicas para equipos terminales.*
- *NOM-EM-151-SCT1-1998, NORMA Oficial Mexicana sobre Interfaz a redes públicas para equipos terminales (NIRPET).*
- *NOM-EM-151-SCT1-1997, NORMA Oficial Mexicana de Emergencia sobre Interfaz a redes públicas para equipos terminales.*
- *NOM-121-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Sistemas de radiocomunicación que emplean la técnica de espectro disperso en las bandas de 902-928 MHz, 2,450-2,483.5 MHz y 5,725-5,850 MHz.*
- *NOM-EM-113-SCT1-1994, NORMA Oficial Mexicana de Emergencia sobre Especificaciones técnicas para los servicios relativos a la conducción de señales entre puntos fijos mediante el uso de los satélites mexicanos.*

- *NOM-103-SCT1-1995, PROYECTO de Norma Oficial Mexicana sobre Interfaz U de Acceso Básico a la RDSI por par metálico.*
- *NOM-102-SCT1-1995, NORMA Oficial Mexicana sobre Protocolo del nivel de enlace de datos del interfaz usuario-red para la Red Digital de Servicios Integrados (canal D).*
- *NOM-101-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Cables de fibras ópticas unimodo para uso exterior. Parte 2.*
- *NOM-100-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Bloques terminales para cables telefónicos.*
- *NOM-092-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 4: Terminología empleada en electroacústica.*
- *NOM-091-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 7: Terminología empleada en radiocomunicación.*
- *NOM-090-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Designación de cables y alambres usados en telefonía.*
- *NOM-089-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Diagramas, gráficas y tablas utilizadas en electrónica. Parte 2: Identificación de elementos.*
- *NOM-088-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Sistemas de relevadores radioeléctricos del servicio fijo multicanal que operan en la banda de 2,300-2,450 MHz.*
- *NOM-EM-086-SCT1-1994, NORMA Oficial Mexicana de Emergencia sobre Estaciones del servicio de aficionados.*
- *NOM-EM-085-SCT1-1993, NORMA Oficial Mexicana Emergente sobre Instalación y operación de estaciones de radiocomunicación a bordo de embarcaciones.*
- *NOM-085-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Instalación y operación de estaciones de radiocomunicación a bordo de embarcaciones.*
- *NOM-084-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Instalación y operación de estaciones destinadas al servicio móvil de radiocomunicación especializada de flotillas.*
- *NOM-083-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Instalación y operación de estaciones destinadas al servicio de radiolocalización móvil de personas.*
- *NOM-081-SCT1-1993, NORMA Oficial Mexicana sobre Sistemas de radiotelefonía con tecnología celular que operan en la banda de 800 MHz.*
- *NOM-081-SCT-1993, PROYECTO de Norma Oficial Mexicana sobre Sistemas de radiotelefonía móvil con tecnología celular que operan en la banda de 800 MHz.*
- *NOM-080-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Diagramas, gráficas y tablas utilizadas en electrónica. Parte 1: Definiciones y clasificación.*

- *NOM-079-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 17: Componentes electromecánicos para equipos electrónicos.*
- *NOM-075-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 3: Terminología empleada en dispositivos semiconductores.*
- *NOM-074-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Equipos para sistemas de sonido. Parte 2: Terminología.*
- *NOM-073-SCT1-1994, PROYECTO de Norma Oficial Mexicana. Terminología empleada en receptores monocromáticos de la banda comercial.*
- *NOM-072-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Definiciones empleadas en teléfonos.*
- *NOM-071-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 12: Radiocomunicaciones espaciales.*
- *NOM-070-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Terminología para equipos de microondas*
- *NOM-069-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 14: Terminología empleada en líneas de transmisión y guía de ondas.*
- *NOM-067-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 2: Electrónica.*
- *NOM-066-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Vocabulario electrotécnico. Parte 1: Definiciones fundamentales.*
- *NOM-065-SCT1-1993, Vocabulario electrotécnico. Parte 15: Telecontrol.*
- *NOM-064-SCT1-1994, PROYECTO de Norma Oficial Mexicana. Vocabulario electrotécnico. Parte 16: Terminología empleada en registro y lectura del sonido e imagen (audio y video).*
- *NOM-065-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Vocabulario Electrotécnico. Parte 15: Telecontrol.*
- *NOM-063-SCT1-1993, Vocabulario electrotécnico. Parte 5: Perturbaciones radioeléctricas.*
- *NOM-062-SCT1-1994, NORMA Oficial Mexicana sobre Terminología y conceptos básicos aplicables a transmisión de telefonía por microondas.*
- *NOM-061-SCT1-1993, NORMA Oficial Mexicana sobre Definiciones empleadas en equipos de radiocomunicación para servicios móviles.*
- *NOM-060-SCT1-1993, Terminología y conceptos básicos aplicables a los sistemas de transmisión de datos. Parte 1: Módems.*
- *NOM-059-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Modulación por impulsos codificados (MIC) de frecuencias vocales. Vocabulario.*
- *NOM-058-SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Símbolos gráficos empleados en diagramas. Parte 10: Telecomunicaciones, transmisión.*

- *NOM-057 SCT1-1994, PROYECTO de Norma Oficial Mexicana sobre Símbolos gráficos empleados en diagramas. Parte 9: Telecomunicaciones, equipos periféricos y de conmutación.*
- *NOM-056-SCT1-1993, NORMA Oficial Mexicana sobre Definiciones para fuentes de alimentación utilizadas en telefonía.*
- *NOM-055-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Terminología empleada en dispositivos semiconductores y sus definiciones.*
- *NOM-EM-053-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Aparatos telefónicos inalámbricos.*
- *NOM-051-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Equipos de respuesta automática y/o equipo de llamada automática paralelo en la red telefónica general con conmutación, con procedimientos para la neutralización de los dispositivos de control de eco en las comunicaciones establecidas, tanto manual como automáticamente.*
- *NOM-048-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Equipos transmisores receptores de microondas con modulación analógica (MF) utilizados en telefonía.*
- *NOM-EM-044-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Amplificador para transmisión de datos en la banda de 300 a 3,400 Hz.*
- *NOM-044-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Amplificador para transmisión de datos en la banda de 300 a 3,400 Hz.*
- *NOM-043-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Módem normalizado de 2,400/1,200 bits por segundo (bits/s) para uso general en la red telefónica conmutada en modo semidúplex.*
- *NOM-042-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Módem normalizado de 1,200/600 bits por segundo (bits/s) para uso general en la red telefónica en modo dúplex completo a cuatro hilos.*
- *NOM-041-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Módem normalizado de 2,400 bit/s que utiliza la técnica de división de frecuencia para uso en la red telefónica pública conmutada en modo dúplex y en circuitos arrendados punto a punto a dos hilos.*
- *NOM-037-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Amplificador de voz bidireccional para uso en la red telefónica.*
- *NOM-EM-036-SCT1-1994, NORMA Oficial Mexicana de Emergencia sobre Teléfonos aplicables a centrales públicas o centrales privadas PABX.*
- *NOM-EM-034-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Equipos accesorios de conmutación telefónica privada con y sin marcación automática.*
- *NOM-EM-033-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Teléfono automático de alcancía.*
- *NOM-032-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Puestos de operadora.*

- *NOM-030-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cubiertas herméticas para empalmes de cables telefónicos subterráneos.*
- *NOM-027-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cubiertas termoplásticas para cables telefónicos usados en planta exterior.*
- *NOM-024-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Conectores secos para conductores de cobre de cables telefónicos.*
- *NOM-023-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cables telefónicos con aislamiento y cubierta termoplástica con pantalla de aluminio tipo Screb.*
- *NOM-019-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Modulación por impulsos codificados (MIC) de frecuencias vocales. Codificación de las señales analógicas.*
- *NOM-EM-018-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Modulación por impulsos codificados (MIC) de frecuencias vocales, especificaciones de los equipos múltiplex primarios MIC para 2,048 kbits/s.*
- *NOM-018-SCT1-1993, PROYECTO de Norma Oficial Mexicana referente a la Norma anterior NOM-I-057/4-1978, Modulación por impulsos codificados (MIC) de frecuencias vocales, especificaciones de los equipos múltiplex primarios MIC para 2,048 Kbits/s.*
- *NOM-017-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cable telefónico de distribución autosoportado.*
- *NOM-016-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cable telefónico relleno con aislamiento celular tipo SCReEBH.*
- *NOM-015-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Cables de fibras ópticas unimodo para uso interior.*
- *NOM-013-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Centrales telefónicas privadas digitales. Parte 3: Señalización.*
- *NOM-EM-012-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Centrales telefónicas privadas digitales. Parte 2: Transmisión.*
- *NOM-EM-011-SCT1-1993, NORMA Oficial Mexicana Emergente sobre Centrales telefónicas privadas digitales. Parte 1: Características generales.*
- *NOM-011-SCT1-1993, PROYECTO de Norma Oficial Mexicana sobre Centrales telefónicas privadas digitales. Parte 1: Características generales.*
- *NOM-010-SCT1-1993, PROYECTO de Norma Oficial Mexicana referente a la Norma NOM-I-212-1991, Módems dúplex a dos hilos que funcionan a velocidades binarias de hasta 9,600 bit/s para uso en la red telefónica pública conmutada y en circuitos arrendados de tipo telefónico.*
- *NOM-EM-009-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Interfaz de usuario a velocidad básica para la RDSI - Capa 1.*
- *NOM-EM-008-SCT1-1994, NORMA Oficial Mexicana Emergente sobre Centrales telefónicas privadas.*

- *NOM-005-SCT1-93, NORMA Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de sistemas de televisión por cable.*
- *NOM-005-SCT1-93, PROYECTO de Norma Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de sistemas de televisión por cable.*
- *NOM-004-SCT1-93, NORMA Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de sistemas destinados al servicio de música continua.*
- *NOM-003-SCT1-93, PROYECTO de Norma Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de estaciones de radiodifusión de televisión monocroma y a color (bandas VHF y UHF).*
- *NOM-002-SCT1-93, NORMA Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de estaciones de radiodifusión sonora en la banda de 88 a 108 MHz; con portadora principal modulada en frecuencia.*
- *NOM-001-SCT1-93, NORMA Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de estaciones de radiodifusión sonora moduladas en amplitud.*
- *PROYECTO de Norma Oficial Mexicana sobre Especificaciones y requerimientos para la instalación y operación de estaciones de radiodifusión sonora moduladas en amplitud.*

Otras normas y estándares

Éstos sólo los mencionaremos sin hacer ya ningún comentario:

- *Normas y estándares de diseño*
- *Normas y estándares de protocolos y comunicación*
- *Normas y estándares de seguridad informática*
- *Normas y estándares de software*

Control interno informático

5

Estructura del capítulo:

Objetivos del capítulo

Estudiar los conceptos y características fundamentales del control interno en los sistemas computacionales, a fin de identificar sus principales aplicaciones en la auditoría de sistemas, para entender cómo se pueden satisfacer, con eficiencia y eficacia, las necesidades de evaluación, razonabilidad y oportunidad en la protección y seguridad de los bienes, de la información y del personal del área de sistemas de una institución; también para el desarrollo de las actividades, operaciones y resultados obtenidos en el procesamiento de la información de las áreas de sistemas de la institución.

Todo ello con el propósito de comprender la importancia del control informático en las áreas de sistemas de las empresas, así como su uso en cada uno de los tipos de auditorías de sistemas para identificar los aspectos fundamentales de aplicación en la auditoría de sistemas de información.

Introducción del capítulo

Ya hemos destacado que el establecimiento del control interno en las empresas tiene como finalidad ayudarles en la evaluación de la *eficacia* y *eficiencia** de su gestión administrativa, resaltando su trascendencia a través de la adopción de los objetivos que se pretenden satisfacer con dicho control; recordemos los objetivos:

- *Establecer la seguridad y protección de los activos de la empresa.*
- *Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa.*
- *Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.*
- *Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.*
- *Implementar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.*

* **Eficaz**. Del latín ***efficax-acis***, de **efficiere**: Realizar, ejecutar... Efectivo... Que logra hacer efectivo un intento o propósito. **Eficiente**. Del latín ***efficiens***:... Capaz de lograr un efecto.... Que tiene facultades para producir determinado efecto o realizar una determinada tarea. ***Op. cit***. *Diccionario Etimológico*. Pág. 160 y *Diccionario Inverso*. Pág. 227

En el capítulo anterior también se destacó la influencia que tiene el *control interno* en la gestión administrativa de las empresas, así como su importancia en la protección de los bienes y en el buen desarrollo de las actividades y operaciones de las mismas.

Sin embargo, después de haber estudiado lo que aportan los prestigiados autores respecto al control interno, lo que pretendemos es enfocar este libro más hacia el control interno informático. Para hacer este análisis, propondremos los siguientes puntos como objetivos específicos del control interno informático:

- *Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.*
- *Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.*
- *Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.*
- *Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.*
- *Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.*

Tomando como punto de partida estos nuevos objetivos, a continuación analizaremos los elementos que se pueden aplicar como *control interno informático* en las áreas de sistemas:

Elementos fundamentales del control interno informático

- *Controles internos sobre la organización del área de informática.*
- *Controles internos sobre el análisis, desarrollo e implementación de sistemas.*
- *Controles internos sobre la operación del sistema.*
- *Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.*
- *Controles internos sobre la seguridad del área de sistemas.*

Como parte del presente estudio, a continuación se presenta un cuadro concentrado del control interno aplicable a la informática; posteriormente se detallarán cada uno de los elementos aquí propuestos.

Cuadro de control interno en el área de informática

Controles internos sobre la organización del área de informática

- *Dirección*
- *División del trabajo*
- *Asignación de responsabilidad y autoridad*
- *Establecimiento de estándares y métodos*
- *Perfiles de puestos*

Controles internos sobre el análisis, desarrollo e implementación de sistemas

- *Estandarización de metodologías para el desarrollo de proyectos*
- *Asegurar que el beneficio de los sistemas sea el óptimo*
- *Elaborar estudios de factibilidad del sistema*
- *Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas*
- *Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema*
- *Optimizar el uso del sistema por medio de su documentación*

Controles internos sobre la operación del sistema

- *Prevenir y corregir los errores de operación*
- *Prevenir y evitar la manipulación fraudulenta de la información*
- *Implementar y mantener la seguridad en la operación*
- *Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución*

Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados

- *Verificar la existencia y funcionamiento de los procedimientos de captura de datos*
- *Comprobar que todos los datos sean debidamente procesados*
- *Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos*
- *Comprobar la oportunidad, confiabilidad y veracidad en la emisión de los resultados del procesamiento de información*

Controles internos sobre la seguridad del área de sistemas

- *Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden en las áreas de sistematización*
- *Controles sobre la seguridad física del área de sistemas*
- *Controles sobre la seguridad lógica de los sistemas*
- *Controles sobre la seguridad de las bases de datos*
- *Controles sobre la operación de los sistemas computacionales*
- *Controles sobre la seguridad del personal de informática*
- *Controles sobre la seguridad de la telecomunicación de datos*
- *Controles sobre la seguridad de redes y sistemas multiusuarios*

5.1 Controles internos para la organización del área de informática

Al instalar este elemento del *control interno informático,* se busca determinar si la estructura de organización del área de sistemas computacionales, con todo lo que esto conlleva, es la más apropiada para que éstos funcionen con eficacia y eficiencia en la empresa; esto se logra mediante el diseño adecuado de la *estructura de puestos, unidades de trabajo, líneas de autoridad y canales de comunicación*, complementados con *la definición correcta de funciones y actividades, la asignación de responsabilidad y la definición clara de los perfiles de puestos*. Todo ello permitirá realizar adecuadamente el trabajo encomendado al área de sistemas de la empresa.

Para este elemento del control interno, dentro del área de informática de cualquier empresa, se proponen los siguientes subelementos de organización:

- *Dirección*
- *División del trabajo*
- *Asignación de responsabilidad y autoridad*
- *Establecimiento de estándares y métodos*
- *Perfiles de puestos*

5.1.1 Dirección

Como señalamos en los *elementos de organización* (inciso 4.3.1. del capítulo anterior), la dirección es uno de los subelementos básicos del control interno en cualquier empresa, ya que ésta es la función primordial de la entidad o persona que tiene la misión de dirigir las actividades en la institución o en un área específica, así como la de coordinar el uso de los recursos disponibles en el área para cumplir el objetivo institucional.

Lo anterior también se aplica a la *dirección* en el *control interno informático*, ya que el titular de la entidad, o persona responsable de dirigir el área de sistemas de la empresa, tiene la responsabilidad de ejercer la autoridad en la conducción de las funciones y actividades del personal de dicha área, así como en la coordinación de los recursos informáticos que le permitirán satisfacer los requerimientos de sistemas de la empresa.

La adopción de este subelemento en el área de informática de la empresa permitirá determinar de manera correcta los niveles de autoridad y responsabilidad que se necesitan en la estructura de organización del área de sistemas, con el fin de poder supervisar y evaluar el cumplimiento de las funciones y el buen desempeño de las actividades del personal asignado a esos puestos, con todo lo que esto implica en la gestión administrativa del área de sistemas.

Los recursos de informática son muy especializados y frecuentemente muy costosos, pero son de suma importancia en las áreas de sistemas; por lo tanto, es necesario aprovecharlos de la mejor manera posible, lo cual sólo se puede lograr mediante el establecimiento de la *dirección* como elemento del *control interno;* con ello se contribuye a la adecuada coordinación del uso y aprovechamiento de esos recursos computacionales.

Este subelemento estará apoyado a su vez por los siguientes subelementos:

- *La coordinación de recursos*
- *La supervisión de actividades*
- *La delegación de autoridad y responsabilidad*
- *La asignación de actividades*
- *La distribución de recursos*

Antes de iniciar el análisis de cada uno de los subelementos señalados, conviene destacar que su aplicación es fundamental para cualquier área de sistemas, debido a lo especializado del manejo de las áreas de sistemas, a la complejidad de sus actividades, al disímbolo volumen de funciones y a la diversidad de operaciones que se realizan en estas áreas.

También es de suma importancia hacer notar que para su óptima implementación, se deben considerar la configuración y las características del equipo de cómputo, el tamaño del área de sistemas y las particularidades del procesamiento establecidas en la empresa, las cuales, como es fácil de entender, difieren diametralmente en la forma de trabajar de un área de sistemas a otra y entre la forma de ejercer la dirección de sistemas de una empresa a otra.

Además, la importancia de la dirección se acentúa todavía más si a lo anterior le agregamos las diferencias que hay de un área de sistemas a otra respecto al hardware, software, instalaciones, información, personal y usuarios del sistema; pero se acentúa más si el sistema de la empresa es monousuarios, redes o multiusuarios.

Para un mayor entendimiento de este subelemento, conviene hacer el análisis de cada uno de los componentes básicos del subelemento de dirección.

5.1.1.1 La coordinación de recursos

Como parte fundamental de la dirección del área de sistemas, se tienen que asignar y distribuir de manera correcta los recursos informáticos disponibles en la empresa, con el fin de que dichos recursos sean más equitativos y productivos; por ejemplo, la coordinación del personal informático y de los usuarios, el tiempo y disponibilidad del uso de hardware, software e información que serán utilizados en la empresa, así como la coordinación general de las actividades necesarias para el adecuado procesamiento de datos en el área de sistemas.

5.1.1.2 La supervisión de actividades

Es la vigilancia que realiza quien dirige el área de sistemas, sobre la realización adecuada de las funciones y actividades que se tienen encomendadas en esta área, supervisando el trabajo que se realiza con los recursos informáticos de la empresa. Su propósito es evaluar el cumplimiento adecuado de los objetivos del área de sistemas, así como el procesamiento oportuno, correcto y confiable de la información de la empresa.

5.1.1.3 La delegación de autoridad y responsabilidad

Para el buen funcionamiento de cualquier área de sistemas, es indispensable hacer una distribución adecuada de los límites de autoridad y responsabilidad, tanto a los puestos de mayor como de menor jerarquía. Su finalidad es obligar al personal del área, de acuerdo con la delegación de autoridad y responsabilidad, a cumplir con las tareas, funciones y operaciones que tienen encomendadas.

Recordemos que un principio fundamental de la organización en la ciencia de la administración, es que *la autoridad se delega a los subordinados, pero la responsabilidad se comparte entre todos los integrantes del área de sistemas.*

5.1.1.4 La asignación de actividades

Este subelemento se aplica cuando la dirección instituye una definición clara y concreta de todas las funciones, tareas y operaciones de cada puesto, con el fin de cumplir de manera adecuada con los objetivos del área de sistemas. Con ello se busca garantizar el procesamiento adecuado de la información en la empresa; por esta razón, se tienen que diseñar, lo más correctamente posible, las actividades de cada uno de los puestos que integran la estructura de organización del área de sistemas.

5.1.1.5 La distribución de recursos

Es la asignación que se hace de los recursos informáticos disponibles en el área de sistemas, con el propósito de que los empleados de esta área cumplan eficientemente con las actividades y tareas que tienen encomendadas; con ello se buscan la equi-

dad y disponibilidad necesarias que respalden el cumplimiento de las funciones de los centros de cómputo, así como el mejor procesamiento de la información de la empresa.

5.1.2 División del trabajo

Como vimos en el capítulo anterior, para el buen desarrollo de las actividades de cualquier empresa es necesario que éstas se realicen de acuerdo a como hayan sido diseñadas en la estructura de organización y de acuerdo con lo delimitado en el perfil de puestos; sin embargo, esto sólo se logra cuando se tiene una distribución correcta de las cargas de trabajo en el área de sistemas, una asignación eficiente de sus funciones y, básicamente, una división adecuada de las actividades que tiene encomendadas cada unidad de trabajo.

Cabe recordar que desde la época de **Taylor** y **Fayol** se ha buscado constantemente hacer una división más efectiva del trabajo en cada una de las áreas de las empresas, ya que es creciente la necesidad de una segmentación de trabajos más eficiente y eficaz; por esta razón, las actividades se dividen en áreas cada vez más especializadas, a tal grado que las labores se han pulverizado en tareas muy concretas y específicas, buscando con esto una mayor especialización.

Es fácil apreciar que *la división del trabajo incrementa la eficacia y eficiencia de las actividades de cualquier empresa.* Esto mismo ocurre en las áreas de sistemas, en donde, por las mismas exigencias de operación de los sistemas computacionales, los cuales son cada vez más especializados, se requiere una división más especializada del trabajo para el cumplimiento de las actividades, operaciones y tareas que se desarrollan en estos centros de cómputo. Cada vez se requiere más que los especialistas en informática realicen sus actividades de manera más concreta, sofisticada y delimitada, dentro de un ramo específico de especialidad. Claro está, dicha especialización debe estar soportada por un amplio conocimiento y experiencia en el ambiente de sistemas, además de una perfecta coordinación con los otros recursos del área de sistemas.

En atención a esto y con el propósito de hacer más claro el entendimiento y la importancia de este subelemento de la organización, a continuación se presentan las funciones básicas de cualquier centro de cómputo:

- *Dirección general del área de informática*
- *Área de análisis y diseño*
- *Área de programación*
- *Área de sistemas de redes*
- *Área de operación*
- *Área de telecomunicación*
- *Área de administración*

5.1.2.1 Dirección general del área de informática

Aunque parece una repetición del elemento anterior, conviene aclarar que ésta es la entidad encargada de integrar, coordinar y supervisar el buen desarrollo de las funciones y actividades de los demás recursos del área; también es la entidad encargada de planear, organizar, dirigir y controlar los objetivos, programas y presupuestos de los recursos asignados al área de informática. En sí, quien ejerce esta función tiene la responsabilidad de utilizar los demás recursos informáticos para cumplir el objetivo del área de sistemas.

5.1.2.2 Área de análisis y diseño

Es la unidad de trabajo encargada de estudiar las necesidades de procesamiento e información de la empresa, así como de proponer mejoras y cambios en el desarrollo de nuevos sistemas, por medio de las metodologías de análisis y diseño de éstos.

5.1.2.3 Área de programación

Sus integrantes son los responsables de realizar todas las actividades y operaciones que se requieren para codificar adecuadamente los programas, a fin de lograr el buen funcionamiento del área de cómputo en la empresa, de acuerdo con las necesidades del usuario y los resultados del análisis de los sistemas. Por lo general, estos requerimientos de programas siguen las especificaciones del diseño de nuevos sistemas, así como las del hardware, software, bases de datos e información de dicha área.

5.1.2.4 Área de sistemas de redes

Es el área que está destinada a la administración y control de los sistemas de redes; algunas de sus funciones son la configuración, manejo y mantenimiento de dichos sistemas, a fin de satisfacer las necesidades de cómputo de la empresa.

5.1.2.5 Área de operación

Como su nombre lo indica, es el área encargada de realizar la operación, procesamiento y uso de los sistemas computacionales, así como de la asignación de sus recursos íntegros para servicio de los usuarios y de las áreas de la empresa.

5.1.2.6 Área de telecomunicación

Es la unidad administrativa responsable de llevar a cabo todos los servicios de comunicación, interna o externa, del sistema, ya sea dentro del propio centro de cómputo a través de interconexiones, redes de comunicación o de cualquier otro sistema, o con otras entidades similares a través de sistemas de comunicación externos, tales como

redes MAN, WAN, Internet, fax-módem, teleconferencia, teleprocesamiento de información o de cualquier otro dispositivo de comunicación.

5.1.2.7 Área de administración

Es la unidad que se encarga de brindar todo el apoyo de tipo administrativo que requiere el centro de cómputo, a fin de que pueda realizar, con eficiencia y eficacia, todas sus funciones.

El estudio de esta propuesta generalizada de actividades del área de sistemas nos permite tener una visión más clara de la necesidad de hacer una división de trabajo dentro de un centro de cómputo; al hacer esta división se tienen que asignar a cada puesto las funciones y actividades que son inherentes a su especialización; dichas asignaciones se realizan en forma independiente, pero coordinada con los demás recursos. Con ello se coadyuva a la mejor realización de sus funciones para el cumplimiento del objetivo general del área de sistemas. Esto, por sí mismo, nos señala la importancia que tiene la división del trabajo en las áreas de sistemas y, por ende, lo fundamental que es el establecimiento de este subelemento del control interno.

Cabe aclarar que la propia necesidad del procesamiento de la empresa, el tamaño del área de informática, la configuración y recursos del sistema computacional, así como la disponibilidad de recursos humanos del propio centro de sistemas, serán determinantes para dividir el trabajo de este centro de cómputo y para la correcta aplicación de este subelemento de organización.

5.1.3 Asignación de responsabilidad y autoridad

Una vez estructuradas la división de actividades y funciones para cada uno de los integrantes del centro de cómputo, el siguiente subelemento a considerar es la asignación de las líneas de autoridad por puesto y el establecimiento de los límites de responsabilidad que tendrá cada uno de éstos, incluyendo los canales formales de comunicación.

Este subelemento nos ayuda a garantizar la eficiencia y eficacia del control interno en las unidades de sistemas, ya que complementa la división del trabajo y delimita claramente la autoridad y la responsabilidad que tendrá cada integrante de esas áreas. Con ello se asegura el mejor desarrollo de las actividades, funciones y tareas y, consecuentemente, la realización del procesamiento de información en la empresa será más eficiente y más eficaz.

Recordemos que en el trabajo especializado de sistemas, es muy común que los integrantes de estas áreas sientan que deben o tiendan a realizar todo tipo de actividades relacionadas con sistemas, aunque éstas no les correspondan, debido a que sus funciones están perfectamente establecidas por la división del trabajo. *Un vicio muy común de quienes trabajamos en sistemas*. Por esta razón, es de suma importancia establecer, lo más claro y preciso posible, el límite de acción de este personal.

5.1.4 Establecimiento de estándares y métodos

En cualquier área de sistemas es de suma importancia estandarizar el desarrollo de todas las actividades y funciones, a fin de que éstas se realicen de manera uniforme conforme a las necesidades concretas de las unidades de informática que integran la empresa. Claro está, en esta estandarización se deben respetar la división del trabajo y la asignación de actividades específicas. Éste es un aspecto básico que se debe contemplar para el establecimiento del control interno informático en cualquier empresa.

Lo anterior es muy importante para el buen desempeño de las funciones en todas las áreas de informática, ya que se deben establecer, de manera uniforme y homogénea, todos aquellos procedimientos y metodologías informáticas que permitan estandarizar la operación de los sistemas, así como el desarrollo de nuevos sistemas computacionales; esto obedece a que dichos sistemas requieren que se capturen, procesen y emitan resultados uniformes.

Además, debido a lo especializado de las actividades que se desarrollan en los centros de cómputo, se tienen que adoptar metodologías y procedimientos similares en cuanto a la estandarización de los métodos, procedimientos y las herramientas que integran los sistemas computacionales de una empresa, concretamente para:

- *Estandarización del diseño e instalación del hardware, así como del uso de sus componentes, procesadores, equipos periféricos y de su arquitectura.*
- *Estandarización del diseño, adquisición y uso del software, así como de lo relacionado con el aprovechamiento de sus sistemas operativos, sus programas de aplicación y sus métodos de procesamiento, los lenguajes de programación, los programas y paqueterías para desarrollo y su aplicación en los sistemas de la empresa.*
- *Estandarización del diseño, implementación y administración de las bases de datos, en las cuales se maneja la información de los sistemas computacionales de la empresa, así como el respaldo y la protección de datos.*
- *Estandarización del diseño, instalación y aprovechamiento de los sistemas de redes y sistemas multiusuarios que se tengan instalados en la empresa, incluyendo la configuración, el hardware, el software, la información y los demás recursos de la red.*
- *Estandarización del mantenimiento y de la modificación parcial o total de los sistemas informáticos de la empresa, con el fin de obtener un mejor aprovechamiento en el procesamiento de la información.*
- *Estandarización de los sistemas de seguridad y protección al personal y usuarios de sistemas, información, bases de datos, hardware, software, mobiliario y equipo, así como de todos los aspectos relacionados con el sistema de cómputo de la empresa.*

La adopción de los anteriores subelementos del control interno de sistemas nos ayudará a garantizar que la realización de sus actividades y cumplimiento de sus funciones será más eficiente y eficaz, desde el punto de vista de la estructura de organización de los centros de cómputo.

5.1.5 Perfiles de puestos

Otro aspecto fundamental para la adopción de este elemento del *control interno informático*, es que nos ayuda a identificar y establecer los requisitos, habilidades, experiencia y conocimientos específicos que necesita tener el personal que ocupa un puesto en el área de sistemas.

Para cumplir con estos requisitos, se debe contemplar, dentro de *un perfil de puestos,* cada una las características que deben poseer quienes ocupen los puestos que integran la estructura de organización del centro informático de la empresa, incluyendo la breve descripción de las funciones sustantivas que tienen que desarrollar, así como sus líneas de autoridad. Es una condición indispensable que cada uno de esos puestos se establezca lo más apegado posible a las necesidades de servicios.

Enseguida se presentan los requerimientos de un perfil de puestos básicos para un centro informático, con el propósito de que sirva de referencia al auditor para evaluar la selección del personal que ocupa esos puestos y, en algunos casos, su desempeño.

Sin embargo, aunque la existencia de este documento (el perfil de puestos) es fundamental para el control interno informático, a veces quienes dirigen las áreas de sistemas dejan de utilizarlo, debido a que no es fácil definir los perfiles de puestos de un centro de cómputo, o porque desconocen su utilidad o simplemente porque ignoran la importancia de considerar en su diseño los siguientes aspectos:

- *La forma de operación establecida para cada puesto, de acuerdo con los sistemas de cómputo de la empresa.*
- *Las necesidades de procesamiento de datos, desde la captura hasta la emisión de resultados.*
- *La configuración de los equipos, instalaciones y componentes del área de sistemas, incluyendo su arquitectura y la forma de administración de los mismos.*
- *La manera como influye esta delineación en el uso de los recursos informáticos, tanto del hardware y software como de los recursos técnicos de comunicación y del propio factor humano informático especializado.*

Como podemos observar, con el perfil de puestos se pretende estandarizar, hasta donde es posible, los requisitos mínimos que se deben contemplar para cada uno de los puestos del centro informático, aunque esto parezca muy sofisticado para las áreas de sistemas, mismas que difieren de una a otra por lo especializado de las actividades, características y especificaciones de los sistemas computacionales utilizados para el procesamiento de información de la empresa. Por lo tanto, también sus perfiles de puestos diferirán entre sí.

Es trascendental destacar la importancia del uso del perfil de puestos para la selección adecuada del personal que ocupará los puestos dentro del área de sistemas, debido a que en ese documento se establecerán en forma precisa y correcta las características, conocimientos y habilidades que deberán tener quienes ocupen dichos puestos. Esto será la garantía de un desarrollo eficiente y eficaz de las funciones y actividades de cada puesto.

5.1.5.1 Contenido del perfil de puestos

En el perfil de puestos, en su forma clásica, se deben contemplar como mínimo los siguientes puntos, los cuales se deben adecuar a las necesidades específicas del propio puesto:

Contenido básico de un perfil de puestos

- Nombre genérico del puesto
- Objetivo del puesto
- Líneas de autoridad:
  - *Dependencia de... y responsabilidad sobre*
- Funciones del puesto
  - *Sustantivas, básicas o fundamentales*
  - *Específicas, concretas o cotidianas*
- Requisitos del puesto:
  - *Conocimientos*
    - *En sistemas*
    - *En áreas similares*
  - *Otros conocimientos del puesto*
- Experiencia
  - *En el puesto*
  - *En el área*
- Características de personalidad
- Otros requerimientos
- Otros conocimientos

5.2 Controles internos para el análisis, desarrollo e implementación de sistemas

Si buscamos encontrar alguna semejanza entre los elementos del control interno que estudiamos en el capítulo anterior y el elemento del control interno informático que a continuación analizaremos, será difícil que podamos establecer algún tipo de similitud

entre ambos, ya que las actividades tan especializadas que se realizan para el análisis, diseño, desarrollo e implementación de sistemas de cualquier empresa son únicas y, por lo tanto, no tienen parecido alguno con otras actividades. Por esta razón, merecen un tratamiento más especializado en su exposición.

Para entender este elemento del control interno informático, es vital que primero presentemos las principales fases de lo que se puede entender como análisis y diseño de sistemas. Para ello, proponemos como modelo la metodología general para el desarrollo de sistemas, misma que utilizaremos para ejemplificar los elementos del control interno, considerando los siguientes puntos:

- *Análisis del sistema actual*
- *Diseño conceptual*
- *Diseño detallado*
- *Programación*
- *Pruebas y correcciones*
- *Documentación del sistema*
- *Capacitación de usuarios*
- *Implementación del sistema*
- *Liberación del sistema*
- *Mantenimiento*

El uso de esta metodología, la cual sólo presentamos en sus principales fases, requiere un seguimiento paso a paso, y un uso casi irrestricto de todas sus fases y de cada una de las etapas que las integran. Con la aplicación de esta metodología para el desarrollo de un proyecto, se puede garantizar el análisis, desarrollo e implementación correctos de cualquier sistema.

Esta metodología sólo se utiliza como ejemplo aplicable al desarrollo de un sistema, enfatizando que, para cumplir con este elemento del control interno informático, es necesario utilizar alguna de las metodologías propuestas por Kendal, Senn, Fitzgerald, Murdick o Roos, la ingeniería de sistemas, la programación orientada a objetos o cualquier otra metodología. Para desarrollar un proyecto de sistemas, es indispensable aplicar un método irrestricto que señale, paso a paso, las etapas requeridas para dicho desarrollo. Es decir, una metodología de sistemas.

A continuación se proponen los siguientes subelementos para el cumplimiento de este elemento del control interno en el área de sistemas:

Estandarización de metodologías para el desarrollo de proyectos

- *Asegurar que el beneficio del sistema sea óptimo*
- *Elaborar estudios de factibilidad del sistema*
- *Garantizar la eficiencia y eficacia en el análisis y diseño del sistema*
- *Vigilar la efectividad y eficacia en la implementación y el mantenimiento del sistema*
- *Lograr un uso eficiente del sistema por medio de su documentación*

5.2.1 Estandarización de metodologías para el desarrollo de proyectos

Para obtener el máximo beneficio en la aplicación de recursos de un sistema de información, tanto en lo relacionado con el análisis y diseño de sistemas como en las demás actividades que se realizan en un centro de cómputo, es necesario homologar y estandarizar dichas actividades.

Para esto, es necesario establecer que existen múltiples metodologías de aplicación general para el desarrollo de sistemas propuestas por diversos autores, desde las establecidas formalmente en libros y documentos editados, hasta las informales que se utilizan en forma local para el desarrollo de proyectos internos, pero la empresa debe adoptar alguna en especial que sea acorde al desarrollo de sus proyectos de sistemas. También puede elegir alguna metodología híbrida que sea combinación de las anteriores.

La aplicación de una metodología estandarizada para el desarrollo de un proyecto informático garantiza la uniformidad en la aplicación de cualquier sistema y contribuye en gran medida a la máxima eficiencia en el uso de los recursos informáticos del área de sistemas; por esta razón, es de suma importancia estandarizar el desarrollo de los proyectos de sistemas en una empresa. Precisamente esto es lo que se busca con la implementación de este subelemento del control interno para el área de sistemas, estandarizar su desarrollo.

Actualmente existen muchas instituciones que crean sistemas, y dentro de las principales actividades que realizan para el desarrollo de los mismos está la estandarización de normas, políticas y lineamientos que regulen la realización de dichos sistemas en la empresa, buscando con ello uniformar el crecimiento de éstos. Sin embargo, también existen muchas otras instituciones que carecen de cualquiera de estas estandarizaciones. Incluso existen aquellas que jamás aplican una metodología uniforme y que utilizan diferentes métodos para desarrollar sus proyectos; por esta razón, sus sistemas no son similares y sus aplicaciones y utilidad para la empresa frecuentemente difieren, debido a que no tienen los mismos estándares, ni las mismas normas, políticas ni lineamientos.

Está claro que es indispensable contar con un elemento de control que regule el desarrollo correcto de un proyecto, ya que este control es el sustento indispensable para estandarizar la realización de cualquier proyecto informático; con esto se contribuye a la máxima eficiencia en la realización de dicho proyecto.

Para conocer los principales puntos que se deberán analizar durante una auditoría de sistemas, en cuanto al desarrollo de proyectos informáticos, a continuación se presentan las estandarizaciones básicas que se deben analizar durante cualquier revisión.

5.2.1.1 Estandarización de métodos para el diseño de sistemas

Consiste en uniformar los métodos y procedimientos establecidos en la unidad de sistematización, a fin de estandarizar el desarrollo de los sistemas, de tal manera que los nuevos proyectos se realicen siempre de la misma manera.

5.2.1.2 Lineamientos en la realización de sistemas

Así como es necesario estandarizar los métodos y procedimientos, también es indispensable establecer formalmente las líneas concretas de acción, las cuales delimitarán, lo más claramente posible, las normas de conducta que deben acatar quienes desarrollen proyectos en la empresa.

5.2.1.3 Uniformidad de funciones para desarrollar sistemas

Para el desarrollo uniforme de los nuevos sistemas en la empresa, también es necesario uniformar las funciones que deben cumplir los encargados de realizar estos proyectos en el área de sistematización; con ello se busca que siempre se desarrollen las mismas actividades para realizar nuevos proyectos; sólo así se garantiza la uniformidad de sistemas en la empresa.

5.2.1.4 Políticas para el desarrollo de sistemas

Para el desarrollo uniforme de los proyectos de sistemas, es obligatorio establecer políticas (*normas de acción que regulan la toma de decisiones*), a fin de que los encargados de realizar los proyectos de sistemas en la empresa sigan las mismas directrices señaladas por la dirección de la empresa y por la del área de sistematización.

5.2.1.5 Normas para regular el desarrollo de proyectos

Entendiendo que las normas son las directrices que marcan la conducta que deben seguir quienes laboran en la institución, para el desarrollo de proyectos son los lineamientos formales que regulan la manera de conducirse por parte de quienes desarrollan los proyectos; con ellas se establece perfectamente la conducta que deberán seguir los usuarios y quienes participan en dicho desarrollo.

Los aspectos anteriores servirán de ejemplo para establecer las estandarizaciones que se requieren para el desarrollo de sistemas, según las necesidades y características de los mismos en la empresa.

5.2.2 Asegurar que el beneficio del sistema sea óptimo

Con la aplicación de este subelemento del control interno, se pretende buscar la optimización de las tareas, operaciones y funciones que resultarán con la implementación de los sistemas; contando para ello con el seguimiento de una metodología uniforme para el desarrollo de nuevos sistemas, con lo cual se pretende garantizar la eficacia y eficiencia de acciones después de que se implemente el nuevo sistema.

Al implementar un nuevo sistema se busca optimizar el desarrollo de las actividades que normalmente se llevan a cabo en la empresa o en cualquiera de sus áreas; con

ello se pretende mejorar las operaciones normales de cómputo que se realizan en la empresa, a fin de incrementar la eficiencia y eficacia de sus sistemas actuales.

Cabe aclarar que la optimización del sistema no se refiere exclusivamente a las aplicaciones informáticas, sino también a la optimización del equipo con el cual se desarrolla su función informática; por ejemplo, los proyectos de elección del software, hardware, periféricos asociados, bases de datos o consumibles, o las demás actividades que rodean a la gestión administrativa del sistema, así como el manejo, adiestramiento y capacitación de los usuarios del sistemas o de las personas que intervienen en la operación normal del mismo. En todos los casos, con la adopción de este subelemento se pretende hacer más eficiente y eficaz el desarrollo de las actividades actuales del sistema; sin este objetivo no se justifica el desarrollo de un nuevo sistema.

De hecho, el objetivo final que se espera en las empresas con la implementación de un sistema informático se puede circunscribir a dos aspectos concretos.

Beneficios tangibles

Con el establecimiento de los sistemas en la empresa se pretende lograr mejoras sustanciales, realmente palpables, por parte de quienes utilizan dichos sistemas, lo cual exige que puedan ser cuantificados resultados tales como una mayor emisión de facturas en la empresa, más y mejores registros contables por jornada, mayor emisión de cheques de nómina en menor tiempo, mejor captura y proceso de impuestos vía sistemas, etcétera. Todos estos resultados son tangibles, debido a que se pueden cuantificar para determinar si se cumple o no con los objetivos esperados del sistema.

Beneficios intangibles

Los beneficios que se espera obtener de los sistemas de cómputo son intangibles, ya que sus resultados no pueden ser contados ni se ven en forma física ni palpable; sin embargo, existen formas de hacer su cuantificación, esto es: la mayoría de los sistemas computacionales tienen ciertos valores cualitativos y es muy difícil darles un valor cuantitativo. Entre los principales ejemplos encontramos la oportunidad en la toma de decisiones con ayuda de los sistemas computacionales, la confiabilidad en los resultados de las nóminas, la veracidad de las operaciones realizadas con sistemas computacionales, etcétera.

Un aspecto específico de aplicación de este subelemento, es que para el análisis y diseño del nuevo sistema se tienen que establecer, de manera clara y los más concretamente posible, todos los beneficios que se obtendrían con el desarrollo de un sistema, enfocándolos desde múltiples puntos de vista; los siguientes son algunos de estos beneficios:

- ***El nivel informático,*** *porque con la instalación de un nuevo proyecto se pretende mejorar los sistemas informáticos de la empresa.*
- ***El económico,*** *debido a que los sistemas tienen un valor económico y con su desarrollo se pretende economizar el servicio informático en las empresas.*
- ***El social,*** *porque congrega gente alrededor de los sistemas que se implementan en las empresas; esta gente se interrelaciona con sus congéneres, creando vínculos sociales con ellos, con la ayuda de los sistemas.*

- ***El de los servicios,*** *porque el propósito final de un sistema computacional es proporcionar servicios sistematizados a las áreas de una empresa.*
- ***El administrativo,*** *ya que ayuda al mejor manejo de la gestión informática de las empresas.*
- ***El operacional,*** *porque con su adopción ayuda a la regulación y mejor realización de todas las operaciones del sistema computacional de la empresa.*

Dentro del análisis de los beneficios que se esperan de un sistema, también se deben contemplar las ventajas y desventajas que se pueden obtener con el desarrollo e implementación del nuevo sistema. Se debe realizar una valoración cuantitativa y cualitativa de todos los factores que intervienen en el desarrollo del proyecto, sin perder de vista que el objetivo final de todo proyecto de sistemas es optimizar las actividades de procesamiento de información de la empresa.

5.2.3 Elaborar estudios de factibilidad del sistema

En los puntos anteriores se señaló la necesidad de estandarizar el desarrollo de los proyectos con el fin de obtener el máximo beneficio con el desarrollo de un nuevo sistema; sin embargo, dentro de un plano más concreto, en cuanto al análisis y diseño de sistemas, todo proyecto de informática se tiene que evaluar desde dos puntos de vista específicos: *la viabilidad y la factibilidad*; es decir, se deben analizar la *viabilidad* de realizar el proyecto y la *factibilidad* de llevarlo a cabo. En estos factores se deben contemplar, cada uno por separado, los puntos de vista *operativo, económico, técnico y administrativo* para poder valorar la optimización del nuevo sistema. Antes de continuar, conviene volver a definir los siguientes conceptos:

Viable:

"Del francés ***viable****, de* vie*: existencia, vida. Que puede realizarse."*[1]

"Adjetivo, que puede vivir. Se dice del asunto con posibilidad de salir adelante."[2]

Factible:

"Del latín ***factibilis****, de* facere*: hacer - hacedero, posible."*[3]

"Que se puede llevar a cabo o que es posible realizar. Realizable, posible, asequible."[4]

Con las anteriores definiciones podemos inferir que para el desarrollo de un nuevo sistema, dentro de su fase de análisis, se deben evaluar a conciencia todos aquellos aspectos que permitan determinar la posibilidad de llevar a cabo el proyecto, apoyándose en su valoración mediante los estudios ***viabilidad*** *(valorar la posibilidad de hacerlo) y* ***factibilidad*** *(valorar si se puede realizar),* considerando los enfoques antes citados. El resultado final de estas valoraciones será la certificación y confianza de que el proyecto será aplicable a las necesidades de la empresa para así poder satisfacer sus requerimientos de control interno de informática.

Un aspecto fundamental que se debe contemplar en la adopción de este subelemento del control interno informático, es determinar el orden en la valoración del desarrollo de los proyectos: *en primer lugar,* se deben elaborar los estudios acerca de la viabilidad de realizar el proyecto y *en segundo término* los de la factibilidad de llevarlo a cabo, ambos enfocados desde los siguiente puntos de vista.

5.2.3.1 Viabilidad y factibilidad operativa

Son los estudios de viabilidad y factibilidad de aquellos aspectos que se refieren a la posible operación del proyecto; en esta parte se estudian anticipadamente todos los aspectos relacionados con la futura operación del sistema que será implementado, con el fin de lograr la adecuada operatividad del mismo.

5.2.3.2 Viabilidad y factibilidad económica

Son los estudios de viabilidad y factibilidad de aquellos aspectos que se refieren a la parte económica del proyecto; en esta parte se estudian anticipadamente todos los aspectos relacionados con el costo –*el beneficio y el gasto-rendimiento del proyecto*.

5.2.3.3 Viabilidad y factibilidad técnica

Son los estudios de viabilidad y factibilidad de aquellos aspectos que serán útiles para valorar la calidad y cualidad de los sistemas desde el punto de vista técnico; con ello se busca contribuir a la mejor operación del nuevo sistema; también se estudian otras calificaciones y cuantificaciones referentes a la parte técnica del proyecto, las cuales se deben hacer durante esta fase de análisis y desarrollo.

5.2.3.4 Viabilidad y factibilidad administrativa

Son los estudios de viabilidad y factibilidad de aquellos aspectos que repercuten en la cuestión administrativa del sistema, los cuales permitirán evaluar las facilidades para la futura administración del mismo.

5.2.3.5 Otros estudios de Viabilidad y factibilidad

Los anteriores son algunos de los principales estudios de factibilidad y viabilidad que se pueden realizar, aunque también existen otros tipos de estudios, los cuales estarán delimitados por las propias necesidades de la empresa en donde se lleven a cabo los proyectos de sistemas; sin embargo, para conocimiento del lector, sólo mencionaremos algunos de los más usuales:

- *Estudios de viabilidad y factibilidad de tipo* ***legal***
- *Estudios de viabilidad y factibilidad de tipo* ***laboral***

- *Estudios de viabilidad y factibilidad de* ***comunicación y telecomunicaciones***
- *Estudios de viabilidad y factibilidad de* ***localización de planta***
- *Estudios de viabilidad y factibilidad de* ***estudios de mercado***
- *Estudios de viabilidad y factibilidad de* ***instalaciones y equipamiento de los sistemas***
- *Estudios de viabilidad y factibilidad de* ***comercialización de los sistemas,*** *etcétera.*

Con el análisis de estos elementos podemos comprender la utilidad del control interno informático en el desarrollo de los proyectos de sistemas computacionales; por cierto, es indispensable realizar dichos proyectos para incrementar la eficiencia y eficacia de los sistemas de la empresa; claro está, adaptándose a las necesidades de la misma.

5.2.4 Garantizar la eficiencia y eficacia en el análisis y diseño del sistema

Para examinar este subelemento del control interno informático, es necesario entender que la premisa fundamental del análisis y diseño de sistemas es la realización de proyectos que optimicen las actividades que se desarrollarán con la implementación de un nuevo sistema computacional; además, debemos entender que un nuevo proyecto sólo se justifica si con él se busca satisfacer la *eficiencia y eficacia* de las actividades de la empresa, lo cual, por cierto, se logra por medio de la adopción de una metodología estándar en la realización de los sistemas. Esto es lo que se debe contemplar para poder garantizar un buen resultado final con su implementación.

Debemos señalar que si estas condiciones no se cumplen o sólo se satisfacen de manera parcial, entonces no tiene caso la existencia de un nuevo proyecto, ya que su consecuencia será muy pobre y deficiente, en cuanto a los resultados esperados.

Para garantizar esa *eficiencia* y *eficacia* en la implementación de un nuevo sistema, es necesario contar con varias herramientas, técnicas, métodos y elementos que permitan uniformar los procedimientos, estándares, normas y lineamientos requeridos para desarrollar eficientemente estas actividades.

Estos son sólo algunos de los muchos aspectos que se deben contemplar para un nuevo proyecto y deben ser adoptados en función a la metodología utilizada. Sin embargo, con el propósito de enfatizar la importancia de este subelemento, a continuación citaremos algunos ejemplos aplicables al mismo.

5.2.4.1 La adopción y seguimiento de una metodología institucional

Es necesario que en la empresa se establezca y se lleve a cabo una metodología única para el desarrollo de proyectos, a fin de que ésta sea de aplicación uniforme en toda la institución; esto se hace con el fin de uniformar las actividades de análisis y diseño de los sistemas. Con ello se consigue la estandarización de la eficiencia y eficacia de los nuevos sistemas.

5.2.4.2 Adoptar una adecuada planeación, programación y presupuestación para el desarrollo del sistema

Para llevar a cabo un nuevo proyecto informático, se debe partir del claro entendimiento de los objetivos que se pretenden con su realización, a fin de satisfacer la eficiencia y eficacia de los sistemas informáticos; una vez establecidos dichos objetivos, el siguiente paso es una eficiente planeación de los eventos y las actividades que se realizarán para alcanzarlos, a las cuales se les asignan recursos y tiempos por medio de la programación y, finalmente, se valora el costo de esos recursos mediante la presupuestación del proyecto.

Esto es la planeación de proyectos, una de las herramientas más útiles para garantizar la eficiencia y eficacia de los sistemas computacionales.

5.2.4.3 Contar con la participación activa de los usuarios finales o solicitantes del nuevo sistema para garantizar su buen desarrollo

Para lograr la *eficiencia* y *eficacia* de un proyecto, es indispensable que en su desarrollo se tenga la participación activa de los usuarios del sistema, ya que ellos serán quienes determinen y valoren los requerimientos específicos del nuevo proyecto, para así diseñar correctamente las acciones a seguir para su consecución. Sin la participación activa del usuario, los resultados del proyecto serían deficientes o limitados.

5.2.4.4 Contar con personal que tenga la disposición, experiencia, capacitación y conocimientos para el desarrollo de sistemas

Para lograr la eficiencia y eficacia en el desarrollo de sistemas, también es necesario que el personal involucrado en el desarrollo del proyecto tenga las calificaciones necesarias en cuanto a experiencia y conocimientos para el buen desarrollo de proyectos informáticos, además de una probada capacidad para entender las necesidades de los usuarios y proyectarlas en el nuevo sistema; también debe tener los conocimientos suficientes en sistemas computacionales, así como la disposición de carácter y ánimo para poder realizar lo anterior.

5.2.4.5 Utilizar los requerimientos técnicos necesarios para el desarrollo del sistema, como son el hardware, software y personal informático

Este punto se refiere a los elementos especializados en informática que se requieren para llevar a cabo los proyectos de sistemas de la empresa; en dichos proyectos se toman en cuenta las características y requerimientos específicos de los sistemas compu-

tacionales, tales como velocidad y tipo de procesamiento, componentes del sistema, sistema operativo, lenguajes y programas de desarrollo, etcétera.

5.2.4.6 Diseñar y aplicar las pruebas previas a la implementación del sistema

Este punto se refiere a la necesidad de elaborar todo tipo de pruebas antes de liberar el sistema, las cuales pueden ser desde pruebas de escritorio, pasando por pruebas con datos ficticios, hasta aquellas pruebas que se realizan en paralelo. Lo importante es examinar previamente el comportamiento del nuevo proyecto antes de implementarlo; con esto se garantiza su eficiencia y eficacia.

5.2.4.7 Supervisar permanentemente el avance de actividades del proyecto

La aplicación de todos y cada uno de los aspectos anteriormente señalados, tiene como fin lograr la eficiencia y eficacia en el desarrollo de un proyecto; estos aspectos se complementan con una permanente y estrecha supervisión de todas y cada una de las actividades que se realizan durante el desarrollo del proyecto, desde la etapa de conceptualización hasta la etapa de liberación. Cumpliendo lo anterior, se puede garantizar la utilidad de este subelemento del control interno informático.

Éstas son algunas de las consideraciones mínimas que se deben tomar en cuenta para la búsqueda de la *eficiencia y la eficacia en el desarrollo de los proyectos*. Las condiciones aquí citadas fueron sólo a nivel de ejemplo, ya que en su aplicación real mucho dependerán de las características y requerimientos de cada área de sistemas.

5.2.5 Vigilar la efectividad y eficiencia en la implementación y mantenimiento del sistema

Así como es necesario buscar la optimización del sistema y adoptar medidas que garanticen la eficacia y eficiencia en su desarrollo, también es necesario vigilar la efectividad en la implementación del sistema y, una vez liberado, también se debe procurar su eficiencia a través del mantenimiento. No basta con elaborar el sistema, también se tiene que implementar totalmente, se tiene que liberar a cargo del propio usuario y se le tiene que dar un mantenimiento permanente para garantizar su efectividad. Sólo mediante la adopción de este subelemento del control interno se pueden garantizar la eficacia y eficiencia de los sistemas computacionales de la institución.

Dentro de una aplicación real de sistemas, encontramos que la vida estimada de un proyecto informático es de seis a ocho años,* por esa razón es de suma importancia no

* Estadísticas realizadas por alumnos del seminario de titulación y auditoría de sistemas, entre 1990 y 1996, en la Universidad del Valle de México, planteles Lomas Verdes y San Rafael.

sólo desarrollar eficientemente el análisis y diseño del nuevo sistema, sino también implementarlo de manera adecuada, así como darle un constante mantenimiento, ya sea de carácter preventivo o correctivo. Esto último es básico para el funcionamiento del sistema, ya que se busca adaptarlo a las necesidades cambiantes del propio proyecto o de la institución y así evitar su rápida obsolescencia.

La adopción de este subelemento del control interno ayudará a garantizar la implementación adecuada y el mejor funcionamiento de los nuevos sistemas de información, y quizá también pueda ayudar a evaluar su correcto funcionamiento posterior. El mantenimiento periódico, sea preventivo o correctivo, será el complemento que garantice la eficiencia y eficacia del sistema.

5.2.6 Lograr un uso eficiente del sistema por medio de su documentación

Después de haber terminado el desarrollo del sistema, o durante su elaboración, es requisito indispensable elaborar los documentos relativos a su buen funcionamiento, en relación con su operación, con las características técnicas operativas, administrativas y económicas que lo fundamentaron, con los manuales que apoyarán al usuario y con todos los demás manuales e instructivos que servirán de apoyo al propio desarrollador del sistema.

Conviene señalar que es de suma importancia que antes o durante la implementación del sistema se proporcione la capacitación a sus usuarios finales, debido a que sólo así se pueden garantizar la eficiencia y eficacia en la implementación del proyecto. También se debe contar con la completa documentación de respaldo y apoyo que sirva de consulta a los usuarios para el buen uso del sistema.

Otra garantía del buen funcionamiento del sistema es el establecimiento del control interno informático en relación con la documentación de dicho sistema, a fin de que sirva de ayuda al usuario y al propio desarrollador del proyecto, lo cual contribuirá a su mejor operación y a su posterior modificación. Esto es de suma importancia para cualquier proyecto informático, y es específicamente lo que debe revisar el auditor cuando evalúe el control interno de sistemas.

Puede haber muchos tipos de documentos útiles para el desarrollo de las actividades del área de sistemas computacionales, según las características y configuración de los sistemas, el tamaño del centro de computo, la experiencia y conocimiento de su personal y otros muchos aspectos; por esta razón, a continuación analizaremos algunos de los principales documentos del sistema.

5.2.6.1 Manuales e instructivos del usuario

Son los documentos que sirven de guía para el usuario, en los cuales se anotan todas las instrucciones sobre el uso del sistema, incluyendo las guías de operación, los términos más comúnmente utilizados, la descripción de las operaciones básicas, pantallas y demás acciones sobre el sistema.

5.2.6.2 Manual e instructivo de operación del sistema

Es el documento en el cual se anotan concretamente los pasos a seguir para la operación normal del sistema, incluyendo el detalle del manejo de los equipos, su encendido y su forma de terminación, las formas de acceso y de captura de la información, su procesamiento, así como la emisión de informes.

5.2.6.3 Manual técnico del sistema

Es un documento especializado en el cual se indican todos los aspectos técnicos que se deben considerar para el adecuado manejo del sistema; estos aspectos suelen ser muy sofisticados y con características especiales sobre el funcionamiento técnico de los sistemas computacionales, no sólo en cuanto al software y hardware, sino también en cuanto a sus instalaciones, equipos y manejo de información.

5.2.6.4 Manual para el seguimiento del desarrollo del proyecto del sistema

Es un documento característico de los sistemas de información, en el cual el desarrollador plantea todas las acciones y tareas que se realizan en el análisis, desarrollo, programación e implementación del sistema. Este documento sirve de referencia y de guía para el desarrollo de proyectos similares o como consulta sobre este proyecto.

5.2.6.5 Manual e instructivo de mantenimiento del sistema

Es un complemento del documento anterior, debido a que en este documento se presentan las actualizaciones, preventivas o correctivas, que van surgiendo durante la vida activa del proyecto. Este documento, al igual que el anterior, garantiza la continuidad del proyecto, ya que sirve de referencia y orientación para entender el funcionamiento del sistema y para su mantenimiento. Además, ayuda al auditor a realizar estadísticas sobre el comportamiento, utilidad, descomposturas y demás detalles del funcionamiento del sistema.

5.2.6.6 Otros manuales e instructivos del sistema

Son aquellos otros documento que sirven de apoyo para conocer el funcionamiento del nuevo sistema, a fin de contemplar todos los aspectos que ayudan al desarrollador y al usuario a conocer las características, comportamiento, componentes y todos los aspectos especiales que ayudan al buen funcionamiento del sistema.

A continuación presentamos algunos ejemplos de esos documentos, sin su respectivo análisis:

- *Manuales de organización*
- *Manuales de métodos y procedimientos*
- *Cursos de capacitación y adiestramiento*
- *Libros de consulta*
- *Diccionarios especializados*
- *Otros documentos técnicos*
- *Otros documentos administrativos, etcétera.*

5.3 Controles internos para la operación del sistema

El desarrollo de sistemas no se refiere únicamente al análisis, diseño e implementación de sistemas, se refiere también a otras actividades, de tanta o más significancia para las funciones de dichos centros, dependiendo de su tamaño, configuración y características; una de las más relevantes es la operación de los sistemas computacionales, la cual se realiza bajo condiciones y con características muy especiales. Por eso es de suma importancia contar con un elemento de control interno que evalúe la adecuada operación de los sistemas. En este caso será la adopción de un elemento que se encargue de vigilar y verificar la eficiencia y eficacia en la operación de dichos sistemas.

Para entender el papel que juega este elemento en el desarrollo de las actividades del centro de cómputo, podemos señalar que su existencia ayuda a garantizar el cumplimiento de los objetivos básicos del control interno, mismos que fueron analizados al principio de este capítulo. De entre ellos destacan:

- *Establecer como prioridad la seguridad y protección de la información, del sistema de cómputo y de los recursos informáticos de la empresa.*
- Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en las empresas.

Contando con este elemento básico podremos prevenir y evitar posibles errores y deficiencias de operación, así como el uso fraudulento de la información que se procesa en un centro de cómputo, además de posibles robos, piratería, alteración y modificaciones de la información y de los sistemas, lenguajes y programas de la institución.

Esto también se puede hacer extensivo al uso, conservación, mantenimiento y seguridad de los equipos y sistemas de procesamiento asignados al área de sistemas; no sólo nos referimos al aspecto físico del equipo y de las instalaciones, sino también al aspecto lógico, a la información y a los recursos humanos del propio centro.

Para este elemento del control interno de sistemas vamos a proponer la aplicación de los siguientes subelementos. Con la instalación de estos subelementos en un centro de cómputo podremos garantizar una mayor eficiencia y eficacia en la operación de los sistemas:

- *Prevenir y corregir errores de operación*
- *Prevenir y evitar la manipulación fraudulenta de la información*
- *Implementar y mantener la seguridad en la operación*
- *Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución*

A continuación analizaremos cada uno de los subelementos aquí propuestos.

5.3.1 Prevenir y corregir errores de operación

Para prevenir y, en su caso, corregir los posibles errores de operación, ya sean involuntarios o premeditados, lo mejor es implementar mecanismos de control que permitan verificar la exactitud, suficiencia y calidad de los datos que serán procesados, vigilando el adecuado cumplimiento de la captura, procesamiento y emisión de resultados.

Es común encontrar que en muchos centros informáticos, principalmente en aquellos que tienen un sistema de procesamiento centralizado, los encargados de verificar y controlar los accesos de información del sistema computacional realizan esta función. Dichos empleados, en su labor cotidiana, supervisan la calidad, suficiencia y todos los demás detalles administrativos que repercuten en la operación del centro de cómputo, en beneficio del usuario y de la información que se procesa en la empresa.

Con estas actividades no sólo se controla la calidad de la información que será procesada en el área de informática, sino que también se realiza una mejor planeación y un mejor control de la operación del propio centro de cómputo, ya que se programa y se dosifica la aceptación de trabajos, lo cual beneficia al procesamiento de la información, a la vez que controla la emisión de resultados y, en su caso, mantiene la operatividad del trabajo que se realiza en dicho centro.

Podemos establecer que este control para el acceso de datos en unidades de informática, sin importar su tamaño, características, configuración y demás aspectos propios de cada centro, es una simulada auditoría a las operaciones del propio centro, ya que se supervisa cotidianamente el desarrollo de los ciclos de trabajo, que van desde la recepción de datos hasta la entrega de resultados al usuario final.

Cabe resaltar la importancia de la aplicación de este elemento del control interno informático para las operaciones de los sistemas, ya que éstos requieren una permanente actualización debido a las siguientes razones:

Constantes cambios en las características y modalidades del funcionamiento de los centros de cómputo, de sus sistemas y de las bases de datos.

Creciente modificación en los sistemas de red y multiusuarios, la adopción de nuevas técnicas de configuración, software y otras formas de comunicación entre los sistemas y componentes del mismo.

Niveles de acceso al sistema por parte del administrador, operadores y usuarios, según su nivel de participación, a fin de satisfacer las necesidades de procesamiento de datos.

Actualización en la programación de sistemas de aplicación que permitan el buen funcionamiento de los sistemas computacionales de la empresa.

Los programas de supervisión de los sistemas operativos, con los cuales se pueden realizar supervisiones de manera rutinaria a los archivos de datos, e incluso un monitoreo de las operaciones del sistema y la emisión de los resultados de dicho monitoreo, tipo auditoría del sistema, los cuales permiten evaluar su funcionamiento.

Vigilar y delimitar los accesos y usos de programas y archivos con información privilegiada y otras formas específicas de procesamiento de información, entre otras muchas operaciones.

Todo ello a fin de prevenir y evitar los posibles errores de operación, lo cual es el objetivo de este elemento del control interno informático.

5.3.2 Prevenir y evitar la manipulación fraudulenta de la información

Así como analizamos la importancia de proteger los sistemas contra los errores de operación, también debemos estudiar la importancia de prevenir y evitar la manipulación fraudulenta y dolosa de los programas propiedad de la institución y la información que se procesa a través de los equipos de cómputo; con lo anterior se evitará un mal uso de la información por parte del personal y usuarios del área de sistemas de la empresa.

Otro aspecto de suma importancia para un adecuado control interno es vigilar la manipulación de la información que será procesada en el sistema, así como establecer las medidas necesarias para controlar su acceso y niveles de uso, para así prevenir un uso inadecuado de los sistemas, ya sea para beneficio de terceros, para realizar algún boicot en la institución, para propiciar errores durante el proceso de datos o para cualquier otro aspecto que sea ajeno de la operación normal de la empresa.

Actualmente, además de la existencia de controles de la información, de la administración de accesos al sistema y del control de procesamiento de los equipos de cómputo, también se utilizan sistemas, técnicas, programas y métodos de prevención en la manipulación de la información; además se establecen *contraseñas de acceso* (*passwords*), con lo cual se busca evitar los malos manejos en las bases de datos y en el software institucional. Con estas medidas se impide o cuando menos se limita el uso inadecuado de la información, así como de los resultados que se obtienen de esos datos, con lo cual se salvaguardan los activos y la información de la institución.

La información es el activo más importante que tiene cualquier área de sistemas, más que sus propios programas, procesadores, equipos, mobiliario, periféricos y consumibles. Por esta razón, es de suma importancia tener un alto grado de seguridad en los accesos al sistema, en la manipulación de los datos y en los resultados obtenidos con su procesamiento. Sobre todo, cuando se pretende prevenir su posible mal uso, siempre se deben realizar las correcciones necesarias para su buen uso. Esto por sí solo destaca la importancia de este elemento.

5.3.3 Implementar y mantener la seguridad en la operación

Hablar de seguridad en la operación equivale a señalar el uso de todas las medidas preventivas y correctivas que es necesario establecer en un centro de cómputo para el buen funcionamiento y protección del procesamiento de datos; estas medidas van desde el control de acceso al sistema para personal, usuarios y personas con derecho, hasta la protección de las bases de datos, de los sistemas institucionales y de los procedimientos para la manipulación de los resultados de dichos procesos, pasando por los respaldos periódicos de los programas y de la información procesada, así como los demás aspectos de seguridad que repercuten en la operación del centro de cómputo.

Ahora que hemos analizado los aspectos anteriores, podemos comprender la importancia de diseñar y establecer las medidas de seguridad necesarias para la protección y prevención de riesgos en la operación de un centro informático.

Es evidente que un centro de cómputo debe contar con las normas, programas y medidas de seguridad que le garanticen la buena operación y la adecuada custodia de sus bienes, programas e información. Esto se logra a través de planes y programas de seguridad de carácter *físico (hardware, instalaciones y equipos periféricos asociados*) y los de carácter lógico (*sistemas operativos, lenguajes, programas e información*).

Posteriormente profundizaremos en el estudio de este subelemento, ya que es uno de los más importantes; por ahora sólo agregaremos que su adopción facilita la salvaguarda y el uso adecuado de los bienes e información de la empresa.

5.3.4 Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución

El primer rubro que se destaca en el estudio inicial de sistemas, es el análisis y la comprensión de los atributos que debe poseer la información que se procesa en un sistema computacional, cualesquiera que sean las características, forma de procesamiento, tamaño y configuración del sistema.

Para entender la importancia de este elemento, recordemos algunos de los principales atributos de la información, como *la confiabilidad, la oportunidad, la veracidad y la suficiencia;* éstos son los elementos básicos que se utilizan para establecer un control interno adecuado en un centro de información; esto obedece a que con su adopción y uso permanente, como norma de trabajo, contribuyen a la cabal comprensión del objetivo fundamental del área de sistemas para la empresa, en cuanto a la captura y procesamiento de datos, emisión de resultados y custodia de la información.

5.4 Controles internos para los procedimientos de entrada de datos, procesamiento de información y emisión de resultados

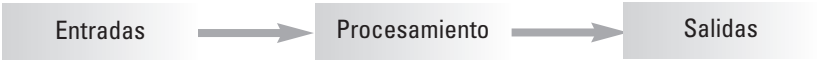
Ya hemos mencionado a lo largo de este estudio del control interno informático que el aspecto más importante para la adopción de estos controles en el área de sistematiza-

ción, es que son de gran ayuda por la confiabilidad que brindan en el procesamiento de información.

Sin embargo, desde un punto vista más sencillo, cuando entendamos que un sistema de información es un procedimiento simple de *entrada, proceso y salida,* en donde un dato de entrada se transforma en información útil de salida mediante algún procesamiento interior, entenderemos también que el control interno informático es útil para verificar que este procedimiento se lleve a cabo correctamente.

Para una mejor comprensión de este punto, señalaremos que dicho proceso está compuesto de tres fases fundamentales:

- *La entrada de datos al sistema*
- *El procesamiento de datos por medio de un sistema de procesamiento interno (caja negra)*
- *La emisión de resultados útiles para la toma de decisiones*



Estas fases son las que dan vigencia a cualquier sistema. Utilizando como referencia lo anterior, a continuación analizaremos los siguientes subelementos del control interno:

- *Verificar la existencia y funcionamiento de los procedimientos de captura de datos.*
- *Comprobar que todos los datos sean debidamente procesados.*
- *Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos.*
- *Comprobar la suficiencia en la emisión de información.*

5.4.1 Verificar la existencia y funcionamiento de los procedimientos de captura de datos

El trabajo de informática se inicia con la entrada de los datos que serán procesados en el sistema de información; por esta razón, es de vital importancia adoptar este subelemento del control interno, a fin de asegurar que la entrada de datos será acorde con las necesidades de captura del propio sistema.

Si consideramos que el objetivo final de un sistema de computación es el procesamiento de los datos capturados, la siguiente frase cobra vigencia para el cabal entendimiento de este subelemento:

Si se captura basura en el sistema de cómputo, como resultado de su procesamiento se obtiene basura.

Al analizar lo anterior, es evidente que se necesita establecer un adecuado control en la entrada de los datos que han de ser procesados en cualquier sistema computacional, ya que de esto depende que se obtengan buenos resultados de ese proceso;

además, con la adopción del control interno se busca que los resultados del procesamiento de datos sean los esperados por el usuario, a fin de utilizarlos de manera oportuna, confiable y adecuada.

Para lograr la *eficiencia y eficacia* que se pretenden al establecer este elemento en la captura de datos, es necesario tener bien establecidos aquellos métodos, procedimientos y actividades que regularán la entrada de datos al sistema, así como las normas, políticas y lineamientos que ayudarán a capturar mejor dichos datos. Con esto se garantiza que el procesamiento de información y la emisión de resultados sean adecuados.

Con la implementación de este subelemento también se pretende dar validez y veracidad a los datos que entran al sistema, para lo cual se establecerán los procedimientos, métodos, pruebas y verificaciones que se deben realizar durante los procesos de captura; por ejemplo, el establecimiento de cifras de control, el cotejo de datos, la captura doble de la información, los chequeos aleatorios de datos y muchos otros exámenes que garanticen la veracidad y confiabilidad de los datos introducidos al sistema.

Sin embargo, no basta con verificar la entrada correcta de los datos capturados, también es necesario comprobar que éstos sean introducidos con la oportunidad que demanda el sistema; esto se verifica con los siguientes procedimientos:

- *El establecimiento y cumplimiento de los procedimientos adaptados para satisfacer las necesidades de captura de información de la empresa.*
- *La adopción de actividades específicas que ayuden a la rápida captura de datos.*
- *El seguimiento de los métodos y técnicas uniformes que garanticen que la entrada de datos al sistema se realice siguiendo los mismos procedimientos.*

En consecuencia, con la aplicación de los procedimientos anteriores se puede garantizar la uniformidad en la entrada de datos, siempre que se utilicen los mismos métodos, técnicas y procesos en tiempos similares, garantizando con ello la oportunidad y utilidad de la información.

Para el buen funcionamiento de este subelemento del control interno, se tienen que contemplar las estructuras que deben tener las bases de datos, a fin de prevenir posibles problemas de captura, como pueden ser las redundancias, los desajustes de datos, las repeticiones de información o cualquier otra contrariedad que llegue a afectar la introducción de datos al sistema. También se debe contemplar la seguridad y la protección en la captura de la información, aspectos que serán tratados en otro subelemento del control interno.

5.4.2 Comprobar que todos los datos sean debidamente procesados

Además de verificar que los datos sean capturados y procesados de manera oportuna, confiable y eficiente, igual que en la emisión de los resultados, también es indispensable que con el control interno informático se tenga la confianza de que todos los datos ingresados al sistema sean procesados de igual manera sin que sufran ninguna altera-

ción, ya sea accidental, involuntaria o dolosa, durante su procesamiento. Cumpliendo con esto se garantiza la uniformidad de los resultados y, consecuentemente, se obtiene una mejor explotación de los mismos.

Debemos remarcar que el procesamiento de datos se debe realizar de la misma manera en todos los casos, sin admitir ninguna variación en lo más mínimo; esto casi siempre se cumple, ya que antes de liberar un sistema, previamente se comprueban los procesamientos de información, primero mediante pruebas con datos falsos, similares a los que se utilizarán en el sistema, y posteriormente mediante pruebas con datos reales; una vez aprobado su funcionamiento, se libera el proyecto con la plena confianza de que su procesamiento interno será siempre igual.

Esto por sí solo justifica la adopción de este subelemento del control interno; sin embargo, además de lo antes señalado, también es necesario establecer métodos, procedimientos y lineamientos en el área de sistemas para evitar la existencia de algún tipo de manipulación externa o interna, accidental o intencional, que altere los procesamientos de información implementados en la empresa.

5.4.3 Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos

Para implementar este subelemento del control interno, es necesario entender que no basta con verificar la confiabilidad de la captura de los datos, sino que también se debe evaluar la veracidad de los datos que se introducen al sistema. Además, es imperioso comprobar la exactitud y suficiencia en el procesamiento de dichos datos, para lo cual es necesario establecer los procedimientos adecuados que ayuden a satisfacer los requerimientos de captura y procesamiento de información en el área de sistemas.

Sin embargo, para el buen funcionamiento de este subelemento, también se deben adoptar acciones concretas que ayuden a capturar y a procesar los datos de manera eficiente; para ello se tienen que establecer métodos, técnicas y procedimientos que sean aplicados de manera uniforme en todas las etapas que intervienen en el procesamiento de información; con esto se pueden garantizar mejores resultados en la verificación de la uniformidad que requiere este subelemento del control interno informático.

Debemos señalar que lo que se busca con este subelemento del control interno es la implementación de los métodos, técnicas y procedimientos que ayuden a uniformar las actividades requeridas en el área de sistematización para la captura de datos, el procesamiento de información y la emisión de informes.

5.4.4 Comprobar la suficiencia de la emisión de información

Si partimos de que el objetivo básico de un centro de cómputo es *proporcionar los servicios de procesamiento de datos que requiere la empresa para satisfacer sus necesidades de información*, entonces entenderemos que uno de los aspectos fundamentales de un centro de cómputo es proporcionar la información que requieren las demás

áreas de la empresa, con lo cual contribuye a satisfacer sus necesidades de procesamiento de datos.

Sin embargo, esa información debe ser adecuada a los requerimientos de la empresa para ofrecer sólo la información requerida, sin dar ni más ni menos datos que los necesarios. A esto se le llama *proporcionar la información suficiente*.

Precisamente esto es lo que se busca satisfacer con la suficiencia de información; para lograrlo, es necesario que el área de sistemas sepa cuáles son los requerimientos reales y específicos de información del usuario; esto se logra mediante un análisis adecuado de sus necesidades y con el diseño correcto de los sistemas que proporcionarán esa información. Evidentemente, dicha suficiencia sólo se logrará mediante un buen análisis y diseño de sistemas.

De lo anterior es fácil comprender que el establecimiento de este subelemento del control interno informático es una necesidad básica en las áreas de sistematización, ya que con este control se verificará que la información proporcionada al usuario sea, ni más ni menos, la necesaria para satisfacer sus requerimientos fundamentales para la realización de sus actividades cotidianas.

5.5 Controles internos para la seguridad del área de sistemas

Dentro de los aspectos fundamentales que se deben contemplar en el diseño de cualquier centro de informática, se encuentra la seguridad de sus recursos informáticos, del personal, de la información, de sus programas, etcétera. Esto se puede lograr a través de medidas preventivas o correctivas, o mediante el diseño de programas de prevención de contingencias para la disminución de riesgos.

Para el mejor entendimiento de la importancia de este elemento y de su aplicación correcta, a continuación se indican sus principales aspectos:

Seguridad física

Es todo lo relacionado con la seguridad y salvaguarda de los bienes tangibles de los sistemas computacionales de la empresa, tales como el hardware, periféricos y equipos asociados, las instalaciones eléctricas, las instalaciones de comunicación y de datos, las construcciones, el mobiliario y equipo de oficina, así como la protección a los accesos al centro de sistematización. En sí, es todo lo relacionado con la seguridad, la prevención de riegos y protección de los recursos físicos informáticos de la empresa.

Seguridad lógica

Es todo lo relacionado con la seguridad de los bienes intangibles de los centros informáticos, tales como software (aplicaciones, sistemas operativos y lenguajes), así como lo relacionado con los métodos y procedimientos de operación, los niveles de acceso a los sistemas y programas institucionales, el uso de con-

traseñas , los privilegios y restricciones de los usuarios, la protección de los archivos e información de la empresa y las medidas y programas para prevenir y erradicar cualquier virus informático. En sí, es todo lo relacionado con las medidas de seguridad, protección y forma de acceso a los archivos e información del sistema.

Seguridad de las bases de datos

Es la protección específica de la información que se maneja en las áreas de sistemas de la empresa, ya sea a través de las medidas de seguridad y control que limiten el acceso y uso de esa información, o mediante sus respaldos periódicos con el fin de mantener su confidencialidad y prevenir las alteraciones, descuidos, robos y otros actos delictivos que afecten su manejo.

Seguridad en la operación

Se refiere a la seguridad en la operación de los sistemas computacionales, en cuanto a su acceso y aprovechamiento por parte del personal informático y de los usuarios, al acceso a la información y bases de datos, a la forma de archivar y utilizar la información y los programas institucionales, a la forma de proteger la operación de los equipos, los archivos y programas, así como las instalaciones, mobiliario, etcétera.

Seguridad del personal de informática

Se refiere a la seguridad y protección de los operadores, analistas, programadores y demás personal que está en contacto directo con el sistema, así como a la seguridad de los beneficiarios de la información.

Seguridad de las telecomunicaciones

Es todo lo relacionado con la seguridad y protección de los niveles de acceso, privilegios, recepción y envío de información por medio del sistema de cómputo, protocolos, software, equipos e instalaciones que permiten la comunicación y transmisión de la información en la empresa, etcétera.

Seguridad en las redes

Es todo lo relacionado con la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de cómputo, en cuanto a la salvaguarda de información y datos de las redes, la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, así como la protección de accesos físicos, del mobiliario, del equipo y de los usuarios de los sistemas. Incluyendo el respaldo de información y los privilegios de accesos a sistemas, información y programas.

Prevención de contingencias y riesgos

Son todas las acciones tendientes a prevenir y controlar los riesgos y posibles contingencias que se presenten en las áreas de sistematización, las cuales van desde prevenir accidentes en los equipos, en la información y en los programas, hasta la instalación de extintores, rutas de evacuación, resguardos y medidas preventivas de riesgos internos y externos, así como la elaboración de programas preventivos y simulaciones para prevenir contingencias y riesgos informáticos.

Además de lo anterior, también se tiene que determinar todo lo relacionado con los riegos y amenazas que afectan a los sistemas de información, así como la prevención de contingencias y la recuperación de la información del sistema en caso de que ocurra alguna contingencia que afecte su funcionamiento. Esto es de suma importancia para el establecimiento de este elemento del control interno informático, ya que la información del área de sistemas es el activo más valioso de la empresa y todas las medidas que se adopten para la prevención de contingencias serán en beneficio de la protección de los activos de la institución.

Con el establecimiento de los siguientes subelementos del control interno informático se busca determinar las bases fundamentales sobre las que se establecerán los requerimientos para manejar la seguridad de los sistemas de información:

Controles para prevenir y evitar las amenazas, riesgos y contingencias en las áreas de sistematización

- *Control de accesos físicos del personal al área de cómputo*
- *Control de accesos al sistema, a las bases de datos, a los programas y a la información*
- *Uso de niveles de privilegios para acceso, de palabras clave y de control de usuarios*
- *Monitoreo de accesos de usuarios, información y programas de uso*
- *Existencia de manuales e instructivos, así como difusión y vigilancia del cumplimiento de los reglamentos del sistema*
- *Identificación de los riesgos y amenazas para el sistema, con el fin de adoptar las medidas preventivas necesarias*
- *Elaboración de planes de contingencia, simulacros y bitácoras de seguimiento*

Controles para la seguridad física del área de sistemas

- *Inventario del hardware, mobiliario y equipo*
- *Resguardo del equipo de cómputo*
- *Bitácoras de mantenimientos y correcciones*
- *Controles de acceso del personal al área de sistemas*
- *Control del mantenimiento a instalaciones y construcciones*
- *Seguros y fianzas para el personal, equipos y sistemas*
- *Contratos de actualización, asesoría y mantenimiento del hardware*

Controles para la seguridad lógica de los sistemas

- *Control para el acceso al sistema, a los programas y a la información*
- *Establecimiento de niveles de acceso*
- *Dígitos verificadores y cifras de control*
- *Palabras clave de accesos*
- *Controles para el seguimiento de las secuencias y rutinas lógicas del sistema*

Controles para la seguridad de las bases de datos

- *Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo*
- *Respaldos periódicos de información*
- *Planes y programas para prevenir contingencias y recuperar información*
- *Control de accesos a las bases de datos*
- *Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos*

Controles para la seguridad en la operación de los sistemas computacionales

- *Controles para los procedimientos de operación*
- *Controles para el procesamiento de información*
- *Controles para la emisión de resultados*
- *Controles específicos para la operación de la computadora*
- *Controles para el almacenamiento de información*
- *Controles para el mantenimiento del sistema*

Controles para la seguridad del personal de informática

- *Controles administrativos de personal*
- *Seguros y fianzas para el personal de sistemas*
- *Planes y programas de capacitación*

Controles para la seguridad en la telecomunicación de datos

Controles para la seguridad en sistemas de redes y multiusuarios

A continuación, como lo hemos hecho a lo largo de este libro, analizaremos por separado cada uno de estos subelementos.

5.5.1 Controles para prevenir y evitar las amenazas, riesgos y contingencias en las áreas de sistematización

El primer paso que se debe seguir para prevenir las repercusiones de posibles amenazas, riesgos y contingencias en las áreas de un centro de cómputo, es identificar aquellos elementos que pueden influir en la seguridad de sus instalaciones, de sus programas, de la

información que se maneja en ellos y del personal que los opera. Esto ayudará a identificar las eventualidades que pueden llegar a presentarse en dicha área.

Este subelemento es de gran utilidad para identificar y establecer los controles informáticos que ayuden a prevenir estos riesgos y contingencias dentro del ambiente de sistemas. Como ya hemos observado, es muy importante prevenir posibles contingencias y riesgos antes que ocurran, así como controlarlos cuando estén ocurriendo, o corregirlos después de que sucedan.

Aunque existen muchos controles para la prevención de contingencias informáticas, las cuales serán determinadas por las empresas de acuerdo con sus características, necesidades y condiciones específicas de procesamiento de información, en los siguientes incisos se presentan algunos controles básicos que deberán ser adoptados en las áreas de sistematización para evitar amenazas a los sistemas, a su información y a sus programas y recursos informáticos.

5.5.1.1 Control de accesos físicos del personal al área de cómputo

Es el establecimiento de las medidas tendientes a controlar el acceso de las personas que tengan que entrar al centro de cómputo; dichas medidas van desde registros en bitácoras o libretas, uso de gafetes y credenciales magnéticas, hasta la vigilancia estrecha de visitantes, áreas y pasillos por medio de circuito cerrado, así como la revisión física del personal que entra y sale de área de sistemas.

5.5.1.2 Control de accesos al sistema, a las bases de datos, a los programas y a la información

Es el control que se establece en el sistema en forma administrativa; esto significa que, por medio de procedimientos, claves y niveles de acceso, se permite el uso del sistema, de sus archivos y de su información a los usuarios y al personal autorizado; dichos procedimientos van desde el registro de los usuarios y la asignación de equipos y terminales, hasta el establecimiento de privilegios, límites y monitoreo de uso de sistemas, programas e información. En todos los casos de acuerdo con el nivel del usuario, a su importancia para el sistema y a las políticas de la empresa y del área de sistemas.

5.5.1.3 Uso de niveles de privilegio para acceso, palabras clave y control de usuarios

Es igual que el punto anterior, sólo que es exclusivo para los sistemas de información; aquí se manejan, mediante un software especial, las limitaciones y los privilegios de los usuarios en el uso del sistema, ya sea al no permitir el acceso a ciertos archivos y programas, o con el uso de contraseñas con las cuales se pueda ingresar al sistema, así

como la revisión periódica de los niveles de accesos autorizados a los archivos e información permisible para el trabajo de los usuarios en el sistema.

5.5.1.4 Monitoreo de accesos de usuarios, información y programas de uso

Es el monitoreo que realiza el administrador del sistema (*ver cómo se está trabajando en el sistema, sin que lo note el usuario*) con el propósito de verificar el uso del sistema, del software, de los archivos y de la información que está permitida al usuario. Se incluye el reporte de auditoría (*listado de actividades y archivos utilizados por jornada y usuario*), la intervención y limitación en las actividades del usuario.

5.5.1.5 Existencia de manuales e instructivos, así como difusión y vigilancia del cumplimiento de los reglamentos del sistema

Es el seguimiento de los diferentes manuales e instructivos, a fin de controlar el uso de los sistemas, programas y archivos, así como el cumplimiento del reglamento de uso del centro de sistematización por parte de su personal y de sus usuarios.

5.5.1.6 Identificación de los riesgos y amenazas para el sistema, con el fin de adoptar las medidas preventivas necesarias

Es la identificación de los posibles riesgos y contingencias que se pueden presentar en el área de sistematización; estas contingencias pueden tener un ***origen humano****: descuidos, negligencia, mal uso de la información, sabotajes, robos, piratería,* etcétera, o un ***origen natural****: terremotos, incendios, inundaciones,* etcétera. Estos riesgos deben ser contemplados dentro de estudios y programas preventivos elaborados por las propias áreas de sistematización.

5.5.1.7 Elaboración de planes de contingencia, simulacros y bitácoras de seguimiento

Es el control de las contingencias y riesgos que se pueden presentar en el área de sistemas; estas contingencias se pueden evitar, controlar o remediar a través de planes y programas preventivos específicos, en los cuales se presenten las actividades a realizar antes, durante y después de alguna contingencia. En estos planes se incluyen los simulacros de contingencias, los reportes de actuaciones y las bitácoras de seguimiento de las actividades y eventos que se presentan en el área de sistemas.

Es evidente que existen muchos más controles para el área de sistematización, pero éstos serán más característicos y específicos de acuerdo con las necesidades de la empresa, a sus sistemas de información y a la forma de administración que tenga pa-

ra la seguridad de sus sistemas. Precisamente en esto es en lo que interviene el auditor, como lo analizaremos más adelante.

5.5.2 Controles para la seguridad física del área de sistemas

Con este tipo de controles se busca salvaguardar los activos tangibles de la empresa, en este caso específico, es la sistematización para la protección y custodia de los equipos de cómputo, periféricos, mobiliario y equipo asignado a esa área, así como la protección y seguridad del personal, de los usuarios y el demás personal involucrado en el centro de cómputo.

Es de suma importancia destacar que el establecimiento de este subelemento del control interno informático ayudará enormemente a salvaguardar los activos informáticos tangibles del área de sistemas, con los cuales se realizan sus actividades y el cumplimiento de sus tareas.

Para el mejor entendimiento de la adopción de este subelemento, y aunque existen muchos controles para la prevención de contingencias y salvaguarda de estos recursos informáticos, a continuación proponemos algunos controles básicos que deberán ser adoptados en las áreas de sistematización para la protección de sus recursos; sin embargo, las empresas deberán determinar estos controles de acuerdo con sus características, necesidades y condiciones específicas de procesamiento de información.

5.5.2.1 Inventario del hardware, mobiliario y equipo

Es el registro de carácter contable que se hace de todos los activos de los sistemas; en dicho registro se anotan las características, la configuración, el tipo de procesadores, la velocidad, los componentes, las especificaciones y demás elementos que componen el hardware de cada uno de los sistemas computacionales. También se registran los costos, las depreciaciones, las actualizaciones, los cambios y otros movimientos del sistema, así como el mobiliario, los equipos y demás activos similares del área de sistemas.

En el capítulo 10 se presenta un formato para un adecuado inventario del hardware.

5.5.2.2 Resguardo del equipo de cómputo

Es la asignación documental del equipo de cómputo, de sus periféricos, mobiliario y demás componentes que se hace al personal o a los usuarios del área de sistematización; por medio de estos documentos se les responsabiliza de la salvaguarda y buen uso del equipo que tienen asignado; la intención es contar con un documento de control sobre este tipo de activos y mantenerlo vigente, así como responsabilizar al usuario del uso adecuado y la protección de estos activos.

5.5.2.3 Bitácoras de mantenimientos y correcciones

Es el registro pormenorizado y cronológico del mantenimiento preventivo y las reparaciones del hardware, periféricos y equipos asociados del sistema computacional, así como de sus instalaciones y mobiliario; estas bitácoras se utilizan con el propósito de evaluar el uso, aprovechamiento e incidencias de cada uno de los sistemas asignados al centro de cómputo. Además, con estas bitácoras, una por cada sistema, se obtienen estadísticas útiles para valorar su utilidad en la empresa.

5.5.2.4 Controles de acceso del personal al área de sistemas

Son las medidas establecidas en las empresas con el propósito de limitar y controlar el ingreso del personal y usuarios al área de sistemas, para evitar contingencias y riesgos físicos a los equipos de dicha área.

5.5.2.5 Control del mantenimiento a instalaciones y construcciones

Es el control que establece el administrador de la empresa, a fin de salvaguardar y mantener en buen estado las instalaciones del sistema, ya sean eléctricas, las comunicaciones vía telefónica, satelital, módem u otros medios similares, así como las conexiones del sistema computacional, sean individuales, redes internas, externas, entre otras.

Es también el control para el mantenimiento de las construcciones del área de sistemas, incluyendo la iluminación, el medio ambiente, el clima artificial para la comodidad de los usuarios, etcétera.

5.5.2.6 Seguros y fianzas para el personal, equipos y sistemas

Son las medidas preventivas para garantizar la reposición de los activos informáticos de la empresa en caso de ocurrir alguna contingencia. Estas medidas se establecen para asegurar la vigencia de las pólizas de los activos informáticos asegurados, así como sus coberturas.

Igual ocurre al afianzar la participación del personal y usuarios del área de sistematización de la empresa, ya sea para salvaguardar su fidelidad, o para protegerse de su ausencia por cualquier motivo.

5.5.2.7 Contratos de actualización, asesoría y mantenimiento del hardware

Es el convenio que se realiza con los proveedores, distribuidores de equipos y demás personas involucradas en el buen funcionamiento del hardware, periféricos, mobiliario y equipo del área de sistemas. Incluyendo la asesoría, actualización de sistemas, los avances tecnológicos y demás aspectos que permiten el uso óptimo del sistema.

Al igual que en la sección anterior, la empresa debe implementar los subelementos antes señalados de acuerdo con sus características y necesidades específicas de seguridad informática.

5.5.3 Controles para la seguridad lógica de los sistemas

Así como es necesario establecer controles para salvaguardar los bienes físicos del sistema computacional de la empresa, también es necesario establecer controles y medidas preventivas y correctivas para salvaguardar sus bienes lógicos. Con ello se pretende un buen uso del software, de los programas, de los sistemas operativos, del procesamiento de información, de los accesos al sistema, de la información, etcétera.

Cabe aclarar que estos controles se deben establecer de acuerdo con el tipo de sistemas de la empresa, al tamaño y configuración de su equipo, a la forma de procesamiento de su información y a sus características concretas y procedimientos de operación, así como de acuerdo con los lenguajes de programación, paqueterías, programas y aplicaciones concretas que se realizan con el sistema computacional.

A continuación proponemos algunos controles que se deben considerar en la seguridad lógica, los cuales, al igual que en las secciones anteriores, se tienen que establecer de acuerdo con las características y necesidades de procesamiento de la empresa.

5.5.3.1 Control para el acceso al sistema, a los programas y a la información

Es la implementación de las medidas de seguridad y de los controles necesarios para delimitar el nivel de acceso de los usuarios y personal al área de sistemas, estableciendo los privilegios, modos de entrada, forma de uso del sistema y otras características, para el control de los usuarios. Estas pueden ser desde la limitación de procedimientos de acceso, pasando por el establecimiento de claves de acceso (password) hasta limitar el uso de programas e información.

5.5.3.2 Establecimiento de niveles de acceso

Es la definición, mediante la programación y las paqueterías específicas de control lógico, de los límites de acceso de los usuarios a los programas institucionales, paqueterías y herramientas de desarrollo, de acuerdo con la importancia del software e información que pueden manejar.

5.5.3.3 Dígitos verificadores y cifras de control

Es el establecimiento de operaciones aritméticas, controles sumarizados y dígitos de verificación matemática de los datos que se capturan y se procesan en el sistema, con el propósito de mantener la confiabilidad de estos últimos.

5.5.3.4 Palabras clave de acceso

Es el control que se establece por medio de palabras clave (contraseñas) para el acceso y uso de los programas y archivos de información. Estas claves son establecidas por el administrador del sistema y por el propio usuario.

5.5.3.5 Controles para el seguimiento de las secuencias y rutinas lógicas del sistema

Este tipo de controles son más especializados para los administradores y operadores del sistema, y se establecen para controlar las rutinas de procesamiento y las secuencias lógicas del sistema operativo, de los lenguajes de programación y de las paqueterías especializadas que permiten el manejo de los sistemas.

Los anteriores son algunos de los posibles controles que se pueden establecer para salvaguardar la seguridad lógica del sistema. Debemos aclarar que estos controles se deben establecer de acuerdo con las características del sistema computacional y a las necesidades de protección del área de sistematización de la empresa.

5.5.4 Controles para la seguridad de las bases de datos

El activo más importante de cualquier empresa es la información que se captura, que se procesa y que se emite en las bases de datos de los sistemas; por lo tanto, es el bien que más se debe proteger.

El control interno informático ayuda a proteger las bases de datos de la empresa, por medio de controles especiales y medidas preventivas y correctivas. Con las restricciones de acceso al sistema se pueden evitar posibles alteraciones, uso fraudulento, piratería, destrucción y sabotaje de la información de la empresa. Estos controles pueden ser establecidos por el área administrativa para vigilar el acceso de los usuarios al sistema, así como para proteger la información a través de respaldos periódicos y recuperación de datos en caso de pérdidas, deterioros y de cualquier mal uso que se haga de ellos.

Los siguientes son algunos de los controles que se pueden establecer para la seguridad de las bases de datos de la empresa.

5.5.4.1 Programas de protección para impedir el uso inadecuado y la alteración de datos de uso exclusivo

Los controles establecidos por medio de programación, ya sean derivados del sistema operativo, de lenguajes y paqueterías o de programas de desarrollo y aplicación, ayudan a proteger la información contenida en los archivos del sistema, ya que sólo el usuario autorizado tiene acceso a ella. También ayudan a proteger dicha información de posibles alteraciones, sean involuntarias o dolosas.

5.5.4.2 Respaldos periódicos de información

Es la implementación de los planes y programas de respaldo (*backups*) de la información de las bases de datos, de la información de cada usuario, la de las diferentes áreas o de toda la institución, según sea el caso; estos programas de respaldo se realizan en forma periódica y programada y se pueden copiar en cintas, disquetes, o en discos ópticos, de acuerdo con las necesidades de la empresa y a la configuración de sus sistemas, así como a su forma de gestión informática.

5.5.4.3 Planes y programas para prevenir contingencias y recuperar información

Es la elaboración, implementación y seguimiento de planes para prevenir contingencias y riesgos que se pueden presentar en el manejo de información de la empresa; dichos planes se establecen con el propósito de salvaguardar las bases de datos de la institución, por medio de medidas preventivas, de control o de recuperación en caso de alteración, pérdida o mal uso de la información institucional. También se incluyen los respaldos, limitación de accesos y administración de bases de datos.

5.5.4.4 Control de accesos a las bases de datos

Es el establecimiento de los controles administrativos y del propio sistema por medio de los cuales se limita el acceso de usuarios no autorizados a las bases de datos; con estos controles también se establecen en forma específica el acceso a las bases de datos para las actividades de consulta, para un primer nivel de acceso; para la manipulación de datos sin pérdida de los mismos ni alteración de las bases de datos en un segundo nivel, y las dos anteriores con alteración y modificación de datos para un tercer nivel, de acuerdo con los privilegios otorgados a los usuarios de las bases de datos y a las características de la información.*

5.5.4.5 Rutinas de monitoreo y evaluación de operaciones relacionadas con las bases de datos

Es el establecimiento de las rutinas y procedimientos de monitoreo de la información de las bases de datos, a fin de evaluar su manejo y uso.

* Recordemos que los usuarios de las bases de datos únicamente pueden tener los siguientes tipos de accesos a la información de una base de datos: **un primer nivel** para accesar sólo a la consulta de datos, sin tener posibilidades de hacer ninguna modificación; **un segundo nivel** para la captura de datos, donde sólo se pueden modificar datos previamente permitidos, y **un tercer nivel** para que los usuarios puedan realizar correcciones a los contenidos de las bases de datos. Otros tipos de acceso que no corresponden a los usuarios son los del personal que administra las bases de datos, para modificar programas, información o cualesquiera otras partes de las bases de datos.

Existen más controles para bases de datos, sin embargo, éstos se adoptarán en función de las características de los programas manejadores de las bases de datos y de las necesidades específicas del área de sistematización en donde se implementen.

5.5.5 Controles para la seguridad en la operación de los sistemas computacionales

Para el buen funcionamiento de los sistemas de procesamiento de datos, es necesario establecer controles y medidas preventivas para evitar accidentes, actos dolosos premeditados o negligencias que repercutan en la operación y funcionamiento del sistema o en la emisión de resultados del procesamiento de la información.

Con la instalación de estos subelementos del control interno informático en las áreas de sistematización de la empresa, se garantiza una buena operación y un buen funcionamiento del sistema computacional; los siguientes aspectos deben ser tomados en cuenta para la seguridad en la operación del sistema.

5.5.5.1 Controles para los procedimientos de operación

Es el establecimiento de métodos y procedimientos de procesamiento de información y emisión de resultados, así como de rutinas de trabajo, de verificación de entrada de datos y de validación de operaciones, los cuales ayudan en la correcta operación de los sistemas; también se pueden establecer otras medidas de acuerdo con los programas de operación del sistema, a sus programas de aplicación y a sus equipos de trabajo.

5.5.5.2 Controles para el procesamiento de información

Es el establecimiento de las medidas de seguridad necesarias para controlar la entrada de datos al sistema, así como para vigilar su procesamiento y la emisión de sus resultados; el propósito es evitar alteraciones, modificaciones, duplicidad o adición de datos durante alguna de estas etapas.

También es la adopción de los controles administrativos, en relación con la seguridad y protección de la operación del sistema *antes, durante* y *después* del procesamiento de información; asimismo, en cuanto a tiempo, a la eficiencia y productividad del operador y del propio sistema, así como en relación a la oportunidad, veracidad y las demás características de la información procesada.

5.5.5.3 Controles para la emisión de resultados

Son los controles que se establecen para asegurar la oportuna, confiable y eficiente emisión de los resultados del procesamiento de datos, así como para la correcta administración y control en distribución, respaldo y resguardo de dichos resultados. El propósito es proteger esta información de utilizaciones indebidas, de alteraciones o de cualquier otro aspecto que sea distinto a su uso normal en la empresa.

5.5.5.4 Controles específicos para la operación de la computadora

Son todas las medidas internas (las del área de sistemas) y externas (las de la empresa, proveedores o distribuidores de equipo) que regulan la operación normal del sistema de cómputo; estas medidas se establecen en función a las características del hardware, software, periféricos y demás componentes asociados del sistema, y se tienen que adoptar para su buen funcionamiento y para la protección de las operaciones que se realizan en el mismo.

5.5.5.5 Controles para el almacenamiento de información

Son las medidas de seguridad y protección, internas y externas, que se adoptan en el área de sistemas para el almacenamiento de la información contenida en las bases de datos, así como de los programas, lenguajes, y paqueterías que se utilizan para la operación normal de dicha área. Un ejemplo de estas medidas son los archivos periódicos de respaldo, los cuales pueden estar en cintas, disquetes, discos ópticos o en cualquier otro medio de grabación de datos.

También en lo referente a la recuperación de archivos en casos de desastres y a las medidas preventivas o correctivas para evitar las deficiencias de almacenamiento de información del sistema.

5.5.5.6 Controles para el mantenimiento del sistema

Es el establecimiento de los reportes de fallas, bitácoras de mantenimiento preventivo y correctivo y de estadísticas que permiten valorar las incidencias sobre el funcionamiento de los sistemas de información, de sus periféricos y demás equipos asociados, a fin de valorar el aprovechamiento en su uso y la repercusión de las fallas que se puedan presentar. Es también el establecimiento de las acciones preventivas para evitar descomposturas, tanto del hardware como del software, en los sistemas.

Los anteriores sólo son algunos de los muchos controles de operaciones que se pueden establecer a fin de salvaguardar al sistema de los imprevistos que pueden suceder durante su operación. Dichos controles deben ser establecidos de acuerdo con las necesidades de información de la empresa, a las características de sus equipos, a la configuración de éstos, a su tamaño, a la forma de procesamiento de información y a muchos otros factores.

5.5.6 Controles para la seguridad del personal de informática

El activo más valioso de las empresas es el personal que labora en ellas, debido a que es el que realiza todas las funciones y actividades, desde la dirección hasta la operación de sus áreas y equipos; evidentemente, en el área de sistemas de una empresa, el personal informático y los usuarios del sistema también conforman el activo más importan-

te, debido a que es el que demanda, analiza, diseña e implementa los sistemas de la empresa; además opera, procesa, emite, almacena y custodia su información.

Por esa razón, es indispensable el establecimiento de los controles internos informáticos en los centros de cómputo a fin de ayudar a proteger y salvaguardar la seguridad de este valioso activo del área de sistematización y de la empresa; con dichos controles se logra un mejor funcionamiento de estas áreas, una mejor operación del sistema y un mejor desarrollo de los nuevos proyectos que ayudan al procesamiento de información de la empresa.

Respecto al control de estos recursos informáticos existen muchas variantes, de acuerdo con las características y necesidades de la empresa, a su forma de administración de personal y a las condiciones especiales de trabajo del área de sistemas; sin embargo, entre los principales subelementos de control que se pueden adoptar para salvaguardar la seguridad del personal de estas áreas se encuentran los siguientes.

5.5.6.1 Controles administrativos de personal

Es el establecimiento de los controles y de todos los demás aspectos normativos, administrativos y disciplinarios de la empresa para el manejo del personal, así como de sus sueldos y prestaciones, derechos y obligaciones, entrada, salida y cumplimiento de las jornadas de trabajo de dicho personal.

5.5.6.2 Seguros y fianzas para el personal de sistemas

Es el establecimiento de las medidas preventivas para asegurar la vida y la salud de los trabajadores y usuarios del área de sistemas de una empresa, con los cuales se protegen tanto a los trabajadores como a los valores de la empresa. También se refieren a las medidas que adoptan las empresas para asegurar la fidelidad de sus trabajadores, en cuanto a su actuación, a la protección de los activos de la empresa y al cumplimento de sus funciones y actividades.

5.5.6.3 Planes y programas de capacitación

Una de las mejores formas de protección de los activos institucionales es el establecimiento de los planes, programas y eventos de capacitación tanto para el personal del área como para los usuarios del sistema, con el fin de utilizar correctamente los sistemas, su información y sus archivos.

5.5.7 Controles para la seguridad en la telecomunicación de datos

En algunos casos es necesario implementar controles internos informáticos en las áreas de sistematización para asegurar el buen funcionamiento de los sistemas de transmisión de datos de la empresa, mismos que van desde el establecimiento de protocolos de comunicación, contraseñas y medios controlados de transmisión, hasta la adopción de medidas de verificación de transmisión de la información, las cuales pue-

den ser dígitos verificadores, dígitos de paridad, protocolos de acceso a frecuencias y otras especificaciones concretas del área de transmisión de datos.

Al respecto existen tipos de controles específicos para la seguridad de las telecomunicaciones, los cuales se establecen de acuerdo con el modo de transmisión de datos, al sistema adoptado para ello, a los protocolos y medios de comunicación, a la forma de conexión de los sistemas y a otras características especiales. Por esta razón, ya no profundizaremos en subelementos específicos del control interno informático, sino que dejaremos este punto para las características y necesidades específicas de control del área de sistemas.

5.5.8 Controles para la seguridad en sistemas de redes y multiusuarios

Debido a que cada día es más frecuente el uso de redes en las instituciones, las cuales van desde simples redes internas y redes locales (LANs), hasta las redes metropolitanas (MANs) o las redes instaladas a escala mundial (WANs). El establecimiento de estos controles para la seguridad en sistemas de redes y sistemas multiusuarios de una empresa es de vital importancia. Razón por la cual se tienen que establecer medidas muy específicas para la protección, resguardo y uso de programas, archivos e información compartida de la empresa.

Respecto a la seguridad en redes, existe un sinnúmero de medidas preventivas y correctivas, las cuales constantemente se incrementan en el mundo de los sistemas. Debido a las características de los propios sistemas computacionales, a las formas de sus instalaciones, al número de terminales y a sus tipos de conexión, es necesario adaptarse a los constantes cambios tecnológicos que buscan garantizar la seguridad en el funcionamiento de las propias redes, de sus programas de uso colectivo, de sus archivos de información y de sus demás características.

La seguridad en las redes es muy eficiente y con una profundidad digna de señalarse, debido a que constantemente se establecen y actualizan sus controles, los cuales van desde la restricción de accesos para los usuarios, hasta el uso de palabras clave para el ingreso a los programas y archivos de la empresa, así como el monitoreo de actividades, rutinas de auditorías para identificar comportamientos, archivos utilizados y demás movimientos, con el propósito de salvaguardar la información y programas de estos sistemas.

Lo mismo ocurre respecto a los planes y programas de contingencia diseñados para la salvaguarda de la información, de los programas y de los mismos sistemas de red establecidos en la empresa.

Debido a lo tardado que resultaría analizar todos los subelementos de control necesarios para la seguridad en redes y multiusuarios, hasta aquí dejaremos nuestro análisis de las medidas de seguridad y protección de los sistemas, de la información y de los programas de redes; aclarando que el auditor estará en posibilidad de elegir el establecimiento de aquellos subelementos del control interno informático que sean necesarios para la evaluación del funcionamiento de los sistemas de la empresa donde se encuentre laborando.

Metodología para realizar auditorías de sistemas computacionales

6

Estructura del capítulo

Objetivos del capítulo:

Proponer una metodología específica que puede ser aplicable a la realización de cualquier tipo de auditoría en el campo de los sistemas computacionales, con el propósito de mostrar una forma concreta de llevar a cabo la planeación, selección de herramientas, desarrollo y presentación de los resultados de estas auditorías, para que el lector pueda adoptar esta metodología y en su caso adaptarla a las necesidades concretas de revisión en su ambiente de sistemas.

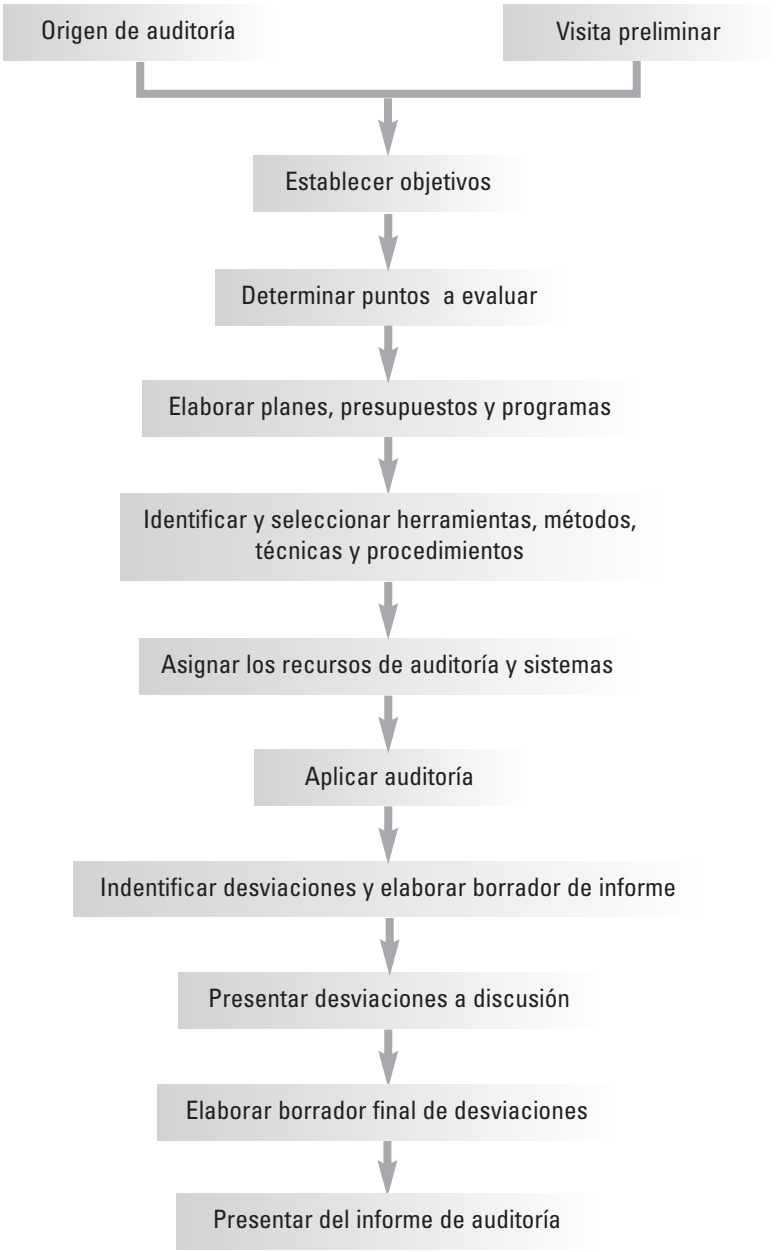
Introducción del capítulo

Llevar a cabo una auditoría de sistemas computacionales requiere una serie ordenada de acciones y procedimientos específicos, los cuales deberán ser diseñados previamente de manera secuencial, cronológica y ordenada, de acuerdo a las etapas, eventos y actividades que se requieran para su ejecución, mismos que serán establecidos conforme a las necesidades especiales de la institución. Además, estos procedimientos se deben adaptar de acuerdo al tipo de auditoría de sistemas que se vaya a realizar, y con estricto apego a las necesidades, técnicas y métodos de evaluación del área de sistematización.

Dichos métodos deberán seguirse también para la determinación de las herramientas e instrumentos de revisión que serán utilizados en la evaluación.

1. Origen de la auditoría
2. Visita preliminar
3. Establecer objetivos
4. Determinar los puntos que deben ser evaluados
5. Elaborar planes, presupuestos y programas
6. Seleccionar las herramientas, técnicas, métodos y procedimientos que serán utilizados en la auditoría
7. Asignar los recursos y sistemas para la auditoría
8. Aplicar la auditoría
9. Identificar desviaciones y elaborar borrador de informe
10. Presentar desviaciones a discusión
11. Elaborar borrador final de desviaciones
12. Presentar el informe de auditoría

Con base en lo anterior podemos entender la necesidad de establecer una metodología específica de revisión, la cual nos permitirá diseñar correctamente los pasos a seguir en la evaluación de las áreas de sistemas y actividades elegidas, a fin de que el seguimiento, desarrollo y aplicación de las etapas y eventos propuestos para esa auditoría sean más sencillos. Dicha metodología



también nos servirá para establecer las técnicas, métodos y procedimientos adaptables a las características especiales de la auditoría del área específica de sistemas a evaluar, incluyendo los recursos humanos, técnicos y materiales necesarios para dicha revisión.

Esta metodología tiene tres etapas fundamentales:

1ª ETAPA: PLANEACIÓN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES
2ª ETAPA: EJECUCIÓN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES
3ª ETAPA: DICTAMEN DE LA AUDITORÍA DE SISTEMAS COMPUTACIONALES

Más adelante analizaremos a profundidad cada una de estas etapas.

6.1 Marco conceptual de la metodología para realizar auditorías de sistemas computacionales

El primer paso para entender la metodología propuesta para desarrollar una auditoría de sistemas computacionales (ASC), es identificar el marco teórico sobre el cual se fundamentan los conceptos que serán aplicables en dicha metodología. Éstos serán definidos a continuación:

Método:

*"Del griego: **methodos,** de meta, con y **odos**, vía. Modo razonado de obrar y hablar [...] Procedimiento, técnica, teoría, tratamiento, sistema [...] Modo de obrar habitual [...] Marcha racional del espíritu para llegar al conocimiento de la verdad [...] Obra que contiene, ordenados, los principales elementos de un arte o ciencia [...]"*[1]

"Modo de realizar las cosas con orden. Procedimiento para hallar el conocimiento y enseñarlo. Conjunto de normas, ejercicios, etc., para enseñar o aprender algo."[2]

"Manera de efectuar una operación o una secuencia de operaciones."[3]

"Modo prescrito para ejecutar una tarea o trabajo determinado, por el cual se pretende alcanzar un objetivo establecido. Procedimiento que generalmente se sigue en las ciencias, por medio del cual se llega a un resultado válido. Los métodos fundamentales son: Analítico, sintético, inductivo y deductivo."[4]

Metodología:

*"Del griego **Methodos**, método, y **Logos**, tratado. Ciencia que trata del método [...]"*[5]

"Estudio de los métodos que se siguen en una investigación, un conocimiento o una interpretación."[6]

"Descripción secuencial de la manera de efectuar una operación o serie de operaciones."[7]

Planeación:

"[...] es el proceso de decidir de antemano qué se hará y de qué manera. Incluye determinar las misiones globales, identificar resultados claves y fijar objetivos específicos,

así como políticas de desarrollo, programas y procedimientos para alcanzarlos[...] La planeación tiene una implicación futura, que se tiene cierta habilidad para el diseño de planes a fin de lograr los objetivos [...]"

"Es el proceso de decidir de antemano qué se hará y de qué manera se hará. Incluye determinar la misión global, identificar los resultados claves y fijar objetivos específicos, así como políticas para el desarrollo, programas y procedimientos para alcanzarlos [...]"[8]

"Conjunto sistematizado de acciones que provienen de una estructura racional de análisis que contiene los elementos informativos y de juicio suficientes y necesarios para fijar prioridades, elegir entre alternativas, establecer objetivos y metas en el tiempo y en el espacio, ordenar las acciones que permitan alcanzarlas con base en la asignación correcta de recursos. La coordinación de esfuerzos y la imputación precisa de responsabilidades que permitan controlar y evaluar sistemáticamente los procedimientos, avances y resultados para poder introducir con oportunidad los cambios necesarios."[9]

Plan:

"El plan es un método detallado, formulado de antemano, para hacer algo [...] Un plan es un curso de acción predeterminado. Esencialmente, un plan tiene tres características. Primero, debe referirse al futuro. Segundo, debe señalar acciones. Tercero, existe un elemento de identificación o causalidad personal u organizacional [...] Los planes se derivan de las decisiones y ofrecen información por adelantado para guiar el comportamiento subsecuente [...]"[10]

"Curso de acción basado en el análisis de un problema, en el que hay que concretar los puntos y las partes de una situación dada, de tal suerte que sea factible ordenarlos y lograr una solución programada."[11]

"Un plan es cualquier método detallado, formulado de antemano para hacer algo."[12]
"Es un instrumento diseñado para alcanzar determinados objetivos, en que se definen, en espacio, tiempo y los medios utilizables para su alcance, se contemplan en forma ordenada, sistemática y coherente las metas y políticas, así como los instrumentos y acciones que se utilizarán."[13]

Programa:

"Conjunto estructurado de diversas actividades con un cierto grado de homogeneidad respecto del producto o resultado final, al cual se le asignan recursos humanos, materiales y financieros con el fin de que produzca en un tiempo determinado bienes o servicios destinados a la satisfacción total o parcial de los objetivos señalados a una función dentro del marco de la planeación."[14]

"Son cursos de acción detallados que señalan los pasos específicos que habrán de realizarse para lograr los objetivos, indicando la secuencia cronológica y los tiempos de duración de dichos pasos."[15]

Presupuesto:

"Estimación programada en forma sistemática de los ingresos y egresos que maneja un organismo en un periodo determinado; puede considerarse como un plan de acción expresado en términos monetarios y cuyo ejercicio abarca generalmente un año de actividad."[16]

Evento:

"Es la determinación de acontecimientos que llevan fines específicos de transmisión de ideas, de imágenes y sonidos, para un fin determinado."[17]

Suceso esperado al cual se debe llegar después de una serie de actividades

Actividad:

"Es el conjunto de operaciones ejecutadas o de actos desarrollados por una o varias personas y que contribuyen al logro de una función."[18]

"Una o más tareas afines que forman parte de una función, y son ejecutadas por una persona o unidad administrativa."[19]

"Conjunto de acciones y movimientos de una persona o cosa [...] Ocupación a la que alguien se dedica [...]"[20]

Tiempo:

*"Del latín **Tempus**, duración de los fenómenos [...]"*

"Duración de las cosas sujetas a cambios. Sucesión continuada de momentos que constituyen el devenir de lo existente. El existir de un mundo subordinado a un principio y un fin, en oposición a la idea de eternidad [...] Periodo más o menos largo [...]"[21]

Políticas:

"Criterio de acción que es elegido como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos a nivel institucional."[22]

"Son esencialmente un principio o varios relacionados entre sí con sus consiguientes reglas de acción que condicionan y gobiernan al logro de un objetivo."[23]

Tarea:

"Es la subdivisión del trabajo para concretizar una actividad."[24]

Plan de trabajo (gráfica de Gantt):

"Es la representación gráfica en la que se muestran las actividades que integran un proyecto, el periodo de tiempo necesario para realizar cada una de ellas y sus responsables así como los de cada actividad."[25]

Con base en el análisis de estas definiciones podemos entender que para la realización de una auditoría se debe llevar a cabo una serie ordenada de acciones, tareas y procedimientos, los cuales serán utilizados conforme a un método minucioso, previamente establecido, a fin de utilizar una serie de herramientas, métodos e instrumentos necesarios en la evaluación del área de sistemas.

6.2 Metodología para realizar auditorías de sistemas computacionales

Con el propósito de interpretar adecuadamente la aplicación de esta ***metodología para realizar auditorías de sistemas***, la cual puede ser aplicable para cualquier tipo de auditoría dentro del campo de sistemas, a continuación presentamos, en forma genérica, todas aquellas fases y pasos que se deben considerar en la planeación de la evaluación. Inicialmente señalaremos, en tres grandes apartados, las principales etapas que nos servirán de guía para la realización de una evaluación dentro del ambiente de sistemas computacionales.

1ª etapa: **Planeación de la auditoría de sistemas computacionales**

- ***P.1*** *Identificar el origen de la auditoría*
- ***P.2*** *Realizar una visita preliminar al área que será evaluada*
- ***P.3*** *Establecer los objetivos de la auditoría*
- ***P.4*** *Determinar los puntos que serán evaluados en la auditoría*
- ***P.5*** *Elaborar planes, programas y presupuestos para realizar la auditoría*
- ***P.6*** *Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría*
- ***P.7*** *Asignar los recursos y sistemas computacionales para la auditoría*

2ª etapa: **Ejecución de la auditoría de sistemas computacionales**

- ***E.1*** *Realizar las acciones programadas para la auditoría*
- ***E.2*** *Aplicar los instrumentos y herramientas para la auditoría*
- ***E.3*** *Identificar y elaborar los documentos de desviaciones encontradas*
- ***E.4*** *Elaborar el dictamen preliminar y presentarlo a discusión*
- ***E.5*** *Integrar el legajo de papeles de trabajo de la auditoría*

3ª etapa: **Dictamen de la auditoría de sistemas computacionales**

- ***D.1*** *Analizar la información y elaborar un informe de situaciones detectadas*
- ***D.2*** *Elaborar el dictamen final*
- ***D.3*** *Presentar el informe de auditoría*

6.3 1ª etapa: Planeación de la auditoría de sistemas computacionales

El primer paso para realizar una auditoría en sistemas computacionales es definir las actividades necesarias para su ejecución, lo cual se logrará mediante una adecuada planeación de éstas; es decir, se deben identificar claramente las razones por las que se va a realizar la auditoría y la determinación del objetivo de la misma, así como el diseño de los métodos, técnicas y procedimientos necesarios para llevarla a cabo y para preparar los documentos que servirán de apoyo para su ejecución, culminando con la elaboración documental de los planes, programas y presupuestos para dicha auditoría.

Concretamente, el responsable de la planeación de esta primera etapa de la metodología para realizar una auditoría de sistemas computacionales deberá iniciar con el planteamiento de los siguientes interrogantes:

¿Por qué se realizará la auditoría?
¿Se debe hacer una visita preliminar al área de sistemas?
¿Cuál es el objetivo que se pretende alcanzar con esta auditoría?

Debido a que existen múltiples métodos y técnicas de planeación, así como una abundante literatura al respecto, a continuación únicamente utilizaremos los principales conceptos que fueron definidos en el inciso anterior y que, de alguna manera, intervienen en *la planeación de una auditoría de sistemas computacionales*, a fin de identificar aquellos puntos que se pueden establecer como la base fundamental para definir las etapas y eventos que sirvan para planear el desarrollo de la auditoría. Esta fase de planeación culmina con la elaboración formal de planes, programas y presupuestos en documentos que sirven para consulta y control de las actividades de la revisión.

Iniciaremos nuestro estudio de esta etapa de planeación con los siguientes puntos:*

1ª etapa: Planeación de la auditoría de sistemas computacionales

P.1 Identificar el origen de la auditoría
P.2 Realizar una visita preliminar al área que será evaluada
P.3 Establecer los objetivo de la auditoría
P.4 Determinar los puntos que serán evaluados en la auditoría
P.5 Elaborar planes, programas y presupuestos para realizar la auditoría
P.6 Identificar y seleccionar los métodos, procedimientos, instrumentos y herramientas necesarios para la auditoría
P.7 Asignar los recursos y sistemas computacionales para la auditoría

* Para efectos de presentación de esta metodología, se utilizan las letras de cada etapa como la numeración a utilizar; sin embargo, el lector puede emplear la numeración que más le convenga.

Cuadro de *1ª etapa:* Planeación de la auditoría de sistemas computacionales

Debido a la importancia de identificar cada uno de los puntos que integran esta primera etapa de la metodología para la auditoría de sistemas computacionales, a continuación presentamos un cuadro completo de los principales puntos propuestos para la planeación de dicha auditoría:

P.1 Identificar el origen de la auditoría

P.1.1 Por solicitud expresa de procedencia interna

P.1.1.1 A petición de accionistas, socios y dueños
P.1.1.2 Por orden de la dirección general
P.1.1.3 Por orden de las gerencias o departamentos a nivel superior
P.1.1.4 A solicitud de funcionarios y empleados de otros niveles

P.1.2 Por solicitud expresa de procedencia externa

P.1.2.1 Por mandato de autoridades judiciales
P.1.2.2 Por ordenamiento de las autoridades fiscales
P.1.2.3 Por revisiones de autoridades de seguridad social y del trabajo
P.1.2.4 Por revisiones de otras autoridades
P.1.2.5 Por solicitud de proveedores y acreedores
P.1.2.6 Por solicitud de distribuidores y desarrolladores de software y hardware
P.1.2.7 A petición de empresas externas

P.1.3 Como consecuencia de emergencias y condiciones especiales

P.1.3.1 De incidencia interna
P.1.3.2 De incidencia externa

P.1.4 Por riesgos y contingencias informáticas

P.1.4.1 Rriesgos y contingencias del personal informático
P.1.4.2 Riesgos y contingencias físicas
P.1.4.3 Riesgos y contingencias operativas (lógicas)
P.1.4.4 Riesgos y contingencias de software
P.1.4.5 Riesgos y contingencias en las bases de datos
P.1.4.6 Otros riesgos y contingencias en el área de sistemas

P.1.5 Como resultado de los planes de contingencia

P.1.5.1 Por la carencia de planes de contingencia
P.1.5.2 Por la elaboración de planes de contingencia
P.1.5.3 Por la aplicación de los planes de contingencia

P.1.6 Por resultados obtenidos de otras auditorías
P.1.7 Como parte del programa integral de auditoría

P.2 Realizar una visita preliminar al área que será evaluada

P.2.1 Visita preliminar de arranque
P.2.2 Contacto inicial con funcionarios y empleados del área
P.2.3 Identificación preliminar de la problemática del área de sistemas
P.2.4 Prever los objetivos iniciales de la auditoría
P.2.5 Calcular los recursos y personas necesarias para la auditoría

P.3 Establecer los objetivo de la auditoría

P.3.1 Objetivo general
P.3.2 Objetivos particulares
P.3.3 Objetivos específicos de la auditoría de sistemas computacionales

P.4 Determinar los puntos que serán evaluados en la auditoría

P.4.1 Evaluación de las funciones y actividades del personal del área de sistemas
P.4.2 Evaluación de las áreas y unidades administrativas del centro de cómputo
P.4.3 Evaluación de la seguridad de los sistemas de información
P.4.4 Evaluación de la información, documentación y registros de los sistemas
P.4.5 Evaluación de los sistemas, equipos, instalaciones y componentes

P.4.5.1 Evaluación de los recursos humanos del área de sistemas
P.4.5.2 Evaluación del hardware
P.4.5.3 Evaluación del software
P.4.5.4 Evaluación de la información y las bases de datos
P.4.5.5 Evaluación de otros recursos informáticos
P.4.5.6 Evaluación de equipos, instalaciones y demás componentes

P.4.6 Elegir los tipos de auditoría que serán utilizados
P.4.7 Determinar los recursos que serán utilizados en la auditoría

P.4.7.1 Personal para la auditoría de sistemas
P.4.7.2 Personal del área que será evaluada
P.4.7.3 Apoyo de los sistemas y equipos técnicos e informáticos
P.4.7.4 Apoyos materiales y administrativos
P.4.7.5 Otros apoyos
P.4.7.6 Recursos económicos

P.5 Elaborar planes, programas y presupuestos para realizar la auditoría

P.5.1 Elaborar el documento formal de los planes de trabajo para la auditoría

P.5.1.1 Carátula de identificación del plan de auditoría
P.5.1.2 Índice de contenido
P.5.1.3 Definición de objetivos
P.5.1.4 Delimitación de estrategias para el desarrollo de la auditoría

P.5.1.5 Planes de auditoría
P.5.1.6 Definición de normas, políticas y lineamientos para el desarrollo de la auditoría

P.5.2 Contenido de los planes para realizar la auditoría

P.5.2.1 Definir los objetivos finales de la auditoría
P.5.2.2 Establecer las estrategias para realizar la auditoría
P.5.2.3 Diseñar las etapas, eventos y tareas en que se dividirá la auditoría
P.5.2.4 Calcular la duración de las tareas y eventos para satisfacer los objetivos de la auditoría
P.5.2.5 Distribuir los recursos que serán utilizados en las diferentes etapas, actividades y tareas de la auditoría
P.5.2.6 Confeccionar los planes concretos para la auditoría

P.5.3 Elaborar el documento formal de los programas de auditoría

P.5.3.1 Gráfica del programa de actividades
P.5.3.2 Definición de las etapas y eventos que se deben llevar a cabo
P.5.3.3 Definición de las actividades y tareas

P.5.4 Elaborar los programas de actividades para realizar la auditoría

P.5.4.1 Definir de manera precisa las etapas de la auditoría
P.5.4.2 Identificar concretamente los eventos que se deben llevar a cabo en cada etapa de la auditoría
P.5.4.3 Delimitar lo más claramente posible las actividades, tareas y acciones para cada evento
P.5.4.4 Distribuir los recursos que serán utilizados en las diferentes etapas, eventos actividades y tareas
P.5.4.5 Calcular la duración de las etapas, actividades y tareas planeadas para la auditoría
P.5.4.6 Determinar fechas de inicio y fin de las etapas, actividades y tareas

P.5.5 Elaborar los presupuestos para la auditoría

P.5.5.1 Asignación de los costos de los recursos
P.5.5.2 Control de los costos de los recursos
P.5.5.3 Seguimiento y control de los planes, programas y presupuestos

P.6 Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría

P.6.1 Establecer la guía de ponderación de los puntos que serán evaluados

P.6.1.1 Definir las áreas y puntos de sistemas que serán auditados
P.6.1.2 Definir el peso de la ponderación por las áreas y puntos que serán evaluados
P.6.1.3 Realizar el documento de ponderación de la auditoría

P.6.2 Elaborar la guía de la auditoría

P.6.2.1 Determinar las áreas y puntos concretos que serán evaluados en el ambiente de sistemas
P.6.2.2 Seleccionar los métodos, procedimientos, herramientas e instrumentos de evaluación
P.6.2.3 Elaborar el documento formal de la guía de evaluación

P.6.3 Elaborar los documentos necesarios para la auditoría

P.6.3.1 Diseñar los instrumentos de recopilación de información para la auditoría
P.6.3.2 *Diseñar los cuestionarios*
P.6.3.3 Diseñar las guías para realizar entrevistas
P.6.3.4 Diseñar los formularios para encuestas
P.6.3.5 Diseñar los modelos y formatos para los inventarios del área de sistemas
P.6.3.6 Diseñar los métodos e instrumentos de muestreo
P.6.3.7 Diseñar los instrumentos especiales de evaluación de sistemas
P.6.3.8 Determinar los puntos que serán evaluados con pruebas
P.6.3.9 Diseñar las pruebas para la evaluación
P.6.3.10 Diseñar los instrumentos y herramientas para pruebas de evaluación

P.6.4 Determinar herramientas, métodos, y procedimientos para la auditoría de sistemas

P.6.4.1 Diseñar las herramientas e instrumentos que serán utilizados en la evaluación
P.6.4.2 Establecer los métodos y procedimientos que serán utilizados en la auditoría
P.6.4.3 Determinar las técnicas y procesos específicos que serán utilizados en la auditoría
P.6.4.4 Elaborar los documentos formales para los procedimientos, métodos, herramientas e instrumentos que serán utilizados en la auditoría

P.6.5 Diseñar los sistemas, programas y métodos de pruebas para la auditoría

P.6.5.1 Determinar los puntos de interés, programas, bases de datos, archivos y sistemas que serán evaluados mediante programas y pruebas de cómputo
P.6.5.2 Diseñar las pruebas, programas y sistemas para realizar las evaluaciones necesarias para el funcionamiento de los sistemas computacionales, bases de datos y archivos
P.6.5.3 Aplicar y obtener los resultados de las pruebas, programas y sistemas para realizar las evaluaciones necesarias

P.6.5.4 Diseñar, aplicar y evaluar los resultados de los programas, métodos y pruebas de simulación al sistema
P.6.5.5 Diseñar otros instrumentos de recopilación
P.6.5.6 Elaborar otros documentos de revisión

P.7 Asignar los recursos y sistemas computacionales para la auditoría

P.7.1 Asignar los recursos humanos para la realización de la auditoría
P.7.2 Asignar los recursos informáticos y tecnológicos para la realización de la auditoría
P.7.3 Asignar los recursos materiales y de consumo para la realización de la auditoría
P.7.4 Asignar los demás recursos para la realización de la auditoría

A continuación se presenta el desglose detallado de cada uno de los puntos antes señalados, a fin de hacer más clara su aplicación en la planeación de la auditoría.

6.3.1 P.1 Identificar el origen de la auditoría

El primer paso formal para iniciar la planeación de una auditoría en el área de sistemas es identificar el origen de la auditoría; es decir, lo primero es saber por qué surge la necesidad o inquietud de realizar una auditoría. Para esto nos debemos preguntar *¿de dónde?, ¿por qué?, ¿quién? o para qué* se requiere hacer la evaluación de algún aspecto de sistemas de la empresa.

Para el responsable de realizar la planeación de la auditoría de sistemas es de suma importancia identificar el origen de la auditoría, debido a que además de proporcionarle los elementos necesarios para hacer una buena planeación de la revisión, también le ayuda a definir los elementos de juicio que contribuirán a normar su criterio de evaluación. Además, conociendo el origen de la auditoría, el auditor también puede definir la manera de enfocar la revisión.

También puede saber de antemano cuáles serán los aspectos primordiales en la evaluación; es decir, puede saber cuáles serán los asuntos más relevantes sobre los que deberá trabajar, a fin de satisfacer lo que se espera de la auditoría de sistemas. Dentro de este punto de la auditoría de sistemas encontramos estas posibles causas:

Por solicitud expresa de procedencia interna

Por solicitud expresa de procedencia externa

Como consecuencia de emergencias y condiciones especiales

Por riesgos y contingencias informáticas

Como resultado de los planes de contingencia

Por resultados obtenidos de otras auditorías

Como parte del programa integral de auditoría

A continuación analizaremos con mayor detalle cada uno de estos aspectos.

P.1.1 Por solicitud expresa de procedencia interna

Podemos decir que éste es un origen oficial sobre la necesidad de realizar una auditoría al área de sistemas de la empresa, debido a que surge de una petición formal de alguien que pertenece a la empresa. Con esta solicitud se marca el requisito formal para poder llevar a cabo una evaluación en el área de sistemas.

Esta petición de revisión a los sistemas de la empresa puede obedecer a muchas causas y generalmente se encomienda a un auditor externo, ya sea a una empresa, despacho o profesionista independiente que no tiene ninguna relación laboral con la empresa o, según la estructura y necesidades de la evaluación, se puede encomendar a los mismos empleados de la institución, si es que ésta cuenta con una área de auditoría. Concretamente, de esta petición podemos identificar los siguientes orígenes internos:

P.1.1.1 A petición de accionistas, socios y dueños

Éste es el más común de los orígenes de una auditoría, incluso de sistemas computacionales, debido a que la solicitud es formulada (ordenada) por los dueños de la empresa, sean accionistas, socios o dueños únicos, con el propósito de saber cómo se administra su patrimonio, cómo se utilizan los recursos de su empresa, cuál es el rendimiento de su patrimonio, si no existen fugas, malos usos o cualquier otro aspecto que interesa a los dueños de la empresa. En el caso de los sistemas, la solicitud de auditoría va enfocada hacia el aprovechamiento de los recursos del área de sistematización de la empresa. Este origen también puede ser requerido por el consejo de accionistas.

La mayoría de las veces estas revisiones se encargan a auditores externos, sean empresas, profesionistas o despachos independientes, siempre y cuando sean ajenos a la empresa, con el propósito de contar con un criterio más objetivo, imparcial y profesional sobre el aprovechamiento de los sistemas computacionales. En contados casos, esta auditoría también se realiza de manera interna, ya sea como parte de la evaluación total de la empresa, por revisión especial de algún aspecto de sistemas, para medir el comportamiento y administración del área de sistemas o por cualquier otro aspecto interno relacionado con los sistemas que les interesa evaluar a los poseedores de la institución.

En estos casos la solicitud de auditoría se considera como una orden y se hace la revisión casi por obligación.

P.1.1.2 Por orden de la dirección general

Esta revisión se realiza por una orden directa de quien ejerce la máxima autoridad en la empresa, pudiendo tener múltiples motivos, tales como una evaluación periódica del área de sistemas, por desconfianza de la actuación de los dirigentes del área, para verificar el cumplimiento de sus actividades, para verificar el aprovechamiento de los sistemas computacionales de la institución o por algún otro motivo. Lo singular de esto es

que se ordena la auditoría e invariablemente se tiene que realizar. Lo deseable es que el responsable de la planeación de la auditoría pueda averiguar previamente los verdaderos motivos de ésta, para enfocar su revisión hacia la satisfacción de dichos motivos.

P.1.1.3 Por orden de las gerencias o departamentos a nivel superior

Esta auditoría se origina por una petición de las gerencias y departamentos de mando superior de la empresa, según sus características, estructura de organización y funciones que desempeñan para la misma; en estos casos, por alguna razón laboral válida, estos funcionarios demandan la realización de una auditoría al área de sistemas computacionales de la empresa, misma que puede o no realizarse; todo dependerá del tipo de demanda de auditoría que se realice, de la importancia que tendrá su realización y de los niveles de autoridad que afecten la realización de dicha auditoría.

P.1.1.4 A solicitud de funcionarios y empleados de otros niveles

El origen de esta auditoría es algo irregular y poco usual en las empresas, ya que la solicitud de la auditoría parte de los niveles más bajo de la jerarquía institucional y, según las políticas y procedimientos de la empresa, para que esta solicitud sea atendida, en muchos de los casos se tienen que seguir los canales formales de comunicación y autorización establecidos en la empresa.

Es muy frecuente que para autorizar la realización de esta evaluación, ésta tiene que ser analizada por los mandos intermedios o superiores de la empresa, y si existe algún motivo real y válido que justifique su ejecución, entonces se llevará a cabo. Aunque por lo general, esta evaluación no procede por el nivel de donde proviene la petición; pero si fuera el caso, sería muy importante averiguar los verdaderos motivos de esta solicitud.

P.1.2 Por solicitud expresa de procedencia externa

Podemos decir que éste es otro origen oficial sobre la necesidad de realizar una auditoría al área de sistemas en la empresa, debido a que surge de una petición formal de alguien ajeno a la empresa, a quien, por alguna causa, le interesa que sean auditados los sistemas computacionales de ésta.

Este tipo de solicitud puede ser obligatorio si es por mandato expreso de alguna autoridad, o bien a voluntad de la empresa si alguien ajeno a ésta solicita la auditoría por tener algún vínculo leve o amplio con ella; en estos casos, la empresa no tiene la obligación de acatar estas solicitudes de auditorías. Estos casos se clasifican de la siguiente manera:

P.1.2.1 Por mandato de autoridades judiciales

Este origen es el más común y siempre se deriva de un mandato de las autoridades judiciales, quienes por algún motivo solicitan (*imponen*) la realización de una auditoría a

la empresa; esta auditoría puede tener varios orígenes específicos: como resultado de alguna auditoría anterior, a petición de algún tercero, por la suposición de un delito o por cualquier otro motivo. En el caso concreto de los sistemas computacionales, éstos son algunos de los orígenes más comunes:

- Casi siempre es por la sospecha de piratería
- Por una suposición de carencia de licencias para uso de software
- Por presunción de utilización indebida del mismo software o de la información de los sistemas
- Por sospecha de un supuesto delito de carácter informático

Es indispensable aclarar que, por lo menos en México, las auditorías obligatorias de carácter legal a los sistemas computacionales solamente se pueden realizar mediante *una orden judicial*; pero, en este caso, en dicho mandato se deben aclarar perfectamente los aspectos específicos de los sistemas computacionales que se tienen que evaluar, hasta dónde será su alcance, cuáles aspectos de sistemas se pueden auditar y cuáles no, y si la auditoría deberá ser de tipo interno o externo, entre muchos casos, pero todos en función al tipo de mandato judicial que sea impuesto.

P.1.2.2 Por ordenamiento de las autoridades fiscales

Éste es uno de los orígenes más importantes de una auditoría externa y es cuando las autoridades fiscales solicitan (imponen) la realización de una auditoría; por lo general ésta es de tipo externo, realizada por una empresa, despacho o auditor independiente, y casi siempre está enfocada a revisar la información de tipo impositivo que se procesa en los sistemas computacionales de la empresa.

Para el caso concreto de sistemas, estas auditorías por lo general son de tipo externo y se derivan de algún mandato de carácter fiscal, en el cual se deben aclarar específicamente todos los aspectos que se requieren evaluar. Aunque debemos aclarar que estas auditorías solamente se practican con el propósito de revisar la información sistematizada de la empresa, ya que en la mayoría de los casos solamente se realizan para verificar el funcionamiento del sistema en el ámbito contable, el correcto y oportuno cálculo de impuestos o los resultados financieros y obligaciones impositivas similares que se manejan en los sistemas de la empresa.

Aunque estas auditorías también pueden realizarse ocasionalmente para verificar las licencias de uso del software y la paquetería institucional, con el fin de evitar la piratería informática o para algún aspecto similar de los sistemas computacionales.

Cabe aclarar que estas solicitudes de auditoría solamente pueden ser obligatorias cuando son por un mandato de las autoridades fiscales (*formalizado por oficio*); de otra manera difícilmente pueden ser obligatorias, mucho menos cuando son por solicitud de alguien que no cuente con la autoridad fiscal para ello.

P.1.2.3 Por revisiones de autoridades de seguridad social y del trabajo

Este tipo de solicitud de auditoría, aunque también es de tipo impositivo, es de origen muy especial, debido a que sólo puede ser derivado de casos inesperados que afecten a los trabajadores y patrones o por la sospecha de algún delito o irregularidad que repercuta en la seguridad social y la del trabajo. Se debe especificar, mediante mandato judicial, el tipo de auditoría de sistemas computacionales que se solicite (imponga).

En la mayoría de los casos, estas revisiones son similares a los aspectos contables manejados anteriormente, ya sea porque se requiere de alguna revisión a los sistemas de cómputo, en cuanto al manejo de la información relacionada con los aspectos contables, impositivos o de aquellos que están relacionados con el manejo de las nóminas, prestaciones y obligaciones de los trabajadores de la empresa. Esto puede llegar a pasar, pero no es común que suceda dentro del ambiente de sistemas.

En cualquier caso, se deben aclarar concretamente los aspectos que serán evaluados, así como los alcances y límites de la auditoría. De esta manera, el auditado puede exigir que no se vaya más allá de lo especificado en la auditoría.

P.1.2.4 Por revisiones de otras autoridades

Serían muy escasas y poco probables las auditorías de sistemas solicitadas (ordenadas) por autoridades federales, estatales o municipales distintas a las señaladas anteriormente, debido a que en la legislación mexicana no existen reglamentos, norma o leyes que faculten a los representantes de estos poderes públicos a que impongan la realización de algún tipo de evaluación en el ambiente de sistemas, cualquiera que sea su origen o necesidad específica.

Conviene destacar que actualmente, por lo menos en México, ni los colegios de profesionales, ni las universidades, ni las asociaciones, cámaras o gremios de cualquier índole, ni alguna otra instancia gubernamental o representativa de la sociedad están facultados para realizar u ordenar auditorías al área de sistemas de una empresa sin la autorización expresa de ésta. Además, tampoco existe autorización alguna para que, a petición de cualquiera de estas instancias, puedan ser auditados el software, hardware, equipos, instalaciones, información o cualquier otro aspecto informático de una empresa, ya que esto es privado y únicamente le compete a la propia empresa.

En el supuesto caso de que se realizara alguna auditoría en una empresa sin que mediara un mandato judicial, se incurriría en un delito sancionado por las leyes mexicanas.

P.1.2.5 Por solicitud de proveedores y acreedores

Actualmente no es difícil encontrar una solicitud de auditoría de sistemas por parte de los proveedores y acreedores de una empresa, pero no pasa de ser una solicitud, ya que la empresa a la que se pretende auditar no está obligada a dar acceso a su información, ni a sus sistemas, ni a sus bases de datos.

Estas auditorías únicamente pueden realizarse con la autorización de la empresa y sólo bajo las condiciones y en los campos de sistemas en donde ésta lo permita. La única excepción es que los acreedores y/o proveedores turnen dicha petición ante una autoridad judicial de manera oficial y específica; en caso de que dicha auditoría fuera aprobada, ésta ya sería de carácter impositivo y las autoridades tendrían que aplicarla de manera externa.

P.1.2.6 Por solicitud de distribuidores y desarrolladores de software y hardware

Este requerimiento es muy similar al caso anterior, debido a que cuando la solicitud de auditoría parte de los distribuidores y desarrolladores de hardware y software, la empresa tiene la facultad de acceder a realizarla o de negarse a ello, según sus intereses particulares, pero jamás puede ser una auditoría de carácter impositivo.

Una gran parte de estas solicitudes se origina por la suposición de que existen delitos informáticos relacionados con la piratería de software, presunción de carencia de licencias y/o desconfianza acerca del buen uso del hardware o de los sistemas de la empresa. Sin embargo, aunque dichas sospechas estén bien fundadas, sólo se podrán auditar los sistemas de una empresa cuando ésta lo permita, y jamás por imposición de los distribuidores o desarrolladores. Esta auditoría sólo puede ser de carácter impositivo mediante una orden judicial; sin la mediación de alguna autoridad, su realización sería un delito sancionable.

P.1.2.7 A petición de empresas externas

Es igual a los casos anteriores, sólo que esta auditoría se realiza a petición de una institución ajena a la empresa;para este caso, dicha auditoría solamente se puede llegar a ejecutar si es la voluntad de la empresa, la cual tiene la facultad de rechazar la evaluación o aceptar que ésta se realice, especificando sus condiciones, alcances y límites.

P.1.3 Como consecuencia de emergencias y condiciones especiales

Este tipo de auditorías se realiza cuando se presentan situaciones de emergencia y condiciones extraordinarias en el área de sistemas, las cuales están fuera de control y parámetros normales de operación en el centro de cómputo,en dichas situaciones, la auditoría se realiza casi de inmediato y, en muchos casos, sin que medie la autorización de funcionarios.

También se realizan debido a la necesidad de medir y valorar las repercusiones que tuvieron esas emergencias

y/o condiciones especiales, ya que se tienen que evaluar el impacto y posibles daños a las actividades y funciones del área de sistemas de la empresa, los cuales pueden ser desde leves problemas hasta verdaderas catástrofes.

Las auditorías que se realizan como resultado de una solicitud de cualquiera de los anteriores puntos, tienen un origen muy particular y están vinculadas con los aspectos de seguridad y protección de los sistemas computacionales de la empresa. Concretamente, encontramos que los orígenes de estas auditorías pueden ser los siguientes:

P.1.3.1 De incidencia interna

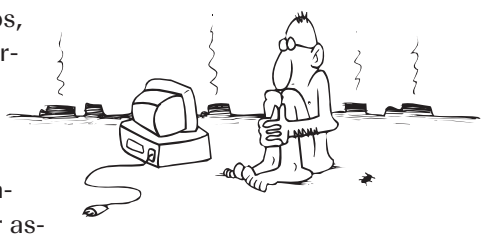
Estas auditorías se realizan cuando se presenta alguna emergencia o incidencia de tipo interno en el área de sistemas, la cual repercute en alguno de sus recursos informáticos, ya sea en el personal o los usuarios, en el equipo de cómputo, la información, instalaciones o en algún otro elemento relacionado con el area de sistemas. Dicha contingencia interna puede ser causada por alguna negligencia, por sabotaje, piratería de información o por algún otro elemento accidental ocurrido dentro de la propia área que pueda influir en el procesamiento de la información.

Evidentemente, al presentarse una emergencia interna, la petición de la auditoria de sistemas es de carácter interno y casi siempre se realiza inmediatamente e incluso, en algunos casos, no tiene que existir tal solicitud sino que, por procedimiento interno, la evaluación de las repercusiones es inmediata o la auditoría forma parte de un programa de emergencia en el área de sistemas de la empresa.

P.1.3.2 De incidencia externa

Por lo general, esta solicitud de auditoría se presenta por contingencias, emergencias y/o incidencias de carácter externo que afectan al área de informática, ya sean ocasionadas por alguna otra área de la empresa, por empresas ajenas o por algún otro agente externo que tenga o que no tenga contacto con la institución.

Al presentarse las contingencias externas en la empresa, repercuten directamente en el área de informática, lo cual hace necesaria la realización de una auditoría a los sistemas. Tomemos como ejemplos las contingencias ocasionadas por virus informáticos, un temblor, una inundación, etc. Al presentarse estos casos es necesario realizar, casi sin requisitos y de inmediato, la evaluación de los daños sufridos en el área de sistemas.



Dentro de este rubro también encontramos solicitudes de auditorías ocasionadas por aspectos externos que tienen repercusión interna, pero que al ser solicitudes de auditorías por origen externo, tienen que ser autorizadas por los directivos del área de sistemas y, en muchas ocasiones, esto no ocurre de inmediato. Entre algunos ejemplos

encontramos la repercusión del avance tecnológico de hardware y software en el funcionamiento de los sistemas de la empresa, ya que su afectación puede ser mínima o irrelevante para el sistema y se debe valorar la realización de una auditoría, o por el contrario, se requiere una auditoría cuando el efecto es mayor.

P.1.4 Por riesgos y contingencias informáticas

Es frecuente que funcionarios, personal o usuarios del área de sistemas soliciten la realización de alguna auditoría cuando ha ocurrido alguna contingencia que afecte el procesamiento de información en la empresa; aunque también puede suceder cuando existe algún riesgo que pueda repercutir en las actividades y funciones del área de sistematización, así como en el manejo de los recursos que se le han asignado. Por esta razón se deben evaluar, mediante una auditoría de sistemas, las repercusiones de cualquiera de estas incidencias, ya sean por riesgos o por la ocurrencia de alguna contingencia de carácter informático.

Los siguientes son algunos de los riegos o contingencias informáticas más comunes de estas áreas:

P.1.4.1 Riesgos y contingencias del personal informático

Esta solicitud de auditoría se origina por los posibles riesgos derivados de la actuación del factor humano del área de sistemas, ya sea del personal, de los usuarios, los asesores o consultores y de los desarrolladores o proveedores de sistemas de la empresa; asimismo, se origina por las contingencias que le pueden ocurrir a este personal. En ambos casos, éstos son algunos de los aspectos que pueden generar la necesidad de realizar una auditoría a estas áreas, ya sea porque pueden existir deficiencias y problemas en el cumplimiento de las actividades, operaciones y funciones de este personal, o por los posibles riesgos a los que está expuesto.

P.1.4.2 Riesgos y contingencias físicas

La solicitud de una auditoría de este tipo se origina por una contingencia o posible riesgo derivado de los aspectos tangibles de la empresa, es decir, de aspectos físicos como acceso del personal al equipo de cómputo, periféricos y componentes, y en sí a todo lo que corresponde al hardware del área de sistemas, así como en lo relacionado con las instalaciones, mobiliario, equipos, construcciones y demás elementos palpables del centro de informática de la empresa..

P.1.4.3 Riesgos y contingencias operativas (Lógicas)

Son las solicitudes de auditoría de sistemas derivadas de las contingencias y riesgos que posiblemente repercutirán en el funcionamiento operativo (lógico) del sistema, en

cuanto al comportamiento de sus lenguajes y programas, así como en los niveles de accesos, privilegios y limitaciones en el manejo de sus archivos, bases de datos, formas de procesamiento de información y en sí de todos aquellos aspectos que de alguna manera van a influir en el buen funcionamiento del sistema computacional.*

P.1.4.4 Riesgos y contingencias de software

Muy similar al anterior, tan es así que a veces se puede confundir; el origen de esta solicitud se debe a las contingencias y riesgos que se pueden presentar debido al manejo de los sistemas operativos, los lenguajes de programación y las paqueterías de aplicación del área de sistemas.

La mayoría de solicitudes de este tipo se originan por mal uso del software, piratería, robos, falta de licencias y otros delitos informáticos.

P.1.4.5 Riesgos y contingencias en las bases de datos

Esta solicitud de auditoría se hace exclusivamente para evaluar el manejo de los datos de la empresa, los cuales están contemplados en la operación de las bases de datos; en este caso la auditoría se enfocará en forma exclusiva a las contingencias y posibles riesgos derivados de la administración, procesamiento, custodia, acceso y uso de los datos, ya sea para detectar alguna negligencia, alteración, dolo o cualquier otra afectación en la información de la empresa.

P.1.4.6 Otros riesgos y contingencias en el área de sistemas

Los riesgos y contingencias que se derivan de otros aspectos relacionados con los sistemas pueden ser innumerables, y forzosamente tienen que ser distintos a los que analizamos anteriormente; sin embargo, cuando la solicitud de auditoría tiene este origen, se debe a que dichos aspectos están muy relacionados con las características y necesidades concretas de procesamiento de información de la empresa; en este caso, identificar el origen de la solicitud de auditoría es de suma importancia, ya que de esta manera se enfocará la evaluación en los aspectos de sistemas que se quieren auditar, los cuales serán contemplados como otros riesgos y contingencias diferentes a los tradicionales.

* El uso cotidiano del término ***lógica del sistema*** es muy común y tiene plena aceptación en las áreas informáticas, ya que el vocablo *lógica* significa: *"[...] Que sigue el proceso adecuado en el desarrollo del pensamiento [...] Ciencia que estudia las operaciones de la razón humana [...] otra corriente, centrada en los aspectos semánticos, se han originado las denominadas <<desviaciones>> de lógica clásica [...] a su vez, de la aplicación de métodos algebraicos a técnicas de aplicación (informática y computación) han surgido la lógica electrónica, la lógica binaria y la lógica terciaria".* Aunque el uso del término ***lógica del sistema*** es aparentemente una incongruencia, es plenamente aceptado en el ambiente de sistemas. Opcit. Gran diccionario del saber, pág. 1138.

P.1.5 Como resultado de los planes de contingencia

Otro de los posibles orígenes de una solicitud de auditoría en el área de sistemas lo constituyen los planes de contingencia; ya sea que se carezca de éstos en el área de sistemas y se necesite evaluar su posible efecto, o que ya estén establecidos y se requiera evaluar su funcionamiento y grado de utilidad para dichos sistemas.

Concretamente, una auditoría de este tipo se puede originar por los siguientes aspectos:

P.1.5.1 Por la carencia de planes de contingencia

El origen de esta auditoría de sistemas se debe a que no existe ningún plan de contingencia, ni un documento similar en donde se contemplen medidas preventivas o correctivas relacionadas con la seguridad de la información del área de sistemas.

Es entonces cuando, al conocer el nacimiento de la solicitud de una auditoría bajo este rubro, mucho ayudaría a valorar la necesidad de evaluar la implementación de los planes, programas y medidas preventivas de seguridad para el área de sistemas.

P.1.5.2 Por la elaboración de planes de contingencia

Esta solicitud de auditoría se origina debido a que se observan ciertas deficiencias en la elaboración de algún plan de riesgos y contingencias, ya sea preventivo o correctivo, ya que mediante esta auditoría se pueden prevenir dichas deficiencias.

En algunos casos, esta necesidad de evaluación se debe a la ausencia de difusión, conocimiento y/o utilización de dichos planes.

P.1.5.3 Por la aplicación de los planes de contingencia

Cuando la solicitud de la auditoría se debe a la aplicación del plan de contingencias, es porque se observan deficiencias en los sistemas computacionales, y en muchos casos es necesario evaluar su funcionamiento y correcta aplicación mediante una auditoría.

También suele suceder que después de haber ocurrido alguna contingencia, y al aplicar la fase final de este plan, es decir en la etapa de restauración, se detectan deficiencias en la recuperación de información, en el funcionamiento de los sistemas o problemas con el software, hardware, periféricos o en la propia área de sistemas; por esta razón es necesario evaluar la eficacia y eficiencia en la operación de los anteriores aspectos.

P.1.6 Por resultados obtenidos de otras auditorías

Es frecuente que como resultado de la práctica de una auditoría en otra área de la empresa, o aún dentro de la propia área de sistemas, surja algún aspecto específico que se tiene que evaluar mediante una auditoría más detallada.

Esta solicitud también puede originarse por algún aspecto especial derivado de los resultados de una auditoría anterior, los cuales por alguna razón repercuten en dicho aspecto, el cual se debe evaluar ya que puede afectar el comportamiento de los sistemas computacionales de la empresa.

P.1.7 Como parte de un programa integral de auditoría

También es frecuente que existan programas concretos de auditoría integral o global, los cuales se aplican en la empresa para evaluar la correcta administración y comportamiento de todas sus áreas; en este caso, la solicitud de auditoría de sistemas forma parte de dichos proyectos de evaluación integral.

Estos programas pueden ser de carácter global y se pueden aplicar una sola vez, cuando la auditoría se realiza en forma conjunta, a fin de hacer la evaluación de todas las unidades de la institución. También puede ser que, dependiendo del programa, se pueda cubrir por etapas cada una de sus áreas en forma progresiva y secuencial. Todo ello dependerá del estilo de dirección, la forma en que la empresa realiza las auditorías y si éstas se realizan de manera externa o interna.

Lo importante a destacar en este caso es que el origen de esta auditoría se debe a los resultados de una auditoría anterior

Aquí no existe propiamente una solicitud, sino que la auditoria es una disposición concreta de la institución; sin embargo, para entender mejor este punto, la vamos a considerar como una petición de auditoría.

6.3.2 P.2 Realizar una visita preliminar al área que será evaluada

Es recomendable, diríamos que casi imprescindible, que el auditor realice una visita preliminar al área de informática que será auditada, justo después de conocer el origen de la petición de auditoría, y antes de iniciarla formalmente; el propósito es que tenga un contacto inicial con el personal de dicha área y que observe cómo se encuentran distribuidos los sistemas, cuántos y cuáles son los equipos que están instalados en el centro de cómputo, cuáles son sus principales características, de qué tipo son las instalaciones, cuáles son las medidas de seguridad visibles que existen, y en sí, que conozca la problemática a la cual se enfrentará, de manera muy simple y de carácter tentativo.

Para ello, el auditor debe contemplar los siguientes aspectos en dicha visita:

P.2.1 Visita preliminar de arranque

Ésta es una visita preparatoria al área de informática que será auditada, la cual tiene como finalidad que el auditor advierta de manera preliminar alguna de estas cuestiones:

¿Cómo se encuentran distribuidos los sistemas en el área?

¿Cuántos, cuáles, cómo y de qué tipo son los equipos que están instalados en el centro de sistemas?

¿Cuáles son, a simple vista, las principales características físicas de los sistemas que serán auditados?

¿Qué tipo de instalaciones y conexiones físicas hay en el área de sistemas, y cómo están distribuidas?

¿Cómo reacciona el personal ante la visita del auditor?

¿Cuáles son las medidas de seguridad visibles que existen?

¿Cómo actúan los usuarios y el personal del área; ya sea que ignoren la posible auditoría o cuando ya lo saben?

¿Qué limitaciones se observan para la realización de la auditoría?

En sí, el auditor debe obtener un panorama general del área que va a auditar, a fin de conocer la problemática que se le presentará en la auditoría. Contando con ese conocimiento inicial, podrá diseñar las medidas necesarias para una adecuada planeación de la auditoría y podrá establecer acciones concretas que le serán de gran ayuda en el desarrollo de dicha evaluación.

P.2.2 Contacto inicial con funcionarios y empleados del área

Dentro de esta visita preliminar, el auditor también aprovecha para establecer un contacto inicial con los funcionarios, empleados y usuarios del área de sistemas; el propósito es que observe sus reacciones ante la realización de la auditoría, y que identifique las posibles limitaciones y temores que influirán en la cooperación de dicho personal.

Conviene destacar que la visita del auditor casi nunca es bien recibida, más bien ocurre lo contrario, crea molestias en el personal, hace que éste se ponga a la defensiva y casi mecánicamente trate de evadir cualquier contacto con el auditor; en muchos casos tiende a ocultar información y presenta resistencia o se niega a cooperar en la auditoría; a veces busca bloquear la evaluación, entre muchos otros problemas a los cuales se enfrenta el auditor.

Esto es muy frecuente en el personal auditado, ya que todavía existe el nefasto concepto de que el auditor sólo va a tumbar las cabezas de los auditados; por esta razón, la mayoría de los empleados se resiste a la realización de cualquier auditoría y tratan de evitarla, sintiéndose culpables anticipadamente, aunque no sean responsables de ningun problema o mala acción que se llegue a detectar.

Debido a todo lo anterior, es muy conveniente que el auditor tenga un contacto preliminar con el personal del área que estará involucrado en la auditoría, ya que se pretende, utópicamente, que trate de limar asperezas mediante este contacto antes de iniciar la evaluación y que encuentre la coope-

ración de ese personal. En realidad, lo que se busca es que el auditor pueda vislumbrar el panorama al cual se enfrentará, para que de ahí diseñe su estrategia para el desarrollo de la evaluación, bajo la expectativa de los funcionarios, empleados y usuarios respecto a la auditoría.

P.2.3 Identificación preliminar de la problemática de sistemas

Además de lo anterior, en esta visita preliminar el auditor puede (y debe) aprovechar para saber cuál es la principal problemática a la que se enfrenta el área de sistemas, su personal y usuarios, su procesamiento de información y la administración de sus bases de datos, etcétera, aunque ésta sea sólo de carácter preliminar.

Lo que se pretende con esta identificación preliminar de las posibles dificultades que hay en los sistemas de la empresa, es que el auditor tenga un panorama anticipado del comportamiento de dichos sistemas, aunque éste sea de carácter muy somero y de dudosa confiabilidad.

P.2.4 Prever los objetivos iniciales de la auditoría

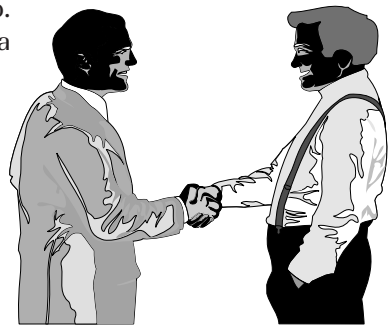
Otro aspecto que también se puede obtener de esta visita al área que será auditada, es que se puede anticipar cuáles objetivos se pueden satisfacer con la auditoría, o por lo menos tratar de entender cuáles son las metas que se quieren alcanzar con la evaluación.

Evidentemente, estos objetivos serían muy poco confiables y podrían desviar al auditor de los verdaderos objetivos de la auditoría; sin embargo, le servirían para normar su criterio respecto al objetivo que pretende alcanzar con dicha auditoría.

En el mejor de los casos, y contando con la habilidad, experiencia y conocimientos para identificarlos, el auditor podría señalar los objetivos que se pretenden satisfacer con su auditoría, o tal vez podría seleccionarlos con esta visita preliminar.

P.2.5 Calcular los recursos y personas necesarias para la auditoría

Otro beneficio de esta visita preliminar al área que será auditada, es la posibilidad de calcular tanto el tipo como la cantidad de recursos que serán necesarios para llevar a cabo la evaluación, contemplando los recursos de carácter humano, informático, material, técnico y económico.



Dicho cálculo se refiere al personal necesario para realizar la auditoría y al apoyo informático, así como a los recursos del área que se requieren en la revisión, entre los cuales destacan el personal informático y los apoyos adicionales del hardware, software, información, bases de datos, equipos y demás aspectos relacionados con el centro de cómputo.

Es evidente que la información que el auditor obtiene de la visita preliminar, se deriva de una ob-

servación personal o por entrevistas y pláticas de carácter informal, a veces aparentemente carentes de fundamentos. No obstante, con estas entrevistas también puede obtener datos importantes que le ayuden a calcular las necesidades de recursos aplicables en la auditoría de sistemas.

6.3.3 **P.3** Establecer los objetivos de la auditoría

El siguiente paso, después de haber identificado el origen de la auditoría y haber realizado una visita preliminar al área que será auditada, es establecer lo más claramente posible el (los) objetivo(s) de la auditoría, ajustándose lo más posible a las necesidades de la evaluación. El propósito es establecer claramente lo que se busca con este tipo de trabajo.

Conviene que iniciemos el tratamiento de este inciso con la siguiente definición:

Objetivo:

"En términos sencillos, los objetivos representan las condiciones futuras deseadas que los individuos, grupos u organizaciones luchan por alcanzar. En ese sentido se incluyen misiones, propósitos, metas, fines, cuotas y plazos [...] En ocasiones se utilizan para legitimar y justificar la función de la organización en la sociedad [...] En otro sentido, los objetivos podrían ser considerados como el conjunto de limitaciones a las que debe restringirse la organización [...] Los objetivos pueden ser considerados desde tres perspectivas primordiales: 1) el ambiental, limitaciones impuestas a la organización por la sociedad; 2) el organizacional, los objetivos de la organización, 3) el individual, los objetivos de los participantes en la organización [...]"[26]

Como podemos observar en esta definición, el objetivo representa las condiciones futuras que pretenden alcanzar los individuos, grupos u organizaciones, lo cual es sumamente aplicable para el caso de la auditoría de sistemas, ya que al establecer el objetivo de una auditoría se busca anticipar lo que se desea alcanzar, ya sea en el área de sistemas o en toda la institución.

Más concretamente, desde el punto de vista de los autores de referencia, en el caso de una auditoría de sistemas el establecimiento del objetivo es el establecimiento de lo que se pretende satisfacer con dicha auditoría; se incluyen los siguientes conceptos:

Misión:	*Deber moral que se impone a la realización de la auditoría de sistemas.*
Visión:	*La forma como se ve la realización de la auditoría y lo que se espera de ella.*
Propósitos:	*Objetivo que se pretende alcanzar con la auditoría.*
Metas:	*Fines específicos de la auditoría.*
Fines:	*Son los últimos aspectos que se busca satisfacer con la auditoría.*
Plazos:	*Los términos en unidades de tiempo en que se satisface el fin que se pretende con la auditoría.*

Dichos objetivos también se pueden complementar, de acuerdo con su ambiente de aplicación, con los aspectos que analizaremos a continuación:

P.3.1 Objetivo general

Es el fin global que se pretende alcanzar con el desarrollo de la auditoría de sistemas, en el cual se plantean todos los aspectos que se pretenden evaluar. De hecho, la determinación de este objetivo dará el fundamento en la realización de la auditoría y la idea total de lo que se va a cubrir con dicha auditoría.

P.3.2 Objetivos particulares

Son los fines individuales que se pretenden alcanzar con el desarrollo de la auditoría, ya sea de un área específica, de un sistema en especial o de alguna función en particular. Éstos pueden ser múltiples, de acuerdo con las necesidades concretas de evaluación.

P.3.3 Objetivos específicos de la auditoría de sistemas computacionales

Es la determinación, en forma detallada, de los fines que se pretenden alcanzar con la auditoría de sistemas, señalando concretamente las áreas a evaluar y, específicamente, los sistemas, componentes o elementos concretos que deben ser evaluados.

A continuación citaremos algunos ejemplos que pueden ser tomados como referencia para elaborar los objetivos de una auditoría de sistemas computacionales, de acuerdo con la empresa donde se realizará dicha auditoría:

Realizar una revisión con personal multidisciplinario y capacitado en el área de sistemas, a fin de evaluar dicha área y emitir un dictamen independiente sobre las operaciones del sistema y la gestión administrativa del área de informática.

Hacer una evaluación sobre el aspecto financiero, la utilización de los recursos financieros en las áreas del centro de información y el aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

Evaluar la utilización y aprovechamiento de los equipos de cómputo, de sus periféricos, de las instalaciones, mobiliario y equipos del centro de cómputo, así como del uso de sus recursos técnicos y materiales para el procesamiento de información.

Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.

Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de sus usuarios.

Realizar la evaluación de las áreas, actividades y funciones de la empresa, contando con el apoyo de los sistemas computacionales, los programas especiales y la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora.

6.3.4 **P.4** Determinar los puntos que serán evaluados en la auditoría

Después de haber determinado el origen de la auditoría y de establecer los objetivos concretos que se pretenden alcanzar con ésta, el siguiente paso es determinar los puntos concretos que serán evaluados.

Esta definición de los puntos que tienen que ser evaluados debe ser realizada considerando aspectos muy específicos de los sistemas computacionales, tales como los siguientes:

La gestión administrativa e informática del centro de cómputo

El cumplimiento de las funciones del personal informático y usuarios de los sistemas

El análisis, diseño y desarrollo de los sistemas computacionales

La operación de los sistemas computacionales

La capacitación y adiestramiento del personal y usuarios del sistema

La protección, custodia y niveles de acceso a las bases de datos

La protección y respaldo de archivos e información

La seguridad y protección de los usuarios, de la información, de los archivos y en general del centro de cómputo

Muchos otros aspectos que se deben considerar

Es de suma importancia destacar que la definición y establecimiento de los puntos que se deben evaluar es el elemento fundamental de apoyo del auditor, debido a que esto es producto de un análisis previo, tanto del origen de la auditoría y de la visita previa como de los objetivos que se pretenden satisfacer con la realización de esta auditoría. Sin este análisis previo difícilmente se pueden establecer los puntos que se deben evaluar. De ahí su importancia. Además, en este paso de la planeación de la auditoría debemos establecer aquellos aspectos de sistemas que vamos a evaluar, para después establecer las herramientas y la manera en que realizaremos la evaluación.

Un error muy común al realizar una evaluación de sistemas, es que dicha evaluación muchas veces se lleva a cabo sin una adecuada planeación, lo cual no sólo conduce al empobrecimiento de la evaluación, sino que el auditor tiene serias deficiencias en la aplicación de las herramientas de auditoría; por lo tanto, los resultados también son muy deficientes y de dudosa calidad. En algunos casos, esta planeación puede ser deficiente, limitada y sin bases reales, lo cual también conduce a las deficiencias antes indicadas.

En relación con la definición de los puntos que serán evaluados, pueden existir muchos criterios en la selección de tales puntos, los cuales, por su propia diversidad, pue-

den y deben ser establecidos de acuerdo a las necesidades de evaluación de la empresa, del equipo y del sistema operativo, así como a la forma de procesamiento de información que se tiene establecida en la empresa, a la experiencia, conocimientos y características profesionales del auditor, a las técnicas, métodos y procedimientos de auditoría de sistemas que se aplicarán, etc. En sí, dependerá de los muchos criterios que se establezcan en torno al desarrollo de la auditoría.

Debido a esa múltiple opción para definir los puntos que serán evaluados en una auditoría, a continuación proponemos una serie de puntos específicos, con los cuales sólo pretendemos anticipar un criterio de selección, más o menos homogéneo, de aquellos aspectos fundamentales que se deberán evaluar en una auditoría de sistemas. Cabe aclarar que este criterio de selección es de carácter general y sólo se presenta al nivel de sugerencia, y el responsable de la auditoría deberá determinar su aplicación real, de acuerdo con las necesidades de evaluación, con su experiencia profesional y con los conocimientos que tenga sobre este trabajo. Los puntos que se deben evaluar se pueden agrupar de la siguiente manera:

Evaluación de las funciones y actividades del personal del área de sistemas

Evaluación de las áreas y unidades administrativas del centro de cómputo

Evaluación de la seguridad de los sistemas de información

Evaluación de la información, documentación y registros de los sistemas

Evaluación de los sistemas, equipos, instalaciones y componentes

Evaluación de los recursos humanos del área de sistemas

Evaluación del hardware

Evaluación del software

Evaluación de la información y bases de datos

Evaluación de otros recursos informáticos

Evaluación de equipos, instalaciones y demás componentes

Elegir los tipos de auditoría que serán utilizados

Determinar los recursos que serán utilizados en la auditoría

Personal de auditoría de sistemas

Personal del área que será evaluada

Apoyo de los sistemas y equipos técnicos e informáticos

Apoyos materiales y administrativos

Otros apoyos

Recursos económicos

A continuación analizaremos una por una estas propuestas de puntos que se deben evaluar.

P.4.1 Evaluación de las funciones y actividades del personal del área de sistemas

La determinación de los puntos que se deben evaluar en estos aspectos se refiere a una valoración del cumplimiento de las funciones y actividades establecidas para cada uno los puestos que integran el centro de cómputo, así como de la observancia de las obligaciones de los funcionarios, usuarios o personal del área.

El propósito fundamental de esta evaluación es verificar si existen o no las funciones y actividades para cada uno de los puestos del área, si se encuentran por escrito y contempladas en documentos formales o informales, si tienen la suficiente difusión, si el personal que las debe cumplir las conoce y tiene acceso a los documentos donde se encuentran, y *cómo, en qué grado y de qué manera los ocupantes de esos puestos* satisfacen las funciones que tienen encomendadas.

También se evalúa el aprovechamiento del sistema y de sus recursos por medio del cumplimiento de estas funciones y actividades.

P.4.2 Evaluación de las áreas y unidades administrativas del centro de cómputo

En este punto se busca evaluar, mediante técnicas y procedimientos de auditoría, todos aquellos aspectos que pueden influir en el grado de cumplimiento de las funciones, actividades y operación de las áreas y unidades de trabajo del centro de cómputo. Esto se puede realizar a través de la evaluación de carácter individual, es decir una área a la vez, o de manera integral, contemplando a todas las áreas del centro de cómputo.

Es importante señalar que uno de los principales criterios para el desarrollo de esta evaluación, es que se debe sujetar al estilo de administración del centro de cómputo, así como a las características, tipo y tamaño de los equipos computacionales, a la distribución de los sistemas y la forma de operación del citado centro de cómputo. Lo mismo para el acatamiento en la evaluación de la estructura de organización por áreas, o en su caso por la división del trabajo de dichos centros.

Respecto a estas áreas y unidades de trabajo del centro de cómputo, existen muchos criterios y opiniones que se deben contemplar al realizar una evaluación.

P.4.3 Evaluación de la seguridad de los sistemas de información

Uno de los rubros que están incrementando su popularidad dentro del ambiente informático, es el relacionado con la seguridad en el área de sistemas; con ello se incrementa cada día más la necesidad de evaluar la seguridad y protección de los sistemas, ya sea en los accesos al centro de cómputo, en el ingreso y utilización de los propios sistemas y en la consulta y manipulación de la información contenida en sus archivos, la seguridad de las instalaciones, del personal y los usuarios de sistemas, así como de todo lo relacionado con el resguardo de los sistemas computacionales.

Es evidente que uno de los aspectos básicos que se deben contemplar en la evaluación de sistemas, es precisamente la protección y resguardo de la información de la empresa, tanto en el hardware como el software, así como de los equipos adicionales que ayudan al adecuado funcionamiento de los sistemas. En esta evaluación también se incluyen el acceso al área de sistemas, el acceso al sistema, la protección y salvaguarda de los activos de esta área, las medidas de prevención y combate de siniestros, y muchos otros aspectos que se pueden valorar mediante una auditoría de sistemas.

Para un mejor entendimiento de estos puntos, a continuación veremos las principales áreas de seguridad que se pueden evaluar en una auditoría de sistemas:

Evaluación de la seguridad física de los sistemas

Evaluación de la seguridad lógica del sistema

Evaluación de la seguridad del personal del área de sistemas

Evaluación de la seguridad de la información y las bases de datos

Evaluación de la seguridad en el acceso y uso del software

Evaluación de la seguridad en la operación del hardware

Evaluación de la seguridad en las telecomunicaciones

P.4.4 Evaluación de la información, documentación y registros de los sistemas

Dentro de lo que se contempla en la evaluación a las áreas de sistemas se encuentra todo lo relacionado con la información, ya sea de las bases de datos y sistemas de almacenamiento, los respaldos o simple y sencillamente la forma de archivar los datos por parte de los usuarios del sistema.

Precisamente con esta apreciación se busca evaluar la protección y custodia del activo más valioso de los sistemas, la información, e incluso como se hace la captura, procesamiento y emisión de los resultados. Todo de acuerdo a las características, forma de procesamiento y sistemas de la empresa.

P.4.5 Evaluación de los sistemas, equipos, instalaciones y componentes

En esta evaluación intervienen muchos factores, tanto de la auditoría como de la propia área de sistemas, ya que se pretende dictaminar como están funcionando casi todos los componentes del sistema computacional de la empresa.

Para esta auditoría es conveniente dividir la evaluación en aspectos concretos que se pueden dictaminar por separado o en forma integral; por esta razón proponemos evaluar los siguientes puntos:

P.4.5.1 Evaluación de los recursos humanos del área de sistemas

Es la evaluación del adecuado cumplimiento de las actividades, tareas y funciones de los integrantes del área de sistemas. En esta valoración se incluye una opinión sobre la experiencia, conocimientos y habilidades que debe tener este personal para el manejo de las actividades y operaciones del sistema de cómputo, así como la disponibilidad y grado de cumplimiento de sus funciones.

P.4.5.2 Evaluación del hardware

Es la evaluación del aprovechamiento y utilización de los sistemas de cómputo, de sus componentes y conexiones, así como de sus periféricos y equipos asociados. Con esta evaluación se busca dictaminar si se satisfacen las necesidades de procesamiento de información de la empresa.

P.4.5.3 Evaluación del software

Es la evaluación del aprovechamiento y explotación de los sistemas operativos, lenguajes, programas de aplicación, paqueterías y de los demás aspectos que integran el software institucional, así como de los sistemas y programas de desarrollo del mismo. Con la identificación de estos objetivos se busca dictaminar si se satisfacen las necesidades de procesamiento de información de la empresa.

P.4.5.4 Evaluación de la información y las bases de datos

Es la evaluación de la protección y el aprovechamiento de los sistemas de almacenamiento de la información que se procesa en el área, en cuanto al acceso a las bases de datos, los niveles de consulta, manipulación y modificación de los datos, los programas y paqueterías de aplicación y manejo de la información institucional, así como a la protección y operación relacionadas con el manejo de los archivos de información.

Con esta evaluación se busca dictaminar si se satisfacen las necesidades de protección y operabilidad de la información de la empresa, en cuanto al volumen, periodicidad, oportunidad, utilidad y disponibilidad de las bases de datos institucionales.

P.4.5.5 Evaluación de otros recursos informáticos

Es la evaluación del aprovechamiento de los demás recursos informáticos con que cuenta el área de sistemas para el procesamiento de la información, tales como sistemas de telecomunicación internos o externos, sistemas multimedia para explotación institucional, sistemas de protección de información y de acceso a las bases de datos, avances tecnológicos en los programas y paqueterías de aplicación institucional.

Con esta evaluación se busca dictaminar si se satisfacen las necesidades de protección y operabilidad de la información de la empresa.

Evaluación de equipos, instalaciones y demás componentes

Es la evaluación del aprovechamiento de los bienes muebles e inmuebles, instalaciones y otros recursos que están directamente involucrados con el bienestar y comodidad del personal y usuarios del área de sistemas, así como del aprovechamiento de la comunicación telefónica y de datos, ya sea dentro de la empresa o con sistemas computacionales externos, tales como redes de cómputo, módems u otros sistemas de telecomunicación.

Con esta evaluación se busca dictaminar si las conexiones de **voz** (*telefónicas*), de **datos** (*módems, redes y otros sistemas de comunicación*) y de **luz** (*las conexiones de energía eléctrica*) son las adecuadas para lograr las metas de operabilidad del área de sistemas.

P.4.6 Elegir los tipos de auditoría que serán utilizados

En esta etapa de la planeación de la auditoría de sistemas, una vez que determinó los puntos que serán evaluados, es imprescindible que el encargado de ésta determine los tipos de auditoría, las herramientas e instrumentos y los métodos de evaluación que utilizará para dictaminar acerca del funcionamiento del área de sistemas, de acuerdo con sus necesidades especificas de revisión y con las características y requerimientos especiales que se pueden auditar en sistemas.

Evidentemente es difícil establecer un tipo de auditoría que se pueda aplicar uniformemente en la evaluación de los sistemas de una empresa, ya que en mucho dependerá de los objetivos que se busca satisfacer con la auditoría de sistemas, así como del tópico que será analizado, y desde qué punto de vista lo evaluara el auditor.

Es indiscutible que no es lo mismo evaluar el funcionamiento de una red de computo, que evaluar la seguridad en el acceso físico de las instalaciones del área; tampoco se aplican los mismos procedimientos para evaluar las metodologías de análisis y diseño de los nuevos sistemas, que para verificar la veracidad de los resultados de un procesamiento de datos en un microsistema; cada uno de éstos tiene aspectos diametralmente opuestos entre sí, los cuales deben ser forzosamente auditados desde diferentes puntos de vista y con diferentes métodos y herramientas.

Estas son las razones por las que el auditor tiene que determinar el tipo de auditoría que va a realizar, de acuerdo con sus objetivos; por eso es de suma importancia identificar cada uno de los anteriores aspectos que hemos tratado a lo largo de esta etapa de planeación.

P.4.7 Determinar los recursos que serán utilizados en la auditoría

Es necesario considerar que los recursos, cualesquiera que sean, son de carácter limitado; por esta razón, después de haber identificado los puntos que serán evaluados, es de suma importancia determinar los recursos que se necesitarán para poder realizar la auditoría de sistemas, siempre en concordancia con lo planeado.

En el caso especial de esta auditoría y por lo técnico del ambiente donde se realiza, estos recursos tienen que ser muy especializados, tanto para la auditoría de sistemas como para el aspecto informático.

Para una mejor comprensión de cómo determinar los recursos necesarios para la auditoría de sistemas, a continuación señalaremos brevemente los principales aspectos de estos recursos:

P.4.7.1 Personal para la auditoría de sistemas

Es el personal especializado en auditoría de sistemas, el cual aplica sus conocimientos, habilidades y experiencia en las diferentes disciplinas de la auditoría, utilizando para ello las técnicas, procedimientos, métodos de evaluación, herramientas e instrumentos de revisión especializados y tradicionales para la evaluación de sistemas.

En los capítulos 9, 10 y 11 de este libro se indican algunas de estas herramientas.

Cabe destacar que este personal tiene que ser especializado en las técnicas y procedimientos de auditoría, pero a la vez debe tener amplios conocimientos y experiencia en el área de sistemas; en muchos casos, es preferible que sea personal multidisciplinario para que cubra todos los aspectos relacionados con sistemas.

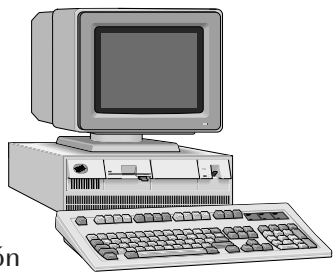
P.4.7.2 Personal del área que será evaluada

Es la estimación de los recursos del área de sistemas con los que contará el auditor para la evaluación.

Debemos señalar que este personal no está a disposición del auditor y que no tiene ningún tipo de autoridad sobre él ni injerencia en su trabajo. Lo más que les puede pedir es que cooperen en la realización de la auditoría proporcionando la información y que participen en las entrevistas, cuestionarios, pruebas y demás herramientas que utilizará para evaluar los sistemas.

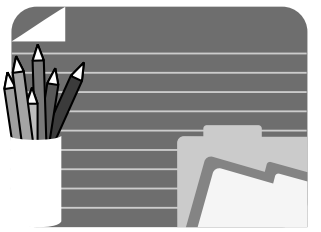
P.4.7.3 Apoyo de los sistemas y equipos técnicos e informáticos

Es la selección de los recursos técnicos, equipos y sistemas computacionales que serán necesarios para la auditoría de sistemas, los cuales pueden ser muy diversos y especializados, de acuerdo con las necesidades concretas establecidas en la planeación de la evaluación. Dichos recursos incluyen el hardware, software, instalaciones, el personal especializado en la operación de los sistemas, los sistemas operativos, los programas de aplicación, las paqueterías, las bases de datos y la información del área auditada.



Además se contemplan todos los aspectos logísticos que necesitará el auditor para el desempeño de sus actividades, tales como sistemas computacionales para su uso exclusivo, software de evaluación especializado para auditoría, apoyo técnico informático especializado en sistemas computacionales, materiales consumibles de sistemas y todos los demás requerimientos informáticos, de acuerdo a las necesidades específicas del área que será evaluada.

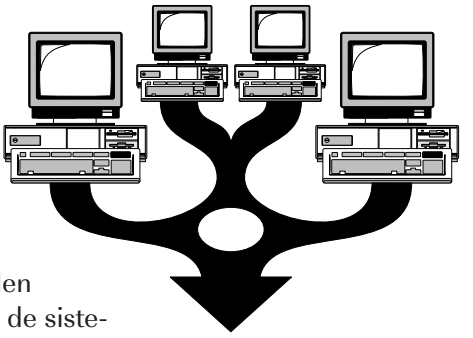
P.4.7.4 Apoyos materiales y administrativos



Éstos son los recursos que no tienen que ver con los sistemas, pero que son imprescindibles para el buen desempeño de los auditores, tales como la asignación de oficinas privadas y lugares de trabajo exclusivos, el apoyo de mobiliario, equipos, materiales y útiles de oficina, así como el apoyo logístico y secretarial necesario para realizar una evaluación. Todo ello de acuerdo con las necesidades contempladas en la auditoría.

Conviene destacar que el auditor necesita de todo el apoyo logístico y administrativo del área de sistemas para que no tenga preocupaciones ni dificultades administrativas y pueda realizar una correcta evaluación; en caso de que no exista este apoyo, el auditor recurrirá al apoyo administrativo de cualquier otra área de la empresa, ya que es importante que realice sus actividades lo más cómodamente posible.

P.4.7.5 Otros apoyos



En algunos casos, dependiendo de las necesidades específicas de la evaluación de sistemas, es necesario contar con recursos especializados para la revisión de ciertos aspectos del área de sistemas que se tengan que auditar de manera particular, los cuales la mayoría de las veces no son de uso común en dicha área.

Algunos ejemplos de estos aspectos pueden ser los programas especializados de evaluación de sistemas, hardware, equipos y periféricos asociados; también los sistemas de telecomunicación, de interredes, los protocolos de comunicación, además de otros aspectos técnicos especializados que sirven de apoyo para la evaluación de los sistemas, de las instalaciones o de cualquier otro rubro importante que se tenga que evaluar, de acuerdo a las necesidades de la auditoría y de la propia empresa.

P.4.7.6 Recursos económicos

Otro de los recursos de gran importancia para el desarrollo de una auditoría es el apoyo financiero que necesita el auditor, en el caso de auditorías externas, para transportarse al lugar donde esté el área o empresa que vaya a evaluar.

El auditor necesita comprobar los gastos efectuados durante la evaluación o, por el contrario, dichos gastos pueden ser libres de comprobación, de acuerdo a las normas y políticas de la empresa; estos gastos están representados por los siguientes rubros:

Viáticos: *Es la cantidad de dinero que se le asigna al auditor, por día, semana o cualquier otro periodo, para cubrir sus gastos de viaje, estancia y alimentación durante la evaluación de los sistemas de la empresa.*

Pasajes: *Es la cantidad de dinero que se entrega al auditor para cubrir su traslado al lugar donde realiza la evaluación; en algunos casos, es la entrega de los boletos y derechos de viaje que amparan el uso de los transportes.*

Otros gastos: *Es la cantidad de dinero que se entrega al auditor para cubrir sus gastos inherentes al desarrollo de la evaluación, ya sea para transporte, gasolina, casetas de peaje, derechos, compras de material informático, utensilios de oficina o cualquier otro gasto.*

6.3.5 **P.5** Elaborar planes, programas y presupuestos para realizar la auditoría

Después de haber considerado todos los puntos antes señalados, el siguiente paso es realizar la planeación formal de la auditoría de sistemas, en la cual se concreten los planes, programas y presupuestos para dicha auditoría; es decir, se deben elaborar los documentos que contemplen los planes formales para el desarrollo de la auditoría, los programas en donde se delimiten perfectamente las etapas, eventos, actividades y los tiempos de ejecución para cumplir con el objetivo, así como los presupuestos de la auditoría, documentos en donde se deben asignar los costos de los recursos que serán utilizados y el tiempo que serán utilizados para determinada actividad.

Antes de continuar, conviene recordar que en las definiciones de la sección 6.3. (***1ª etapa***: *Planeación de la auditoría de sistemas computacionales*) se señalan los aspectos que se deben considerar en esta actividad.

P.5.1 Elaborar el documento formal de los planes de trabajo para la auditoría

Es la elaboración específica y escrupulosa de los planes formales de trabajo para la auditoría de sistemas computacionales. Estos planes se presentan en un documento oficial llamado *plan de auditoría de sistemas*, el cual contiene todos los aspectos

relacionados con la realización de dicha auditoría. A continuación tenemos algunos de estos aspectos:

Las actividades que se van a realizar, los responsables de realizarlas, los recursos materiales y los tiempos

Los eventos que servirán de guía de acción

La estimación de los recursos humanos, materiales e informáticos que serán utilizados

Los tiempos estimados para las actividades y para la propia auditoría

Los auditores responsables y participantes en dichas actividades

Las demás especificaciones del programa de trabajo para la auditoría

El auditor responsable de elaborar la planeación de la auditoría determinará, en base a sus conocimientos, habilidades y experiencia, el contenido formal de este documento; sin embargo, en este inciso presentamos los aspectos de forma y contenido que se deben considerar en el documento formal.

P.5.1.1 Carátula de identificación del plan de auditoría

Es la primera hoja del documento de planeación, en la cual se establecen lo más claramente posible los siguientes puntos:

AUDITORÍA EN SISTEMAS A.C.

FECHA			HOJA
DD	MM	AA	
26	3	96	26 de 29

EMPRESA: Instituto Nacional de Migración

PERÍODO: 01 al 16 de marzo de 1996

AUDITOR: Ma. Araceli Arceo Gálvez

ÁREA AUDITADA: Dirección de Informática y Estadística

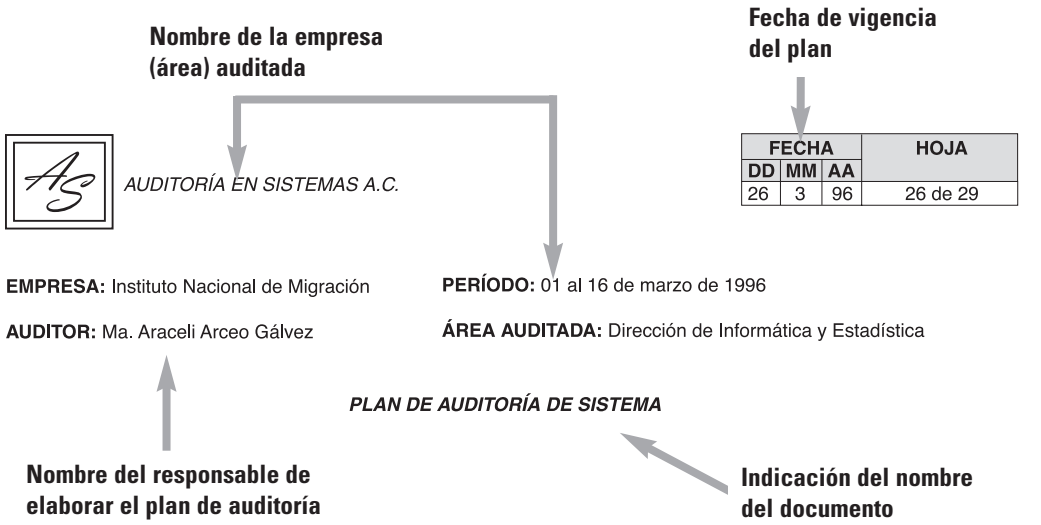
PLAN DE AUDITORÍA DE SISTEMA

Nombre y logotipo de la empresa responsable de la auditoría

Contiene la identificación oficial de la empresa responsable de realizar la auditoría, en caso de ser auditoría externa; es indispensable que esta carátula esté en un papel membreteado de la institución, despacho o auditor independiente que la llevará a cabo. Si la responsable de realizar esta evaluación es el área de auditoría interna de la empresa, el logo y nombre será de la empresa, pero con la clara identificación del área de auditoría interna.

Indicación del nombre del documento

Es la clara identificación de que se trata de un documento oficial, en el cual se indica claramente que su contenido se refiere *al plan de auditoría de sistemas de la empresa* y/o del área que se indica en la misma carátula.:



Nombre de la empresa (área) auditada

Se anota lo más notoriamente posible el nombre la de empresa o del área específica de sistemas que será auditada, de preferencia inmediatamente después del punto anterior.

Nombre del responsable de elaborar el plan de auditoría

Se señala el nombre del auditor responsable de llevar a cabo la auditoría; por lo general este auditor es el mismo que supervisa la realización de la auditoría, aunque nada impide que otro lo haga.

Fecha de vigencia del plan

En algunos casos es el periodo de realización de la auditoría, desde que inicia hasta que concluye con la entrega del dictamen formal. En otros casos es la fecha en que se presenta a discusión y aprobación el plan de auditoría. En ambos casos deberá indicar el día (dos dígitos), el mes (dos dígitos) y el año (cuatro dígitos).

P.5.1.2 Índice de contenido

Es conveniente que en estos documentos siempre se incluya una sección en donde se señalen, por nombre del contenido o apartados y por página, todos los puntos en que se dividió el plan de auditoría, con objeto de ayudar a una rápida consulta del documento.

P.5.1.3 Definición de objetivos

Es la definición formal, por escrito, de los objetivos que se pretenden alcanzar con la auditoría, conforme a lo señalado al principio de este capítulo.

P.5.1.4 Delimitación de estrategias para el desarrollo de la auditoría

En algunos casos es conveniente que en este plan se contemplen las estrategias para las diferentes partes de la auditoría de sistemas; además puede contener las estrategias de acción y de actuación de los participantes en la revisión.

P.5.1.5 Planes de auditoría

Son los planes formales de la auditoría, en los cuales se detalla cada una de las acciones para la evaluación; estos planes serán presentados de acuerdo a las preferencias y necesidades específicas de auditoría de la empresa, así como de acuerdo a los estándares de documentación establecidos por la empresa responsable de la evaluación.

P.5.1.6 Definición de normas, políticas y lineamientos para el desarrollo de la auditoría

Es muy conveniente que los aspectos que regularán las actividades de los auditores estén perfectamente establecidos en este documento, incluyendo sus alcances y limitaciones. También se deben establecer las políticas y lineamientos de acción, de acuerdo al tipo de auditoría y a la experiencia de los auditores en revisiones similares; todo de acuerdo con las especificaciones de las empresas, tanto de la responsable de realizar la auditoría como de la que será auditada.

Éstos son algunos de los puntos más importantes que debe contener este documento.

P.5.2 Contenido de los planes para realizar la auditoría

Es la elaboración escrupulosa de todos los planes formales que el auditor debe plasmar en un documento oficial llamado *plan de auditoría de sistemas*, el cual debe contener muy detalladamente las fases, etapas, actividades, recursos y tiempos para realizar la auditoría.

Es evidente que el auditor determinará el contenido mínimo de estos planes, en base a sus conocimientos y experiencia; sin embargo, en la elaboración de este documento guía de auditoría, cuando menos se debe considerar los siguientes aspectos:

P.5.2.1 Definir los objetivos finales de la auditoría

Es la definición formal de los objetivos finales de la auditoría, mismos que establecimos perfectamente en el punto P.3, "Establecer los objetivo de la auditoría", de esta primera etapa de planeación.

Estos objetivos se deben redactar de manera sencilla, objetiva y concreta en el documento oficial de la auditoría.

P.5.2.2 Establecer las estrategias para realizar la auditoría

Como producto de las anteriores etapas de planeación, en este documento se redactan en forma precisa las estrategias para realizar la auditoría, con el fin de que los auditores las entiendan rápida y perfectamente.

P.5.2.3 Diseñar las etapas, eventos y tareas en que se dividirá la auditoría

Es la determinación precisa y detallada de cada una de las etapas, eventos y tareas que deberá cumplir el personal encargado de realizar la auditoría, de acuerdo a lo definido en los anteriores puntos de esta planeación.

P.5.2.4 Calcular la duración de las tareas y eventos para satisfacer los objetivos de la auditoría

Una vez que fueron precisadas las etapas, eventos y tareas concretas del plan para la auditoría, el siguiente paso es estimar, lo más exacto posible, su duración, de acuerdo con su importancia, necesidades concretas y forma en que se satisfacerá en objetivo concreto de la auditoría. También se debe considerar la disponibilidad de los recursos para la auditoría.

P.5.2.5 Distribuir los recursos que serán utilizados en las diferentes etapas, actividades y tareas de la auditoría

Con base en los aspectos que analizamos en la etapa de planeación, y con la perfecta definición de las etapas, eventos y tareas indicadas en la parte anterior, en esta parte se establece, en forma precisa y lo más detalladamente posible, la asignación de los recursos que serán utilizados en la auditoría, así como el tipo de recursos, el tiempo que serán utilizados en la tarea, y en sí todos los detalles sobre su utilización.

P.5.2.6 Confeccionar los planes concretos para la auditoría

Es el establecimiento formal, de preferencia por escrito y de manera gráfica, de las etapas, eventos, tareas y actividades que integran el plan de auditoría, incluyendo la duración de cada uno de estos aspectos, así como el tiempo de asignación de los recursos, el tipo de recursos y en sí todos los aspectos formales del plan de auditoría, los cuales hacen que este documento sirva de base a los auditores para realizar la evaluación.

Debemos reiterar que el auditor es el responsable de identificar y establecer los puntos que serán evaluados, con base en un estudio concienzudo de lo señalado en las secciones anteriores.

P.5.3 Elaborar el documento formal de los programas de auditoría

En este documento se anotan, de preferencia en forma de gráfica, todas las etapas, eventos y actividades que se realizarán durante la auditoría; además, se anota el período de duración de cada una de las partes en que se dividió el trabajo de evaluación. En algunos casos, también se anotan los recursos que serán utilizados y la forma de identificarles, y si es necesario, su costo.

AUDITORÍA EN SISTEMAS COMPUTACIONALES

VIGENCIA	DD	MM	AA
DEL	28	3	98
AL	31	4	98

EMPRESA: Instituto Nacional de Computación **PERÍODO:** 01 al 16 de marzo de 1996

AUDITOR: Ma. Araceli Arceo Gálvez **ÁREA AUDITADA:** Dirección de Informática y Estadística

PLAN DE AUDITORÍA DE SISTEMA

ACTIVIDAD			SEMANAS							
No.	**Nombre**	**responsable**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Elaborar plan de auditoría	J. Dpto. asignado								
2	Aprobar plan de auditoría	Director								
3	Prepara instrumentos de remisión	Resp. Auditor								
4	Iniciar preparativos	Aud. Senior								
5	Cobrar viáticos y pasajes	Aud. Asignados								
6	Iniciar viaje	Aud. Asignados								
7	Iniciar auditoría	Aud. Asignados								
8	Auditar gestión informática	Aud. Sr. 1								
9	Auditar Bases de datos	Aud. Sr. 2								
10	Auditar Sistemas de cómputo	Aud. Sr. 3								
11	Auditar personal informático	Aud. Sr. 4								
12	Auditar la seguridad de los sistemas	Aud. Sr. 5								
13	Presentar borrador de inforrme	Resp. Auditor								

Este documento debe estar unido al anterior, ya que es parte integral de él, y debe contener los mismos aspectos señalados para el plan de auditoría, sólo que se complementa con los siguientes apartados:

P.5.3.1 Gráfica del programa de actividades

Es un documento visual de fácil comprensión, en donde se describe detalladamente y en forma de gráfica el plan de trabajo; es decir, todas las etapas, eventos y actividades contempladas para la evaluación de los sistemas, así como su duración y los recursos necesarios para llevarlas a cabo. Este documento puede ser una *gráfica de Gantt, de ruta crítica, de Pert* o cualquier otra herramienta de planeación y control.

En este documento no sólo se describen las etapas y actividades de la auditoría, sino que también se puede utilizar para su control y supervisión.

P.5.3.2 Definición de las etapas y eventos que se deben llevar a cabo

Es la descripción documental y detallada de la forma de planear el desarrollo y cumplimiento de las etapas o eventos en que está dividida la evaluación de los sistemas. Todo de acuerdo con lo determinado en la planeación.

P.5.3.3 Definición de las actividades y tareas

Es la descripción detallada de las acciones y pasos que se deben realizar en cada una de las etapas de la evaluación, de las herramientas, instrumentos y métodos de evaluación que se van a utilizar, así como de los recursos para su desarrollo.

P.5.4 Elaborar los programas de actividades para realizar la auditoría

En este punto se establecen por escrito y de preferencia en forma de gráfica, todos los tiempos en que se llevará a cabo cada una de las etapas, eventos y actividades de la auditoría, considerando para ello el período de duración de cada una de las partes en que se dividió el trabajo de evaluación. En algunos casos también se anota el tiempo que se utilizarán los recursos y, de ser necesario, sus periodos de asignación, descanso y cualquier otro uso de estos recursos, tanto en lo individual como en lo colectivo.

PLAN DE AUDITORÍA DE SISTEMA

ACTIVIDAD			SEMANAS							
No.	**Nombre**	**responsable**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Elaborar plan de auditoría	J. Dpto. asignado								
2	Aprobar plan de auditoría	Director								
3	Prepara instrumentos de remisión	Resp. Auditor								
4	Iniciar preparativos	Aud. Senior								
5	Cobrar viáticos y pasajes	Aud. Asignados								
6	Iniciar viaje	Aud. Asignados								
7	Iniciar auditoría	Aud. Asignados								
8	Auditar gestión informática	Aud. Sr. 1								
9	Auditar Bases de datos	Aud. Sr. 2								
10	Auditar Sistemas de cómputo	Aud. Sr. 3								
11	Auditar personal informático	Aud. Sr. 4								
12	Auditar la seguridad de los sistemas	Aud. Sr. 5								
13	Presentar borrador de inforrme	Resp. Auditor								

Este documento se elabora con el anterior, ya que es parte integral del documento de planeación, y debe contener los mismos aspectos señalados para el plan de auditoría.

Este documento se divide en esta parte sólo para su identificación y conocimiento, ya que realmente no puede ser separado, y se complementa con los siguientes puntos, los cuales también se pueden elaborar por separado o en forma conjunta:

P.5.4.1 Definir de manera precisa las etapas de la auditoría

El responsable de la planeación de la auditoría de sistemas deberá definir, lo más preciso que pueda, las posibles etapas en que se dividirá la misma, buscando ser congruente y coherente en la división de las actividades, en cuanto al volumen de trabajo, importancia del aspecto que será evaluado, en los recursos requeridos y en el peso específico que tendrán dichas etapas para toda la auditoría.

Esta definición de las etapas de la auditoría debe estar directamente relacionada con lo determinado en los puntos anteriores y con los objetivos que se buscan satisfacer con la auditoría.

P.5.4.2 Identificar concretamente los eventos que se deben llevar a cabo en cada etapa de la auditoría

Tomando como base las etapas establecidas con anterioridad, el siguiente paso es definir, lo más concretamente posible, cada uno de los eventos que integrarán cada una de las etapas propuestas en que se dividió la auditoría, de acuerdo con las necesidades concretas identificadas en los puntos anteriores. Se recomienda utilizar la gráfica de ruta crítica, la gráfica de Gantt o el programa Project de Microsoft.

Tomando el evento como un suceso esperado, al cual se debe llegar después de una serie de actividades, la identificación de todos estos eventos es una parte fundamental en la definición de las etapas en que se divide la auditoría de sistemas.

P.5.4.3 Delimitar lo más claramente posible las actividades, tareas y acciones para cada evento

Una vez que se han definido los eventos que se requieren para integrar las etapas en que se dividió la auditoría, el siguiente paso es determinar, lo más clara y concretamente posible, todas y cada una las actividades y tareas concretas que se deberán llevar a cabo para cada evento.

El auditor será el responsable de establecer estas actividades, tareas y acciones.

P.5.4.4 Distribuir los recursos que serán utilizados en las diferentes etapas, eventos, actividades y tareas

Una vez establecidas todas las acciones, actividades y tareas para cada uno de los eventos de las etapas de la auditoría, el siguiente paso es determinar tanto los recursos humanos como los recursos adicionales que serán utilizados en cada una de esas etapas, ya sea en forma individual o en forma conjunta.

P.5.4.5 Calcular la duración de las etapas, actividades y tareas planeadas para la auditoría

Otro de los puntos fundamentales para elaborar el programa de auditoría, es determinar la duración de cada uno de los eventos, etapas, actividades tareas y acciones que

integrarán dicho programa; para ello, se deben considerar los recursos que se utilizarán en la evaluación, ya sean de carácter humano o los adicionales que apoyan el trabajo del auditor.

Dicha estimación se debe hacer de acuerdo a la disponibilidad de los recursos, a la prioridad de cada etapa y a la habilidad del responsable de la planeación.

P.5.4.6 Determinar fechas de inicio y fin de las etapas, actividades y tareas

Contando con la estimación de recursos, la duración de cada evento y la asignación de las actividades, tareas y acciones necesarias para realizar la auditoría, se podrán establecer las fechas de inicio y fin, no sólo de la auditoría, sino de cada una de sus etapas, fases, actividades y eventos. Todo de acuerdo con lo determinado en la etapa de planeación y lo establecido en cada uno de las partes de este programa.

P.5.5 Elaborar los presupuestos para la auditoría

Este presupuesto es parte integral los dos documentos anteriormente analizados, ya que se contemplan los recursos que se utilizarán en el plan y programa de trabajo, sólo que se agregan los costos y el tiempo que se utilizarán estos recursos durante la evaluación.

Para complementar los anteriores documentos, veremos que en la elaboración de presupuestos se deben contemplar, dentro de un mismo documento, cada uno de los siguientes aspectos:

P.5.5.1 Asignación de los costos de los recursos

Es la designación en número, tiempo y costo que, de acuerdo con los programas de trabajo de la auditoría, se hace para utilizar los recursos contemplados para el desarrollo de dicha auditoría.

P.5.5.2 Control de los costos de los recursos

Debido a lo limitado de los recursos para el cumplimiento de las actividades de la auditoría, y aunque no es indispensable esta parte del presupuesto, es conveniente dar a conocer en este documento los costos de dichos recursos, con el propósito de valorar el aprovechamiento y adecuada utilización no sólo de los recursos humanos, sino de los otros recursos informáticos.

P.5.5.3 Seguimiento y control de los planes, programas y presupuestos

Propiamente esta parte no es del contenido de un presupuesto de una auditoría, sino es una herramienta de control utilizada por el responsable de la auditoría; sin embar-

go si es conveniente su inclusión en este documento de presupuesto. Aunque también pude formar parte de cualquier de los anteriores; lo importante es que se contenga en el documento.

De este presupuesto no se citan ejemplos, en virtud de que sería demasiado presuntuoso, a la vez que inoperante, el tratar de encasillar el desarrollo de los presupuestos en un solo formato, razón por la cual, únicamente se deja al nivel de mención este punto.

6.3.6 P.6 Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría

El siguiente paso es determinar los documentos y medios con los cuales se llevará a cabo la revisión a los sistemas de la empresa, lo cual se logrará a través de la selección o diseño de los métodos, procedimientos, herramientas e instrumentos necesarios,* de acuerdo con lo indicado en los planes, presupuestos y programas establecidos para la auditoría. Para lograr esto, sugerimos considerar los siguientes puntos:

P.6.1 Establecer la guía de ponderación de los puntos que serán evaluados

Una de los aspectos más importantes que se deben considerar para realizar una auditoría de sistemas es la técnica de ponderación, la cual, como se señala en el capítulo 9 de este libro, es un método especial que ayuda a definir la forma de valorar cada una de las partes importantes del área de sistemas, con el fin de aplicar los mismos criterios de evaluación en todos los aspectos que serán evaluados.

El propósito de utilizar esta herramienta es buscar un equilibrio entre las áreas o sistemas de informática que tienen mayor peso y trascendencia, con aquellas que tienen poco peso e importancia en la evaluación; es decir, para que el auditor realice la evaluación de todas las áreas y sistemas de la misma manera, y de acuerdo con lo establecido en los planes, programas y presupuestos de la auditoría.

Como hemos visto, esta técnica de evaluación es un instrumento que permite al auditor compensar las posibles descompensaciones de las áreas o sistemas de informática que tienen mayor peso e importancia en la evaluación, comparadas con aquellas que tienen poco peso e importancia. Esta ponderación se logra mediante los siguientes puntos:

P.6.1.1 Definir las áreas y puntos de sistemas que serán auditados

De acuerdo con la planeación de la auditoría, el primer paso es definir las áreas, los aspectos de sistemas o los puntos de interés que se van a evaluar, dándole un peso es-

* En los capítulos 9, 10 y 11 se presentan estas herramientas, métodos y procedimientos utilizados en este punto.

pecífico a cada factor; el auditor establece ese peso a su libre albedrío, y de acuerdo a su experiencia, habilidad y conocimientos sobre el tema.

Lo que se busca en este paso es definir los factores de mayor jerarquía o los más representativos de un grupo o sector de sistemas que se desea evaluar. El propósito fundamental de esta definición es darle a cada uno de estos factores un valor porcentual (*peso específico*), el cual representará la importancia de cada factor en toda la evaluación.

P.6.1.2 Definir el peso de la ponderación por las áreas y puntos que serán evaluados

Una vez que fueron definidas las áreas, tópicos o aspectos que serán ponderados, el siguiente paso es asignarle un valor porcentual a cada uno de los factores elegidos, el cual es un valor particular que establece el auditor para cada una de las actividades que serán evaluadas, de acuerdo a su libre albedrío. La suma total de estas actividades invariablemente será 100%. El ejemplo del siguiente cuadro es una aplicación de un peso específico determinado para una gestión informática.

Factores primarios que serán ponderados	**Peso específico**
1. Objetivos del centro de informática	10 %
2. Estructura de organización	10 %
3. Funciones	15 %
4. Sistema de información	20 %
5. Personal y usuarios	15 %
6. Documentación de los sistemas	2 %
7. Actividades y operación del sistema	14 %
8. Configuración del sistema	4 %
9. Instalaciones del centro de informática	10 %
Peso total de la ponderación	**100 %**

P.6.1.3 Realizar el documento de ponderación de la auditoría

Después de los puntos anteriores, el siguiente paso es elaborar el documento de ponderación de manera formal, sometiéndolo a la opinión y consenso de los demás participantes en la auditoría, a fin de que entre todos elijan criterios más o menos homogéneos de ponderación; esto tiene el propósito de buscar que todos los tópicos que serán evaluados sean aplicables de manera similar.

Este documento se presenta a todo el personal de auditoría, a fin de que cada auditor entienda cuál será su participación en esta evaluación de sistemas.

P.6.2 Elaborar la guía de la auditoría

Después de diseñar la ponderación de la auditoría de sistemas, el siguiente paso es elaborar la guía de la auditoría; éste es un documento de carácter formal, en el cual se anotan todos los puntos que deberán ser evaluados, ya sea del centro de cómputo, del sistema en evaluación, de la gestión informática o de cualquiera de los aspectos del área de sistemas. También se anotan la técnica y la forma en que será evaluado cada punto, así como su ponderación o peso específico.

Ya sea que el auditor tenga experiencia o que carezca de ella, la guía de evaluación será el documento que le permitirá realizar, en forma eficiente y efectiva, su investigación para la auditoría del sistema, centro de cómputo, gestión informática o de cualquiera de los puntos que se tenga que evaluar, ya que le indicará todo el procedimiento que deberá seguir, los puntos que deberá evaluar y las herramientas e instrumentos que deberá utilizar para hacer su revisión. Es decir, este documento le puede guiar paso a paso en todos los aspectos que serán auditados.

Entre los principales aspectos que se deben considerar en la elaboración de la guía de la auditoría encontramos los siguientes:

P.6.2.1 Determinar las áreas y puntos concretos que serán evaluados en el ambiente de sistemas

Es la elección especifica de todas las áreas, puntos concretos y demás aspectos de sistemas que serán evaluados, determinados de acuerdo con el programa de auditoría que se aplicará. Primero se debe elaborar una lista de las áreas y los puntos que serán evaluados, listándolos de manera ordenada. En el capítulo 10 se explica más detalladamente la elaboración de la guía de la auditoría.

P.6.2.2 Seleccionar los métodos, procedimientos, herramientas e instrumentos de evaluación

Una vez identificadas las áreas y puntos que serán evaluados, se deben seleccionar las técnicas, métodos, procedimientos, herramientas y/o instrumentos* que servirán para realizar la evaluación de cada punto específico. Esto con el propósito de que el auditor sepa lo que debe utilizar para evaluar el punto que se le indica, así como la manera de efectuar la evaluación; en algunos casos también se puede incluir un breve detalle de lo que se desea obtener con el uso de tales herramientas.

* Debido a que éste es uno de los aspectos más importantes de la auditoría de sistemas computacionales, en los capítulos 9, 10 y 11 se trata ampliamente cada uno de estos aspectos; por esta razón, aquí sólo se hace una breve mención de lo mismos.

P.6.2.3 Elaborar el documento formal de la guía de auditoría

Una vez hechos los trabajos anteriores, se debe elaborar formalmente un documento llamado guía de auditoría de sistemas; también se recomienda que éste sea sometido a la opinión y consenso de los demás participantes en la auditoría, a fin de que entre todos seleccionen las técnicas, métodos, procedimientos, herramientas y/o instrumentos que sean aplicables a todos los tópicos que serán evaluados.

Este documento sirve para diseñar las partes que el personal de auditoría debe evaluar, a fin de que cada auditor entienda cuál será su participación en esta evaluación.

P.6.3 Elaborar los documentos necesarios para la auditoría

Una vez definidos todos los aspectos señalados en las fases anteriores, y de acuerdo con lo indicado en los documentos terminados de *la ponderación de la auditoría y la guía de auditoría de sistemas*, el siguiente paso es elaborar los documentos formales que servirán para recopilar la información útil para hacer la valoración de los aspectos que serán auditados en el área de sistemas.

Concretamente, y de acuerdo con lo establecido en la guía de auditoría, se deben diseñar, seleccionar o elaborar los documentos formales que se utilizarán para la recopilación de información y para la aplicación y uso de pruebas e instrumentos que servirán para comprobar el buen funcionamiento de los sistemas de la empresa.

El propósito es contar con las herramientas, procedimientos e instrumentos que permitan obtener información útil para la auditoría a los sistemas computacionales de la empresa, lo cual se logra por medio de los siguientes puntos:

P.6.3.1 Diseñar los instrumentos y herramientas de recopilación de información para la auditoría

El responsable de la auditoría en la etapa de planeación debe definir lo más claramente posible los instrumentos de recopilación de información que se requiere en la auditoría, de acuerdo con las características y necesidades de evaluación de sistemas que realizará, razón por la cual debe adoptar, diseñar y aplicar los instrumentos de recopilación que están definidos en los capítulos 9, 10 y 11 de este libro.

Cabe señalar que en la guía de auditoría se deben elegir, preferentemente, los instrumentos, técnicas, procedimientos y herramientas de recopilación que satisfagan las necesidades de evaluación, de acuerdo con las características de los sistemas computacionales que se van a auditar y de acuerdo con la experiencia y conocimientos de los auditores que participarán en la misma.

P.6.3.2 Diseñar los cuestionarios

Como resultado de la planeación de la auditoría o derivado de la guía de auditoría, el encargado de la auditoría será el responsable de elaborar y autorizar los cuestionarios

que se necesitan para el levantamiento de información útil para la evaluación del aspecto de sistemas que se trate; de acuerdo con las necesidades, características y requerimientos específicos que fueron señalados en la guía de auditoría.

Es de suma importancia que el auditor de sistemas computacionales sepa cómo elaborar correctamente estos cuestionarios, ya que se debe seguir un método específico en su formulación, mediante el cual le permitirán: definir el objetivo del cuestionario, elegir el tipo de preguntas (dicotómicas, opción múltiple, abiertas, etcétera) y el número de éstas; también establecer el universo y la muestra de quienes responderán este instrumento y en sí, debe cumplir con características específicas para el mejor diseño de estos instrumentos de recopilación.*

Recordemos que los cuestionarios son las formas de recopilación de información más utilizadas y de mayor utilidad para el auditor, y consisten en recopilar datos, mediante la aplicación de cédulas con preguntas impresas, en donde el encuestado responde de acuerdo con su criterio, a fin de que el auditor concentre, agrupe y tabule las respuestas para obtener, por medio del análisis e interpretación, información significativa para poder evaluar lo que está auditando.

P.6.3.3 Diseñar las guías para realizar entrevistas

Similar al cuestionario, como resultado de la planeación de una auditoría o de la guía de auditoría, el auditor o el responsable de la auditoría deben definir el tipo de entrevista que más le conviene a su evaluación, a fin de establecer las formas como se debe conducir la entrevista y las maneras de obtener la mejor información. Esto obliga al auditor a definir la guía de preguntas que realizará, de acuerdo con su experiencia y conocimientos en la aplicación de esta herramienta de recopilación de información.**

Recordemos que una de las técnicas más utilizadas en la auditoría de sistemas es la entrevista, que se define como: la recopilación de información que se obtiene en forma directa, cara a cara, a través de algún medio de captura de datos, en donde el auditor interroga, cuestiona, investiga y confirma sobre los aspectos que está auditando, siguiendo una serie de preguntas preconcebidas, las cuales va adaptando conforme recibe la información del entrevistado y de acuerdo con las circunstancias que se le presentan para obtener mayor información.

Es indiscutible la utilidad de esta técnica, pero debe saber manejarse adecuadamente, para lo cual el auditor debe contar con amplia experiencia y conocimientos para utilizarla, además de apegarse a la guía de entrevista, en donde se definen todos los puntos que tendrá que seguir para que este instrumento sea útil y valioso para su trabajo de auditor.

* En la sección 9.2 “Cuestionarios”, del capítulo 9, abordaremos con amplitud todo lo relacionado con el cuestionario de auditoría de sistemas computacionales.

** En la sección 9.1 “Entrevistas”, del capítulo 9, se profundizará sobre el uso, características y aplicación de este instrumento de recopilación de datos.

P.6.3.4 Diseñar los formularios para encuestas

También, como resultado de la planeación de auditoría o de la guía de auditoría, el auditor debe definir los tipos de encuestas que utilizará, sus características y los formularios de preguntas que utilizará en su auditoría, a fin de obtener las opiniones de los auditados en relación con los sistemas computacionales, sus servicios, satisfacción de la función informática y muchos otros tópicos de opinión útiles para su evaluación.

La encuesta se define como: La recopilación de datos concretos, dentro de un tópico de opinión específico, mediante el uso de cuestionarios y/o entrevistas, diseñados con preguntas precisas para medir opiniones de los encuestados y con ellas obtener respuestas confiables, las cuales permiten conocer su sentimiento hacia aspectos específicos, después de hacer una rápida tabulación, análisis e interpretación de esa información. Es un valioso instrumento de obtención de información y opinión, por ello debe saber bien utilizar este instrumento.*

P.6.3.5 Diseñar los modelos y formatos para los inventarios del área de sistemas

Como resultado de la planeación de auditoría o de la guía de auditoría, surge la necesidad de levantar información sobre los activos informáticos del área de sistemas, por esa razón el auditor deberá elaborar los formatos en donde se levantarán los inventarios de hardware, software, mobiliario y equipos, personal de sistemas, información y de todos los demás bienes asignados al área, a fin de compararlos contra los registros contables de los mismos y evaluar su uso adecuado.**

Los inventarios se definen como: La recopilación de todos los bienes y materiales que posee un área de sistemas, a fin de comparar las existencias reales y confrontarlas con los registros contables. Es uno de los medios más valiosos para evaluar el uso adecuado de los bienes de la empresa, por eso es de suma importancia definir, previamente, el tipo de inventarios a realizar y los modelos o formatos que nos servirán para su aplicación adecuada.

P.6.3.6 Diseñar los métodos e instrumentos de muestreo

En su recopilación de información, el auditor no puede ni debe recopilar toda la información disponible en el área de sistemas, ya que a la vez que sería inoperante, resultaría fatigoso y muy dilatado el proceso de recopilación de datos, por ello deberá saber aplicar las herramientas estadísticas y matemáticas que le permitan obtener informa-

* En la sección 9.3 "Encuestas", del capítulo 9, se profundizará sobre la utilidad, uso y formas de aplicación de este instrumento.

** En la sección 9.5, "Inventarios", del capítulo 9, realizaremos un profundo análisis de las características, requerimientos y aplicaciones de este instrumento.

ción que sea útil para su evaluación, mediante la elección correcta de los métodos e instrumentos de muestreo que le permitan tratar mejor a este tipo de recopilación.*

Esta definición del tipo de muestreo y herramientas estadísticas debe ser el resultado de la planeación de la auditoría que se define en la guía de auditoría.

P.6.3.7 Diseñar los instrumentos especiales de evaluación de sistemas

De igual manera que en el punto anterior, el responsable de la auditoría debe adoptar, diseñar y aplicar los instrumentos de especiales de evaluación, que le permitan definir, lo más claramente posible, todos aquellos métodos, técnicas, herramientas e instrumentos de evaluación que sean aplicables en la auditoría de sistemas computacionales. Esto se define en la etapa de planeación de auditoría, de acuerdo con las necesidades de evaluación de los sistemas computacionales de que se trate. En los capítulos 9, 10 y 11 de este libro se profundiza sobre los instrumentos de evaluación que puede utilizar el auditor.

P.6.3.8 Determinar los puntos que serán evaluados con pruebas

Como producto de la planeación de auditoría, puede surgir la necesidad de determinar algunos puntos que permitan evaluar el funcionamiento adecuado del hardware, equipos periféricos y sus componentes, o del software institucional, sistemas operativos, los programas, aplicaciones, paquetes, utilerías, o también del procesamiento de información, las bases de datos o cualquier otro tipo de evaluación a los sistemas computacionales de la empresa; por esta razón, en la etapa de planeación de la auditoría se deben establecer concretamente los puntos que se requieren evaluar mediante el uso de pruebas a los sistemas; esto de acuerdo con las características específicas de los sistemas que se quieren evaluar en la empresa.

P.6.3.9 Diseñar las pruebas para la evaluación

Como resultado del punto anterior, y parte importante de la planeación de auditoría, en esta etapa se determinan, lo más claramente posible, el tipo de pruebas, su alcance e intensidad, sus características y especificaciones, de acuerdo con las necesidades de la auditoría y las características de los sistemas. Claro está, respetando los puntos diseñados en la sección anterior y las especificaciones de procesamiento de los sistemas computacionales que se evaluarán.**

Es de suma importancia recalcar que el diseño y aplicación de las pruebas o exámenes de auditoría se harán en relación con los puntos definidos en la sección anterior.

* En la sección 9.6, "Muestreo", del capítulo 9, se hace el análisis del muestro aplicable a la auditoría de sistemas computacionales.

** En la sección 10.1, "Exámenes", del capítulo 10, se profundiza lo relacionado con exámenes al área de sistemas

P.6.3.10 Diseñar los instrumentos y herramientas para pruebas de evaluación

Cuando ya están perfectamente definidos los puntos a evaluar y las pruebas que se realizarán (secciones P.6.3.8 y P.6.3.9), el auditor ya puede elegir o diseñar los instrumentos, herramientas, métodos y procedimientos que le permitirán realizar dichas pruebas; esto obedece a que los sistemas computacionales tienen características muy específicas y, antes de realizar cualquier prueba, se deben analizar a profundidad con el fin de no afectar el funcionamiento normal de los sistemas. No es lo mismo realizar un procesamiento de datos de prueba a un sistema en funcionamiento (aunque sea con datos falsos), que un procesamiento de datos a un sistema paralelo (aun con datos verdaderos).

Recordemos que el auditor evalúa el funcionamiento de los sistemas a través de pruebas, pero estas pruebas no pueden ni deben interferir en el actual funcionamiento de los sistemas. De ahí la importancia de saber elegir, perfectamente, el tipo de instrumentos con los cuales se realizarán las pruebas.

En los capítulos 9, 10 y 11, el auditor encontrará instrumentos valiosos que le ayudarán a elegir estas herramientas de evaluación de prueba de los sistemas.

P.6.4 Determinar herramientas, métodos y procedimientos para la auditoría de sistemas

Una vez que ya fueron definidos los puntos señalados en las fases anteriores y que ya se cuenta con los documentos necesarios para aplicarse a las necesidades de auditoría establecidos en la ponderación de auditoría de sistemas y la guía de auditoría de sistemas, el siguiente paso es determinar las herramientas, métodos y procedimientos que se utilizarán para llevar a cabo la evaluación en el ambiente de sistemas que se auditará.

En la sección P.6.3 señalamos que es necesario definir los documentos a utilizar, mientras que en esta etapa tenemos que seleccionar los instrumentos a utilizar en la auditoría, ya sea que se elijan los instrumentos que ya se han probado con anterioridad, de los que se necesitan rediseñar para esta evaluación o de aquellos que tienen que diseñarse para aplicar a las necesidades de esta auditoría. Todo en función de las características de los sistemas que se están auditando.

En los capítulos 9, 10 y 11 de este libro se profundizará sobre la utilidad, diseño y uso de estas herramientas de evaluación para la auditoría de sistemas computacionales.

P.6.4.1 Diseñar las herramientas e instrumentos que serán utilizados en la evaluación

Se refiere a la definición específica de los instrumentos y herramientas informáticos que el auditor utilizará para evaluar los sistemas computacionales de la empresa. En especial, los elementos de sistemas computacionales que utilizará para evaluar a los propios sistemas y para aquellas aplicaciones específicas del sistema computacional.

Estos puntos serán tratados con amplitud en los capítulos 9, 10 y 11 del libro.

P.6.4.2 Establecer los métodos y procedimientos que serán utilizados en la auditoría

Se refiere a la definición específica de los métodos de trabajo y procedimientos de auditoría que el auditor aplica para llevar a cabo su auditoría a los sistemas computacionales de la empresa. Dichos métodos y procedimientos son las guías de trabajo, rutinas, experiencias y conocimientos específicos de auditoría que sigue el auditor para realizar su trabajo. Éstos pueden estar apoyados en los anteriores instrumentos.

Estos puntos también serán tratados con amplitud en los capítulos 9, 10 y 11 del libro.

P.6.4.3 Determinar las técnicas y procesos específicos que serán utilizados en la auditoría

Las técnicas se refieren a las habilidades, prácticas, destrezas y pericias que tiene el auditor para realizar su evaluación, mientras que los procesos son las etapas, actividades y tareas que sigue el auditor para llevar a cabo su evaluación. Ambos, técnicas y procesos, determinan las acciones a seguir en la evaluación de los sistemas de la empresa.

También en los capítulos 9, 10 y 11 del libro, se analizan estos conceptos.

P.6.4.4 Elaborar los documentos formales para los procedimientos, métodos, herramientas e instrumentos que serán utilizados en la auditoría

Cuando el auditor o responsable de la auditoría ya tienen perfectamente definidos todos y cada uno de los puntos que utilizará en su auditoría, como resultado de la planeación de la auditoría, debe plasmar en un documento formal cada uno de los instrumentos, técnicas, procedimientos y herramientas que utilizará. Detallando lo más posible las características y formas de uso de cada instrumento, así como el objetivo que se pretende satisfacer con las mismas.

Estos instrumentos, técnicas, procedimientos y herramientas vienen a conformar la guía de auditoría.*

P.6.5 Diseñar los sistemas, programas y métodos de pruebas para la auditoría

En una auditoría de los sistemas computacionales, entre otras muchas cosas, en auditor debe evaluar, forzosamente, el adecuado funcionamiento de los sistemas computa-

* En la sección 11.1, "Guías de evaluación", del capítulo 11; se profundiza sobre el uso y utilidad de este instrumento.

cionales de la empresa, lo cual se realiza a través del diseño de programas específicos que aplica en esos sistemas, así como de métodos de pruebas especiales, exclusivos de estos sistemas computacionales. Éstos, en su conjunto, constituyen la evaluación técnica al funcionamiento de los sistemas de la empresa.*

Precisamente como resultado de la planeación de auditoría y de manera específica en la guía de auditoría, el responsable de la auditoría debe plasmar, formalmente, los sistemas, programas y métodos que aplicará, en forma de pruebas, para evaluar los sistemas computacionales de la empresa.

P.6.5.1 Determinar los puntos de interés, programas, bases de datos, archivos y sistemas que serán evaluados mediante programas y pruebas de cómputo

En esta fase el responsable de auditoría determina, lo más ampliamente posible, todos los puntos que serán evaluados durante la auditoría, detallando los aspectos de sistemas que le conviene auditar. De preferencia, especificando el objetivo y las características y las formas de la evaluación que se utilizarán para tales puntos.

P.6.5.2 Diseñar las pruebas, programas y sistemas para realizar las evaluaciones necesarias para el funcionamiento de los sistemas computacionales, bases de datos y archivos

Contando con los puntos del inciso anterior, ahora diseña las pruebas, programas y sistemas que utilizará para las evaluaciones que determinen el funcionamiento adecuado de los sistemas computacionales de la empresa, sus bases de datos, archivos de información y de todos los aspectos relacionados con el procesamiento de información en el área de sistemas. Incluyendo el hardware, software, instalaciones, periféricos y demás componentes del mismo.

Estos puntos deben corresponder con los señalados en la guía de auditoría.

P.6.5.3 Aplicar y obtener los resultados de las pruebas, programas y sistemas para realizar las evaluaciones necesarias

Una vez que ya se han diseñado los procedimientos, técnicas y herramientas determinados en el punto anterior, el auditor los aplica conforme fueron establecidos, para así obtener los resultados de su funcionamiento y con ellos lleva a cabo el análisis de su comportamiento en la función informática de la empresa. Esto le permitirá hacer las evaluaciones a estos resultados.

* En el capítulo 12 se presentan evaluaciones específicas a los sistemas computacionales. Mientras que en los capítulos 9, 10 y 11 se presentan las principales técnicas, herramientas, instrumentos y procedimientos para este tipo de evaluaciones.

P.6.5.4 Diseñar, aplicar y evaluar los resultados de los programas, métodos y pruebas de simulación al sistema

En algunos casos, además de aplicar los métodos y pruebas previamente diseñados, será necesario realizar simulaciones de los resultados, a fin de evaluar el comportamiento de estos resultados a la luz de otras pruebas simuladas en equipos similares o en el mismo equipo, pero con otro tipo de datos. Esto ayuda a complementar la evaluación de los resultados que se obtienen del sistema en auditoría.

P.6.5.5 Diseñar otros instrumentos de recopilación

Producto de las pruebas, programas y métodos de evaluación antes señalados, puede ser necesario diseñar otros instrumentos que ayuden a evaluar mejor los resultados alcanzados, razón por la cual se puede recurrir a nuevos instrumentos que se elaboran para complementar la evaluación de los sistemas. Todo en función de las necesidades de evaluación y las características específicas de los sistemas.

P.6.5.6 Elaborar otros documentos de revisión

En algunas ocasiones se deben elaborar otros instrumentos que contribuyen a evaluar, de mejor manera, los sistemas computacionales de la empresa, para lo cual se debe considerar las necesidades concretas de evaluación y los requerimientos de pruebas, programas y métodos de evaluación que serán necesarios.

6.3.7 P.7 Asignar los recursos y sistemas computacionales para la auditoría

Una vez definidos todos los aspectos señalados en las fases anteriores, el siguiente paso es asignar los recursos que serán utilizados para realizar la auditoría, de acuerdo con los aspectos ya establecidos con anterioridad. Con la asignación de estos recursos especializados, sean humanos, informáticos, tecnológicos o cualesquiera otros que se hayan establecido para la auditoría, es como se lleva a cabo la misma.

En la sección P.4.7 hice un análisis más específico de estos recursos, sin embargo, a continuación señalo los principales puntos que el responsable debe establecer para la realización de la auditoría:

P.7.1 Asignar los recursos humanos para la realización de la auditoría

Los responsables de realizar la auditoría son los recursos humanos especializados en informática y auditoría, ya que con ellos se llevan a cabo todas las actividades programadas para la revisión de los sistemas, la elaboración de pruebas, operación de los sistemas, la evaluación al funcionamiento de los sistemas, sus bases de datos, el uso correcto y adecuado de la información, y en sí de todos los aspectos informáticos que serán evaluados.

Estos recursos humanos, por lo especializado de la actividad que realizan para la auditoría, pueden ser auditores en el área informática, cuyos conocimientos les permiten evaluar casi todos los aspectos de sistemas.

Sin embargo, la actividad de los sistemas computacionales de una empresa suele ser sumamente especializada, ya sea por el tipo de sistemas, la plataforma que se utilice, el software específico que se emplee o cualesquiera otras especificaciones que sólo el personal del área domine; por esa razón, el auditor también puede recurrir al personal del área, de carácter interno, que le ayude a evaluar el funcionamiento de los sistemas que se auditan, lo cual es muy frecuente y muy válido. Recordemos que un auditor no necesariamente debe conocer todos los sistemas computacionales, pero sí debe utilizar la técnicas de auditoría y apoyarse en los expertos informáticos para realizar su operación.

Los recursos a los que puede acudir para su evaluación suelen ser aquellos especialistas que pertenecen al área de sistemas computacionales auditada, quienes cooperarán con el auditor para realizar las pruebas, programas y procedimientos de evaluación que determine el auditor.

Estos especialistas también pueden ser de carácter externo, conformado con personal ajeno a la empresa y/o área auditadas.

P.7.2 Asignar los recursos informáticos y tecnológicos para la realización de la auditoría

Así como se asignaron los recursos humanos para la auditoría, también se tienen que asignar los recursos informáticos y tecnológicos que requiere el auditor para realizar su auditoría, los cuales vienen a ser sus herramientas de trabajo.

Estos recursos informáticos pueden ser los sistemas computacionales que utilizará durante su evaluación, que incluyen los propios sistemas, sus componentes y periféricos, además de los programas, paquetes y utilerías especializadas de evaluación, las bases de datos e información (real o simulada) del sistema y en sí todo el hardware, software, bases de datos y demás componentes de sistemas que utilizará durante su auditoría. Todo de acuerdo con la determinación de los recursos establecida en las etapas anteriores.

Igual con los recursos tecnológicos especializados que se lleguen a necesitar para la evaluación de los sistemas; según las especificaciones técnicas de la evaluación que realice.

P.7.3 Asignar los recursos materiales y de consumo para la realización de la auditoría

Al igual que los anteriores, también se tienen que asignar los materiales y consumibles que serán utilizados durante la auditoría, a fin de que el auditor cuente con todos los elementos necesarios para su evaluación, que pueden ser desde disquetes, cintas, papelería, equipos de oficina, como de cualesquiera otros elementos no especializados que utilice durante su evaluación.

El objetivo de asignar estos recursos es que el auditor realice su evaluación sin contratiempos al contar con el material necesario para el buen desempeño del trabajo encomendado.

P.7.4 Asignar los demás recursos para la realización de la auditoría

Aquí se incluyen todos los demás recursos ajenos a los anteriores que serán utilizados por el auditor, de los cuales destacamos los apoyos materiales y financieros, los viáticos, pasajes y otros gastos, por citar sólo algunos.

Sin embargo, la asignación de estos otros recursos estará determinada por lo establecido en la sección P.4.7.

6.4 2ª etapa: Ejecución de la auditoría de sistemas computacionales

El siguiente paso después de la planeación de la auditoría es su ejecución, la cual estará determinada por las características concretas, los puntos y requerimientos que se estimaron en la etapa de planeación.

Debido a que esta etapa es de realización especial, de acuerdo con la planeación de la auditoría, en este inciso sólo se indican sus puntos más importantes, en la inteligencia de que se aplicará verdaderamente de acuerdo a las características específicas de la auditoría que se trate. Los principales puntos son los siguientes:

Concretamente, tenemos los siguientes conceptos:

- *Realizar las acciones programadas para la auditoría*
- *Aplicar los instrumentos y herramientas para la auditoría*
- *Identificar y elaborar los documentos de desviaciones*
- *Elaborar el dictamen preliminar y presentarlo a discusión*
- *Integrar el legajo de papeles de trabajo de la auditoría*

Como éstas ya son las actividades concretas, resultado de la práctica de la auditoría de sistemas, a continuación haremos un breve análisis de los puntos señalados en esta parte:

E.1 Realizar las acciones programadas para la auditoría

De acuerdo con el programa de auditoría, cada auditor tiene que realizar las actividades que le corresponden conforme fueron diseñadas, en la cronología que le fue asignada a cada una, y de acuerdo con los tiempos y recursos que le corresponde utilizar; el propósito es ejecutar los eventos programados y alcanzar el objetivo de la auditoría.

E.2 Aplicar los instrumentos y herramientas para la auditoría

Aquí lo importante es que, conforme a la guía de auditoría, se tienen que utilizar, uno a uno, los instrumentos y herramientas elegidos para llevar a cabo la evaluación, ya sea mediante la recopilación y análisis de la información, la observación, las pruebas y simulaciones de los sistemas, o mediante cualquier otro instrumento de los que se diseñaron previamente para esta revisión.

E.3 Identificar y elaborar los documentos de desviaciones encontradas

Una vez que se realizaron las actividades diseñadas en el programa de trabajo de auditoría, que se utilizaron los instrumentos de recopilación de información y/o se utilizaron los instrumentos determinados para la auditoría, entonces se buscan las posibles desviaciones y se procede a elaborar los documentos de desviaciones, en los cuales se anotan las situaciones encontradas, las causas que las originaron y sus posibles soluciones, así como los responsables de solucionar dichas desviaciones y las posibles fechas para hacerlo. En el capítulo 8, inciso 8.4, analizaremos más a fondo este tópico.

El auditor puede elaborar este documento cuando lo considere necesario; es decir, lo puede elaborar conforme va realizando cada evaluación, conforme va evaluando áreas completas, conforme va realizando cada evento programado o conforme a cualquier otro criterio. Lo importante es que conforme el auditor detecte las desviaciones, elabore de inmediato el documento de desviaciones.

E.4 Elaborar el dictamen preliminar y presentarlo a discusión

Una vez que el auditor determinó las desviaciones encontradas durante la evaluación, debe elaborar un documento que contenga todas las desviaciones detectadas, o lo puede elaborar con cada una de las desviaciones por separado, de acuerdo a las necesidades de la empresa. Una vez hecho esto, es obligación del auditor comentarlas con las personas que están involucradas directamente en las desviaciones, a fin de encontrar de manera conjunta las causas que las originaron y, derivado de este intercambio de opiniones, debe determinar las posibles soluciones para cada una de estas causas. También puede asignar a los responsables de solucionarlas y, de ser posible, las fechas para hacerlo.

Es muy conveniente señalar que la importancia de la auditoría no sólo estriba en reportar las desviaciones encontradas en una operación normal, sino que las personas que están involucradas directamente en la operación deben conocerlas; el propósito es que estén conscientes de las desviaciones encontradas en su trabajo para que puedan emprender las acciones necesarias para corregirlas, si es que las correcciones están en sus manos. En el capítulo 8 analizaremos más profundamente este tema.

La auditoría no se lleva a cabo para cortar las cabezas de los auditados; es una disciplina que ayuda a detectar las desviaciones en las operaciones de los auditados, así como a conocer las causas de tales desviaciones y sus posibles soluciones.

E.5 Integrar el legajo de papeles de trabajo de la auditoría

El auditor tiene la obligación de conservar en el llamado legajo de papeles de la auditoría cada uno de los instrumentos aplicados en la evaluación, con el propósito de sustentar, llegado el caso, las observaciones reportadas. En el siguiente capítulo se hace un profundo análisis de este documento y su importancia.

6.5 3ª etapa: Dictamen de la auditoría de sistemas computacionales

El último paso de la metodología que hemos estudiado es emitir el dictamen, el cual es el resultado final de la auditoría de sistemas computacionales. Para ello presentamos los siguientes puntos:

- *la información y elaborar un informe de situaciones detectadas*
- *Elaborar el dictamen final*
- *Presentar el informe de auditoría*

6.5.1 D.1 Analizar la información y elaborar un informe de situaciones detectadas

La actividad previa, o más bien paralela, a la detección de las desviaciones, es el análisis de los papeles de trabajo y la elaboración en borrador de las llamadas situaciones detectadas; el propósito es que el auditor elabore su borrador y comente las desviaciones con los auditados. Después de comentarlas, debe elaborar las modificaciones pertinentes, así como el informe definitivo de las situaciones encontradas.

Es necesario advertir que el fin de una auditoría de sistemas computacionales no es encontrar culpables, sino ayudar a corregir las desviaciones encontradas en la operación normal de dichos sistemas; esto se logra comentando las desviaciones con los responsables directos, con el fin de que las conozcan y tomen las acciones necesarias para su corrección.

Concretamente, este punto contendrá las siguientes actividades:

D.1.1 Analizar los papeles de trabajo

El auditor debe hacer un estudio de los papeles de trabajo* resultantes de la auditoría, con el propósito de detectar las posibles desviaciones en la operación normal del área o sistema computacional que está auditando. Después debe plasmar las desviaciones que encontró en el formato** de situaciones, causas y soluciones, mismo que debe elaborar primero en borrador para comentar estos aspectos con los involucrados, y después debe alaborarlo en forma definitiva.

D.1.2 Señalar las situaciones encontradas

El auditor debe plasmar en forma específica y lo más concretamente posible las desviaciones encontradas en la operación del sistema o en el área que está evaluando y, si es posible, debe señalar las causas que las generaron.

El auditor, ya sea el responsable de la auditoría o el encargado de aplicarla, será quien, basándose en los papeles de trabajo, su experiencia en el ramo y las situaciones encontradas, elaborará el borrador de las desviaciones que encontró durante la evaluación de los sistemas, procurando detallar, hasta donde le sea posible, en que consisten, su repercusión y los demás aspectos que crea pertinentes, a fin de señalar concretamente lo observado.

En el capítulo correspondiente al informe de auditoría analizaremos más a fondo el formato de situaciones encontradas.

* En el capítulo 7 se explica la manera de presentar los papeles de trabajo y su contenido.

** En el capítulo 8 se presenta todo lo relacionado con el dictamen de auditoría

D.1.3 Comentar las situaciones encontradas con el personal de las áreas afectadas

Una vez que ha detectado las desviaciones, es obligación ineludible del auditor comentarlas en forma directa y abierta con los responsables de la operación, a fin de que las conozcan, acepten, aclaren, complementen y/o las modifiquen con detalles y pruebas. El auditor no debe, en ningún caso y bajo ningún concepto, presentar las desviaciones encontradas sin antes haberlas comentado con el auditado. Sin embargo, si el auditor no tiene la suficiente experiencia, los comentarios con los auditados se pueden desviar e incluso provocar fricciones que es necesario evitar.

Es un requisito que el auditor comente las desviaciones encontradas, debido a que además de servirle para refirmar sus observaciones, le ayudará a comprobarlas, complementarlas y en su caso ampliarlas; esto también le ayudará a establecer las causas que ocasionaron las desviaciones, así como sus posibles soluciones.

En algunos casos, el auditor puede obtener la firma del auditado para comprobar que se han comentado y aceptado las desviaciones, aunque a veces esto no es posible.

D.1.4 Realizar las modificaciones necesarias

Después de que el auditor haya comentado ampliamente las desviaciones con los involucrados, deberá ratificar las observaciones y, de ser necesario, elaborar las correcciones que sean pertinentes, modificando el borrador, las causas o las posibles soluciones. También podría elaborar nuevamente el borrador del informe, e incluso lo podría comentar nuevamente si fuera necesario.

Es menester que el auditor comente con el auditado, en forma abierta y clara, las desviaciones encontradas, a fin de que éste lo retroalimente, modifique tales desviaciones y, si es el caso, le ayude a complementarlas o a determinar sus posibles correcciones.

D.1.5 Elaborar un documento de situaciones relevantes

Una vez que el auditor ha comentado y corregido el borrador inicial, conforme a lo señalado en los puntos anteriores, debe proceder a elaborar un documento que contenga las situaciones relevantes que encontró durante la auditoría y, según el plan de trabajo y la costumbre laborar, puede continuar con la elaboración del dictamen de auditoría.

El auditor puede elaborar los documentos y comentarlos con los responsables de las áreas auditadas conforme va concluyendo las evaluaciones y, si es necesario, conforme va detectando las desviaciones; todo de acuerdo con su forma de trabajar y con la forma de supervisión establecida en la planeación inicial de la auditoría.

6.5.2 **D.2** Elaborar el dictamen final

El auditor debe terminar de elaborar el informe de auditoría de sistemas y complementarlo con el dictamen final (opinión del auditor), y después presentarlo a los directivos del área de sistemas auditada para que conozcan la situación actual de dicha área, antes de presentarlo al responsable de la empresa.

D.2.1 Analizar la información y elaborar un documento de desviaciones detectadas

Por lo general, el auditor responsable de la auditoría es quien analiza las desviaciones que comentó con los auditados, para después elaborar el informe final de las desviaciones encontradas, lo cual es una garantía de que los auditados ya aceptaron dichas desviaciones, mismas que plasmará en el documento llamado *Desviaciones encontradas*. En el siguiente capítulo trataremos ampliamente éste y otros formatos.

D.2.2 Elaborar el informe y el dictamen formales

Después de analizar los informes anteriores (el borrador inicial comentado), el auditor debe elaborar, de manera formal, el informe de las desviaciones encontradas, especificándolas por área, por servicio o por cualquier otro formato de presentación, de manera clara y precisa. También deberá presentar las desviaciones conforme a la costumbre de la empresa; ya sea por importancia, por orden cronológico, por secuencia de operaciones o por cualquier otro criterio, siempre y cuando éste sea igual en toda la elaboración del informe.

Cuando el auditor elabora su dictamen debe tomar en cuenta todas las desviaciones, analizarlas y emitir su opinión acerca de la situación de las áreas y sistemas auditados, especificando, lo más clara y sinceramente posible, su opinión respecto a dichas desviaciones y, de ser posible, debe presentar una sugerencia profesional para corregirlas. En el siguiente capítulo analizaremos más profundamente lo relacionado al informe y al dictamen de la auditoría de sistemas computacionales.

D.2.3 Comentar el informe y el dictamen con los directivos del área

Así como el borrador del informe de auditoría se debe comentar con los auditados, este informe final se debe comentar con los directivos del área de sistemas; ya sea con el jefe inmediato, con el gerente o con el directivo principal de esta área, según las políticas de la empresa auditora.

Debemos aclarar que el informe de auditoría se debe comentar exclusivamente con los directivos del área; pero se debe tener especial cuidado para poder comentar y aclarar lo necesario en este tipo de reuniones.

D.2.4 Realizar las modificaciones necesarias

Después de comentar el informe y el dictamen con los directivos del área de sistemas, el auditor podrá ratificar o rectificar las observaciones presentadas en estos documentos. Después de hacer las modificaciones necesarias, podrá elaborar el informe y dictamen finales de la auditoría.

Si en opinión del auditor no procede ninguna modificación, o si sus observaciones fueron sustancialmente modificadas, puede volver a comentar el informe y el dictamen, si lo considera necesario.

6.5.3 D.3 Presentar el informe de auditoría

El último paso de esta metodología que hemos estudiado, es presentarle formalmente el dictamen de la auditoría al más alto directivo de la empresa, con el propósito de informarle los resultados de dicha auditoría. Esta presentación se debe hacer con toda la formalidad del caso, con la elaboración correcta y profesional del dictamen de la auditoría, y en medio de una reunión directiva. El informe de auditoría debe contener los siguientes puntos:

- *La carta de presentación*
- *El dictamen de la auditoría*
- *El informe de situaciones relevantes*
- *Anexos y cuadros adicionales*

D.3.1 Elaboración del dictamen formal

En esta fase son fundamentales la experiencia, los conocimientos y la capacidad del auditor para elaborar, lo más profesionalmente posible, el dictamen de la auditoría y el informe de las desviaciones encontradas durante la revisión; el auditor debe hacer el dictamen tomando en cuenta el informe comentado con los directivos, el formato de desviaciones y los papeles del trabajo de los demás auditores.

D.3.2 Integración del informe de auditoría

Es de suma importancia destacar que el dictamen y el informe final de la auditoría deben ser elaborados perfectamente y no deben tener error alguno. También deben contener, de la manera más clara y concreta, las desviaciones detectadas en la evaluación.

D.3.3 Presentación del informe de auditoría

Es la reunión plenaria con el nivel directivo más alto, para entregarle en mano el dictamen de la auditoría realizada; en este caso ya no existen comentarios ni aclaraciones

sobre el informe, sólo es la lectura o entrega física del dictamen y el informe final de la auditoría. Esta presentación es de carácter formal y protocolario.

D.3.4 Integración de los papeles de trabajo

El paso siguiente después de presentar el informe de auditoría (dictamen e informe final), es que la empresa auditora debe integrar perfectamente los papeles de trabajo, ya que servirán en caso de aclaraciones posteriores y para dar seguimiento a las soluciones de las desviaciones encontradas. Esto será ampliado en el capítulo correspondiente a los papeles de trabajo.

7

Papeles de trabajo para la auditoría de sistemas computacionales

Estructura del capítulo

Objetivos del capítulo:

Identificar el apoyo documental que requiere el auditor al realizar cualquier auditoría de sistemas computacionales, a fin de contar con el soporte que le permita avalar y testimoniar la aplicación de técnicas, métodos y procedimientos de auditoría. Con dicha documentación podrá respaldar su trabajo y con su uso cubrirá las necesidades específicas de soporte documental para la auditoría de sistemas.

Introducción del capítulo

Ya señalamos que una de las características fundamentales de la auditoría de sistemas computacionales, y en general de cualquier tipo de auditoría, es el registro eficiente de la información que el auditor va recolectando durante su evaluación; esa información le sirve para sostener las opiniones que emite en el informe de la auditoría.

Para ello tiene que recopilar los datos obtenidos durante la auditoría y registrarlos formalmente en documentos; estos documentos pueden ser manuscritos, manuales, instructivos, gráficas, resultados de procesamientos, concentrados de bases de datos en disquetes, respaldos (*backups*) o cualquier otro medio escrito o electromagnético, en los cuales recopilará los hechos, pruebas, tabulaciones, interpretaciones, así como el análisis de los datos obtenidos. Con todo lo anterior, el auditor tendrá un apoyo para confirmar los hechos y validar la información que utilizará como base para elaborar el informe de auditoría.

No obstante, al realizar este registro formal de datos, de inmediato surgen los siguientes interrogantes:

- *¿En dónde, cómo y para qué concentrar los datos que se obtienen en la auditoría* de sistemas?
- *¿Los datos recopilados sirven para fundamentar las observaciones y para emitir un dictamen?*
- *¿En dónde, cuándo y para qué se registra la información que se obtiene en la auditoría de sistemas computacionales?*
- *¿Qué medios se utilizan para concentrar, validar, tabular e interpretar los datos obtenidos?*
- *¿Quién es el responsable de registrar, concentrar y controlar la información recopilada durante la auditoría? ¿En dónde, cuándo y cómo?*
- *¿En dónde, cuándo, por qué y cómo se registra la información documental, la emitida por el sistema computacional y la recopilada directamente en el campo?*
- *¿Qué tan válido es guardar la información recopilada del sistema computacional en medios electromagnéticos?*

Es evidente que para satisfacer éstos y muchos otros interrogantes, el auditor necesita cierto tipo de apoyo que le ayude a registrar formalmente (por escrito) la información que obtuvo al realizar la evaluación; asimismo, este apoyo proporciona un adecuado orden al desarrollo de su trabajo; además le sirve como soporte documental para registrar y, en su caso, mostrar las evidencias y pruebas de las situaciones relevantes encontradas durante la evaluación y reportadas en el informe.

El soporte fundamental, aparentemente muy simple, para la auditoría, es el registro de la información recopilada en los llamados *papeles de trabajo* (para el caso de auditoría de sistemas computacionales pueden ser documentos, gráficas y medios electromagnéticos), en los cuales se van anotando los hechos, acontecimientos y fenómenos observados durante la revisión; asimismo, estos *papeles de trabajo* se utilizan para transcribir y concentrar los resultados de entrevistas, cuestionarios, pruebas, encuesta, investigaciones, observaciones y opiniones del personal auditado.

También se utilizan como memoria detallada para asentar la evaluación de los documentos formales del área, de los resultados de las pruebas que se aplican en el sistema, de la documentación testimonial de los auditados y/o de cualquier otra evidencia documental o sistematizada que se utilice para concentrar la información relacionada con la administración y seguridad del área de sistemas, la operación del sistema, el comportamiento de las bases de datos o cualquier otro aspecto que afecte la operación normal del área o de los sistemas auditados.

El uso de los papeles de trabajo es universal y no es privativo de la profesión de auditoría, ya que estos documentos se utilizan en las empresas para registrar operaciones, atestiguar acciones, formalizar acuerdos, fundamentar propiedad y para registrar muchas otras operaciones desarrolladas en las instituciones. Sin embargo, en el caso específico de la auditoría, no sólo se utilizan para evaluar el registro adecuado de las operaciones, también se utilizan para asentar, tabular y concentrar opiniones, registrar respuestas y elaborar tabulaciones y gráficas que sirven de apoyo para la interpretación de esa información; también le sirven de apoyo al auditor al emitir una opinión y, en su caso, para contar (por escrito) con las evidencias necesarias para sostener sus comentarios.

Es necesario reiterar que uno de los elementos básicos de la auditoría de sistemas es la elaboración de papeles de trabajo (o su equivalente en los medios electromagnéticos de información); también debemos reiterar que es fundamental que el auditor elabore estos documentos o registros electromagnéticos para asentar todo lo que encuentre durante su revisión.

En la práctica, para una buena auditoría, cualquiera que sea el tipo y ambiente donde se realice, el uso del apoyo documental cobra una relevancia tal que muchos funcionarios de las empresas auditadas y los propios auditores consideran que *los papeles de trabajo* son el aspecto primordial sobre el cual descansa una evaluación; además, como ya hemos citado, sirven como soporte de las opiniones del auditor.

En la actualidad, muchas empresas y áreas de auditoría, incluso los propios auditores y no pocas entidades federativas de México, exigen, para hacer válida la opinión emitida como resultado de una auditoría de carácter contable, fiscal o financiera, que

tanto la evaluación como el dictamen estén sustentados en la existencia de papeles de trabajo, en los cuales estén anotados los hechos encontrados durante la auditoría. Esto se acentúa, aún más, en caso de que se requiera una auditoría, ya sea a voluntad de la empresa o por imposición de alguna autoridad, ya que el dictamen del auditor se fundamenta y se acepta con base en los documentos de trabajos fiscales y contables.

En una auditoría de sistemas computacionales, *los papeles de trabajo* representan el sustento para registrar los datos e información que se van recolectando durante la evaluación; sin embargo, por la especialidad de medios que se utilizan para el registro de la información de las áreas de cómputo, la recopilación de datos se puede realizar en documentos o en medios electromagnéticos de captura y resguardo de datos. Estos últimos pueden ser discos duros, discos flexibles, cintas, cartuchos, CD-ROM, DVD y otros medios electromagnéticos de registro exclusivo en sistemas computacionales. En estos *papeles de trabajo* (documentos o medios electromagnéticos), el auditor también señala y destaca las observaciones que son de interés para él, a fin de cimentar el resultado de su evaluación; también le sirven para mantener el sentido e importancia de las desviaciones que encontró durante la revisión, así como para establecer las posibles causas de las desviaciones y para proponer las probables soluciones que reporta como parte de su trabajo.

Existen múltiples formas de elaborar y utilizar los papeles de trabajo de una auditoría de sistemas computacionales, las cuales estarán determinadas por la experiencia, conocimientos y habilidades del auditor, así como por su necesidad de usar los documentos y medios de cómputo para concentrar la información; hay notorias similitudes (y diferencias) en la confección y uso de los papeles de trabajo, las cuales van desde uniformar el diseño de los documentos, métodos y sistemas de captura de datos, la forma concreta de recopilar, concentrar y archivar la información, la manera de hacer acotaciones con los mismos estilos, opiniones y uso de claves similares, hasta la aplicación de una serie de aspectos específicos y particulares para cada una de las áreas de sistemas auditadas.

Para que *los papeles de trabajo o medios de captura* se puedan admitir como soporte documental de una auditoría de sistemas, y para que se utilicen para fundamentar los resultados y opiniones que presenta el auditor, es necesario que, tanto en su diseño como en su uso, reúnan ciertos requisitos y formalidades, mismos que serán determinados previamente por la empresa encargada de realizar la auditoría, o por el auditor responsable de llevarla a cabo.

7.1 Contenido del legajo de papeles de trabajo

Los aspectos que analizaremos a continuación son de carácter general; asimismo, al presentarlos pretendemos dar una idea precisa de la cantidad mínima de documentos

con la que se podrán integrar los papeles de trabajo del auditor de sistemas; también proyectamos señalar un criterio de orden y conservación para el llamado *legajo de papeles de trabajo de la auditoría de sistemas*. Aunque, claro está, lo aquí señalado es sólo una sugerencia hecha con el único propósito de ayudar a unificar las formas de utilizar y guardar estos documentos; sin embargo, nada impide que el auditor utilice su experiencia, conocimientos y criterio personal para determinar el contenido y orden que deben tener los papeles de trabajo que utilizará en su evaluación. *Lo importante es que dichos papeles existan.*

El legajo de papeles de trabajo, por su naturaleza y contenido, es el aspecto fundamental para elaborar el dictamen de la auditoría, y su uso es confidencial y exclusivo del auditor de sistemas, debido a que éste va integrando en estos papeles de trabajo los documentos reservados y de uso exclusivo de la empresa, mismos que recopila durante su revisión y los complementa con los registros, en papel o en medios electromagnéticos, que obtiene como evidencias formales de alguna desviación en el área de sistemas auditada.

Debemos señalar que el contenido de los papeles de trabajo puede variar de un auditor a otro y de un tipo de auditoría a otra, ya que en cada trabajo existen procedimientos, técnicas y métodos de evaluación especiales que forzosamente harán diferente la recolección de los documentos. Lo mismo ocurre con la forma de obtener evidencias e incluso con la forma de concentrar los papeles de trabajo.

A continuación presentaremos una propuesta para integrar estos papeles:

- *Hoja de identificación*
- *Índice de contenido de los papeles de trabajo*
- *Dictamen preliminar (borrador)*
- *Resumen de desviaciones detectadas (las más importantes)*
- *Situaciones encontradas (situaciones, causas y soluciones)*
- *Programa de trabajo de auditoría*
- *Guía de auditoría*
- *Inventario de software*
- *Inventario de hardware*
- *Inventario de consumibles*
- *Manual de organización*
- *Descripción de puestos*
- *Reportes de pruebas y resultados*
- *Respaldos (backups)de datos, disquetes y programas de aplicación de auditoría*
- *Respaldos (backups) de las bases de datos y de los sistemas*
- *Guías de claves para el señalamiento de los papeles de trabajo*
- *Cuadros y estadísticas concentradores de información*
- *Anexos de recopilación de información*
- *Diagramas de flujo, de programación y de desarrollo de sistemas*
- *Testimoniales, actas y documentos legales de comprobación y confirmación*

- *Análisis y estadísticas de resultados, datos y pruebas de comportamiento del sistema*
- *Otros documentos de apoyo para el auditor*

En la *figura 7.1* se muestra un ejemplo del contenido de estos documentos, los cuales varían en volumen, contenido y forma, de acuerdo con las necesidades de información del auditor.

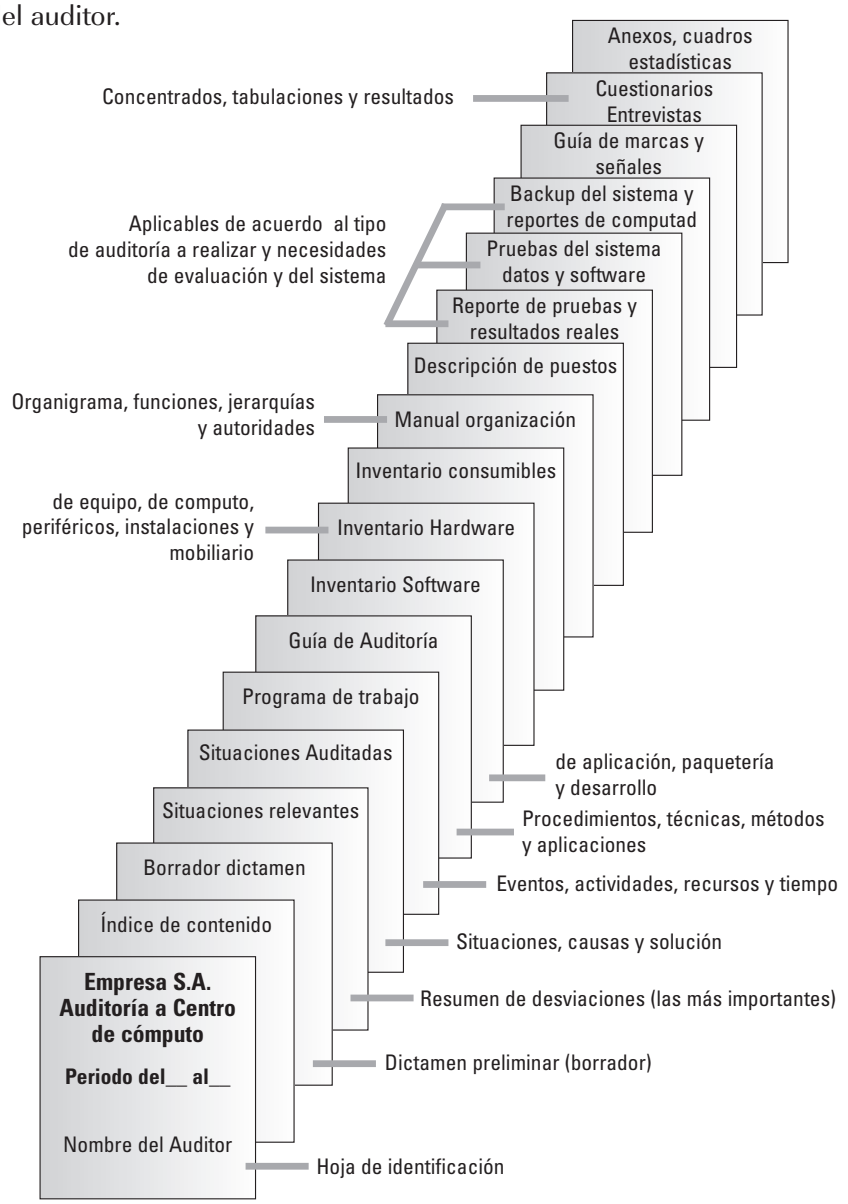


Figura 7.1 *Legajo de papeles de trabajo de la auditoría de sistemas computacionales*

7.1.1 Hoja de identificación

Ésta es la parte frontal del legajo de papeles de trabajo de la auditoría de sistemas computacionales, y es el primer documento formal que se identifica en dicho legajo; en esta hoja, que puede ser una carátula formal rigurosamente empastada o una simple portada de cartón o de papel común y corriente, se anotan los datos elementales que sirven para identificar la documentación contenida en el legajo. Esta portada (*figura 7.2*) debe contener como mínimo los siguientes datos:

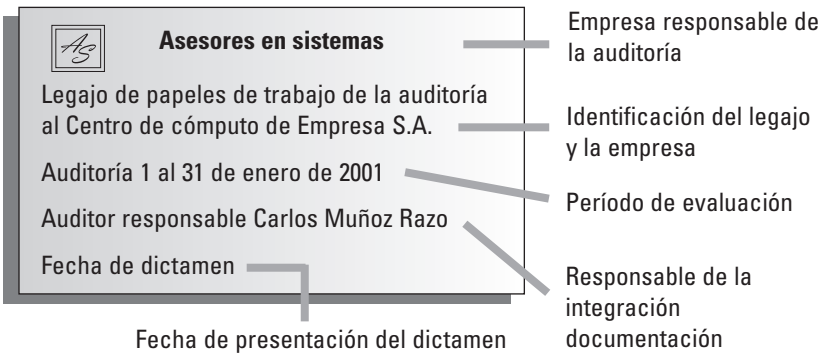


Figura 7.2 *Hoja de identificación*

7.1.1.1 Nombre de la empresa responsable de llevar a cabo la auditoría de sistemas

En esta parte se anotan el logotipo y nombre de la institución, cuando es una empresa de auditoría externa la responsable de realizar la auditoría de sistemas, o el nombre de la empresa y la designación del área de auditoría interna, cuando es el área de auditoría interna la responsable de llevarla a cabo. Es indispensable anotar los datos de una sola empresa (externa o interna); no es válido anotar los de ambas.

7.1.1.2 Identificación del legajo de papeles de trabajo

Aquí va el nombre genérico que se le da al documento y sirve para identificar que se trata de la concentración de los documentos que avalan la realización de la auditoría de sistemas. En algunos casos puede admitirse con otros nombres, según la preferencia del auditor o empresa. Lo importante es que esta parte sirve para identificar, claramente, el contenido de los documentos relacionados con la auditoría de sistemas.

7.1.1.3 Nombre de la empresa o área de sistemas auditada

En este lugar se anota el nombre completo de la *empresa* a la cual se practica la auditoría de sistemas, junto con el nombre del *área de sistemas* en donde ésta se lleva a cabo. En caso de tratarse de una auditoría interna, entonces se anota el nombre del área de sistemas auditada. Lo esencial es que se puedan identificar, lo más claramente posible, los nombres completos de la empresa y del área de sistemas donde se realiza la auditoría.

7.1.1.4 Periodo en que se realizó la auditoría

En este lugar se anota la fecha de inicio de la auditoría (desde que empezó la revisión) y su terminación (hasta el último día de revisión); de preferencia se debe anotar con el formato **Día** (*con números*) **Mes** (*con letras*) **Año** (*con cuatro dígitos*), o con el formato que el auditor prefiera.

7.1.1.5 Puesto y cargo del responsable de realizar la auditoría

Aquí se anota el nombre completo del responsable de llevar a cabo la auditoría; en caso de ser un grupo, se anota el nombre del responsable de la conducción de la auditoría. Se puede anotar a todos los participantes si así se desea, pero siempre se debe destacar al responsable de la auditoría.

7.1.1.6 Fecha de emisión del dictamen final

Es la fecha en la que se presenta por escrito el dictamen final de auditoría; es propiamente la fecha en la que se entrega el resultado de la auditoría del área de sistemas, y éste es aceptado por la dirección superior del área. Lo fundamental es presentar con toda oportunidad dicho informe.

Los puntos anteriores son los que se deben contemplar como mínimo para elaborar la carátula de los papeles de trabajo de la auditoría de sistemas, aunque nada impide que se puedan reseñar otros datos importantes en ella, de acuerdo con las necesidades y características de la empresa auditora; aunque estos datos también pueden ser dictaminados por la empresa o área auditada.

La importancia de este punto es que esta carátula sirve para saber lo más claramente posible a quién pertenecen los papeles de trabajo, el período en que se realizó la auditoría y quién fue el responsable de llevarla a cabo.

7.1.2 Índice del contenido de los papeles de trabajo

En esta parte se hace la descripción detallada y se pagina el contenido total de los papeles de trabajo, con el propósito de identificar rápidamente la página en donde se encuentra cada una de las partes que integran este legajo de papeles.

Respecto al índice, no existe ninguna condicionante ni forma especial de presentarlo, salvo lo estipulado de acuerdo con las necesidades o preferencias de la empresa de auditoría o del auditor responsable de la misma. La única condición es que sea una presentación ordenada y que se identifiquen claramente las páginas y su contenido.

Sin embargo, sugerimos numerar con siglas cada capítulo o parte importante de la auditoría, seguidas de un número consecutivo que vuelva a iniciar en cada parte; por ejemplo: SI-001 (Seguridad Informática – hoja 001). También sugerimos utilizar los siguientes apartados para los documentos de trabajo:

HW	Para la documentación relacionada con el equipo físico, periféricos y demás equipos de sistemas
SW	Para la documentación relacionada con el software y paqueterías
SG	Para la documentación relacionada con la seguridad informática
BD	Para la documentación ralacionada con las bases de datos, información y demás archivos de datos
DS	Para la documentación relacionada con el análisis, diseño y desarrollo de sistemas
IS	Para la documentación relacionada con las instalaciones del área de sistemas
CC	Para la documentación relacionada con el centro de cómputo
GA	Para la documentación relacionada con la gestión administrativa del centro de cómputo
CM	Para la documentación relacionada con los consumibles del área de sistemas

7.1.3 Dictamen preliminar (borrador)

El auditor utiliza esta sección para conservar, como papeles de trabajo, el resultado del dictamen preliminar que presentó a discusión con los involucrados en la evaluación, a fin de hacer el análisis y consulta posteriores de todos los aspectos que presentó en forma de borrador.

Este dictamen preliminar es un borrador (o varios borradores) que contiene un resultado preparatorio de la evaluación del área de informática, del sistema auditado, de la función específica de dicha área o de cualquier otro aspecto relacionado con los sistemas de la institución. Debemos señalar que este documento* es un bosquejo en el cual se indican las desviaciones encontradas y el llamado dictamen (juicio) que hace el auditor de lo que encontró durante su revisión.

Todo este material se debe guardar, casi siempre, como documentos de trabajo, para utilizarlo como soporte en aclaraciones posteriores o para preparar el informe final.

Debido a la importancia que tiene este documento para la auditoría, a que éste es el resultado de una evaluación de sistemas, a las características y técnicas especiales para su elaboración, así como los manejos específicos de su redacción y presentación, en el siguiente capítulo haremos una presentación más completa y detallada del dictamen de auditoría de sistemas. Por esta razón, dejaremos este punto sólo como una mención.

7.1.4 Resumen de desviaciones detectadas (las más importantes)

Otro de los documentos importantes que debe conservar el auditor en el legajo de papeles de trabajo es la copia de los documentos originales, y en algunos casos el borrador manuscrito, de las desviaciones que considera como las más importantes encontradas durante la revisión, así como sus causas y posibles soluciones, que presenta en el formato de desviaciones encontradas..

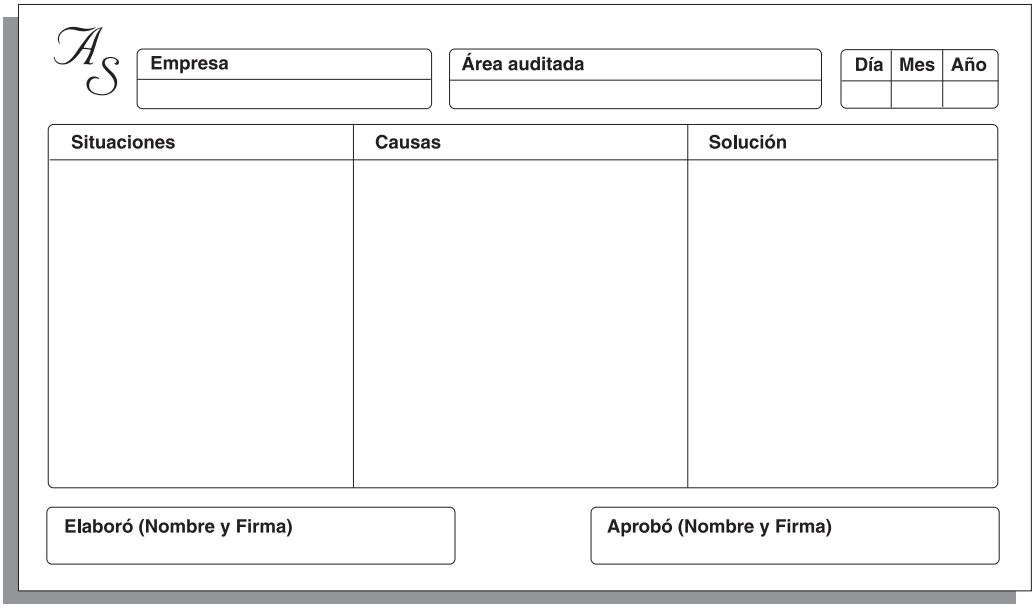


Figura 7.3 *Desviaciones relevantes*

* En el siguiente capítulo analizaremos más a fondo el dictamen de auditoría y su informe formal

En la imagen anterior sólo se muestran los puntos básicos del formato propuesto para presentar las desviaciones más importantes de una auditoría de sistemas, ya que en el capítulo siguiente explicaremos más a fondo su elaboración y uso.

El auditor elaborará el informe final con base en el análisis de estas desviaciones relevantes, y lo presentará como informe final y dictamen de auditoría de sistemas computacionales.

7.1.5 Situaciones encontradas (situaciones, causas y soluciones)

En esta parte de los papeles de trabajo se presentan los manuscritos, y en ocasiones los borradores mecanografiados, de todas las situaciones detectadas durante la auditoría, conforme al formato que se propone en el capítulo siguiente, separando en *situaciones encontradas,* las *causas* que las originan y las posibles *soluciones*; también se anota al *responsable* de solucionarlas y las *fecha de solución* para cada causa o situación reportada, conforme se describe en el formato que presentamos a continuación:

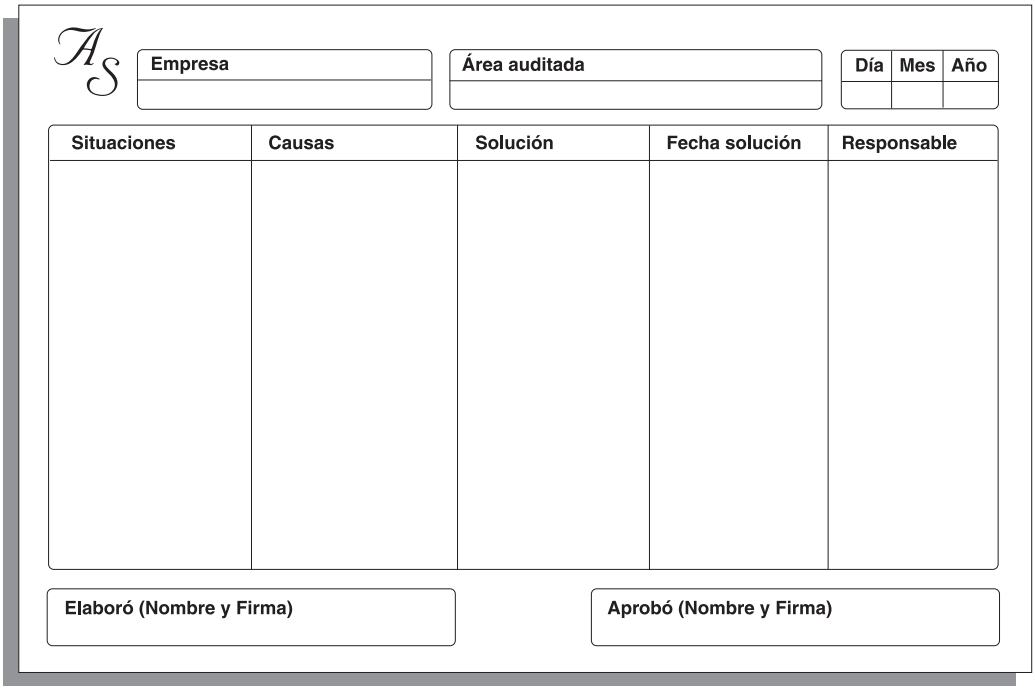


Figura 7.4 *Situaciones encontradas*

El propósito de guardar los formatos de desviaciones en esta sección es tener a mano los problemas reportados durante la revisión, guardando desde el primer borrador hasta el último de las llamadas *situaciones detectadas*, o algún nombre similar que

se dé a las incidencias que se reportan en este formato. El análisis de las desviaciones detectadas se podrá tomar como base para identificar las desviaciones relevantes señaladas en la sección anterior.

Debido a la importancia de este punto, en el siguiente capítulo también analizaremos más a fondo la elaboración y presentación del formato de presentación de desviaciones encontradas, sus causas y soluciones.

7.1.6 Programa de trabajo de auditoría

Es el documento formal (por escrito) de los planes, programas y presupuestos hechos para el control y desarrollo de la auditoría; este documento se elabora en un formato especial o en una gráfica en la cual se anotan las etapas y actividades para la evaluación, así como los tiempos para llevarla a cabo; también se anotan los recursos disponibles para realizar todas esas actividades. Estos aspectos se deben señalar en forma cronológica, secuencial y correctamente coordinada.

Por la importancia que tiene este punto para el desarrollo de una auditoría de sistemas, en el capítulo anterior, *Metodología para realizar auditorías de sistemas computacionales*, analizamos detalladamente el plan o programa de trabajo; por esta razón, únicamente señalaremos los principales conceptos que el auditor debe contemplar como parte del programa de trabajo:

1ª etapa: **Planeación de la auditoría de sistemas computacionales**

- ***P.1*** *Identificar el origen de la auditoría*
- ***P.2*** *Realizar una visita preliminar al área que será evaluada*
- ***P.3*** *Establecer los objetivo de la auditoría*
- ***P.4*** *Determinar los puntos que serán evaluados en la auditoría*
- ***P.5*** *Elaborar planes, programas y presupuestos para realizar la auditoría*
- ***P.6*** *Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría*
- ***P.7*** *Asignar los recursos y sistemas computacionales para la auditoría*

2ª etapa: **Ejecución de la auditoría de sistemas computacionales**

- ***E.1*** *Realizar las acciones programadas para la auditoría*
- ***E.2*** *Aplicar los instrumentos y herramientas para la auditoría*
- ***E.3*** *Identificar y elaborar los documentos de desviaciones encontradas*
- ***E.4*** *Elaborar el dictamen preliminar y presentarlo a discusión*
- ***E.5*** *Integrar el legajo de papeles de trabajo de la auditoría*

3ª etapa: **Dictamen de la auditoría de sistemas computacionales**

- ***D.1*** *Analizar la información y elaborar un informe de situaciones detectadas*
- ***D.2*** *Elaborar el dictamen final*
- ***D.3*** *Presentar el informe de auditoría*

7.1.7 Guía de auditoría

Este documento, llamado *guía de auditoría*, es fundamental para el buen desarrollo de una auditoría, ya que es una herramienta auxiliar para el trabajo del auditor; por esta razón, debe tener una descripción detallada de todos y cada uno de los puntos importantes que se deben auditar, según las necesidades de evaluación y características específicas del área de sistemas de la empresa. Aquí se presenta un ejemplo:

Referencia	Actividad o función a evaluar	Técnica de evaluación	Ponderación	Calificación	Observaciones
GA-01	Evaluar la estructura de organización del área de sistemas de la empresa, sus puestos, funciones, líneas de autoridad y perfil de puestos	Revisión documental de manual de organización Entrevistas con funcionarios y empleados	.05%		

Figura 7.5 *Guía de auditoría*

En este documento se indica* cada uno de los puntos que deberá evaluar el auditor, así como la forma de evaluarlos y la descripción de las técnicas, métodos y herramientas que deberá utilizar en dicha evaluación, mismos que deben ser diseñados previamente, de acuerdo con el tipo de auditoría y la especialidad informática que se tenga que evaluar en el centro de cómputo de la empresa (vea la figura 7.5).

Es de gran utilidad para el auditor integrar la guía de auditoría a los papeles de trabajo, ya que en este documento anota cada uno de los puntos que evaluó, así como las técnicas, métodos y procedimientos de auditoría que aplicó en la evaluación. También anota toda la información que obtuvo de cada uno de los aspectos que analizó, así como

* Debido a la importancia que tiene este documento, en el capítulo 11, relacionado con las herramientas especializadas de auditoría de sistemas, especificaremos la importancia y utilidad de todos sus puntos.

la obtención y/o generación de documentos, datos e información que le sirven como referencia para corroborar las evidencias sobre las desviaciones encontradas. Asimismo, esta guía servirá de referencia para planear las próximas auditorías.

7.1.8 Inventarios

Una de las principales herramientas que utiliza el auditor de sistemas son los inventarios, los cuales le sirven para contar los elementos que existen en el área que va a evaluar, según los equipos, artículos o partes del sistema que se traten; además, con la información que obtiene puede comparar lo que debería existir y lo que realmente existe de los elementos que se están inventariando; con ello puede comprobar que la guarda y custodia de los bienes de la empresa sean adecuadas.

Aunque existen muchos tipos de inventarios, es recomendable utilizar los inventarios que se hayan acordado en la planeación de la auditoría, de acuerdo con su origen y objetivos, así como con las especificaciones de revisión que se hayan establecido. Por esta razón, a continuación presentaremos los principales inventarios para el área de sistemas:

Inventario de software
Inventario de hardware
Inventario de bases de datos e información de la empresa
Inventario de proyectos y desarrollos computacionales
Inventario de puestos de trabajo en el área de sistemas
Inventario de reportes de pruebas y resultados
Inventario de mobiliario y equipos
Inventario de instalaciones de voz, datos y energía
Inventario de instalaciones de redes
Inventario de manuales e instructivos
Inventario de respaldos, disquetes, cintas y sistemas de resguardo de información
Inventario de consumibles

A continuación presentaremos la manera de diseñar el *inventario de software*. En el capítulo 9*, Instrumentos de recopilación de datos aplicables en una auditoría de sistemas computacionales*, analizaremos más detalladamente el diseño y aplicación de los demás inventarios señalados anteriormente.

7.1.8.1 Inventario de software

Uno de los documentos fundamentales que el auditor debe integrar en el legajo de papeles de trabajo, es el inventario de los programas, lenguajes, paqueterías, sistemas operativos y cualquier otro software que se utilice en la institución para el procesamiento de la información y la operación de los sistemas.

En el documento que presentamos a continuación se debe anotar la versión del software, las licencias para su uso y en general todas sus características, así como a los responsables de su resguardo (vea la figura 7.6).

FECHA DD MM AA 28 03 02 — **HOJA** 12 de 29

EMPRESA: Bonzai Audi Area Auditada *Centro de Cómputo*
PERÍODO: 04 marzo 96 al 08 marzo 02
RESPONSABLE: Claudia de León Rámirez

Inventario de Software

REF	Software	Versión	No. Inventario	Licencias	Presentación	Asignado a	Localización
W01	Windows NT	311	09 234-1	20	CD-ROM	C. Cómputo	Servidor 1
W02	Office	95	09 334-1	1	CD-ROM	C. Cómputo	Servidor 1
W03	Office	95	09 334-2	1	CD-ROM	Contabilidad	Finanzas
W04	Office	97	09 334-2	1	CD-ROM	Diseño	Producción
W05	Office	97	09 334-2	1	CD-ROM	R. Humanos	Admos.
BD 1	Easy Case	12	15 234-1	3	8 Disk	C. Cómputo	Desarrollo
BD 2	Informix	14	15 345-3	1	10 Disk	C. Cómputo	Desarrollo
SO 1	MS-DOS	60	01 565-2	1	3 Disk	C. Cómputo	Desarrollo
SO 2	Unix	30	01 456-3	1	CD-ROM	C. Cómputo	Desarrollo

Figura 7.6 *Inventario de software*

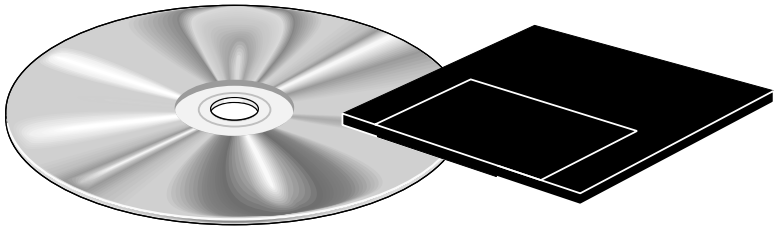
El propósito de este documento es que el auditor tenga un registro pormenorizado del total de software que hay en la empresa, ya sea el de cada computadora instalada, el que está disponible en la red de sistemas, el adquirido a terceros (llamado software comercial), el que ha sido desarrollado en la empresa (llamado software desarrollado) e incluso las paqueterías, lenguajes, sistemas operativos, etcétera.

Con esa información en sus papeles de trabajo, el auditor puede analizar y comprobar la utilidad, aprovechamiento, suficiencia y seguridad del software. Además le sirve de soporte en caso de haber desviaciones en la existencia y actualización del mismo.

7.1.9 Respaldo de datos (BACKUPS), información y programas de aplicación de auditoría

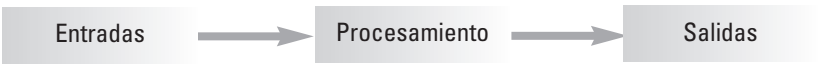
Los sistemas computacionales tienen características específicas en cuanto a la forma de captura, almacenamiento y emisión de información; por esta razón, encontramos que el respaldo de documentos es muy importante en una auditoría de sistemas computacionales. Estos documentos de trabajo, que contienen información importante, se

pueden archivar en disquetes, cintas, CD-ROMs, DVDs o en algún otro medio eletrónico de captura y lectura de datos.



En este tipo de auditorías, los llamados papeles de trabajo adquieren un matiz muy especial debido a la forma en que se archiva la información en ellos; así encontramos que debemos documentar datos que muchas veces no están archivados en papel sino en sistemas computacionales; por lo tanto, debemos saber cómo capturar, extraer y archivar esa información en algún medio electromagnético de captura y lectura de información. Sin embargo, no sólo es por la forma de almacenar la información, sino también por la cantidad, periodicidad y utilidad de la información que va a ser documentada. Está claro que no se puede documentar como papeles de trabajo toda la información que se procesa en los sistemas computacionales, sino únicamente la que haya sido designada de algún proceso de recopilación específico.

Es bueno recordar que un sistema computacional es un sistema de entrada de datos, procesamiento de información y emisión de resultados, compuesto por un conjunto de equipos físicos (*hardware*) que capturan los datos a través de sus unidades de entrada (*teclado, disquetes, disco duro, CD-ROM*), y los procesan (*en la CPU*) a través de sus lenguajes, programas y paquetes (*software*) para emitir información (en *pantalla, impresora, disco duro, disquetes*) útil para la empresa.



Sin embargo, el auditor sólo utiliza la información que producen los sistemas, si ésta le es útil para evaluar algún aspecto relacionado con la revisión que está realizando, y casi nunca toma en cuenta las operaciones y actividades internas que realiza el sistema para arrojar esa información.

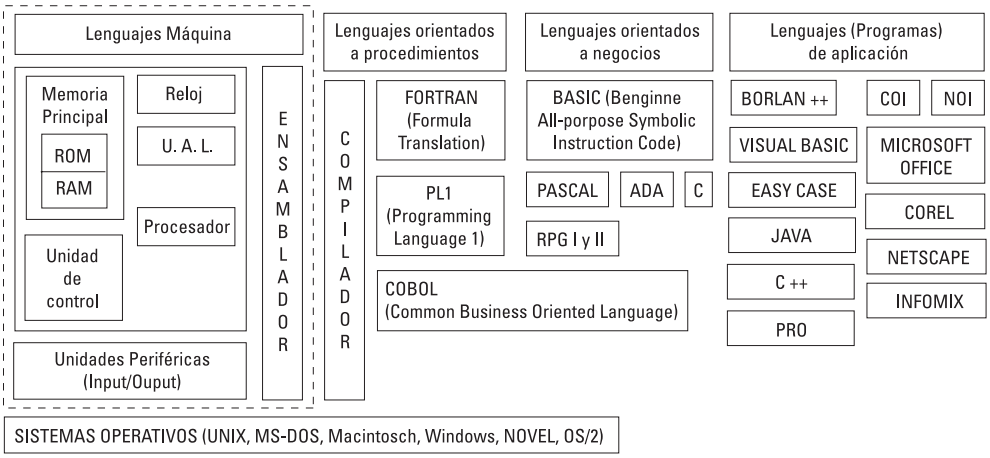


Figura 7.7 *Composición de una CPU*

En la *figura 7.7* se hace un pequeño esbozo de los sistemas computacionales, sus características, marco conceptual y de algunos otros aspectos básicos que serán útiles para que el auditor recuerde o conozca los aspectos más importantes de lo que va a auditar.

Los papeles de trabajo que contienen la información que se maneja en los sistemas se deben almacenar en dispositivos especiales; por esta razón, a continuación indicaremos dos de los principales tipos de datos e información, así como los medios de almacenamiento que se deben considerar como documentos de los papeles de trabajo de la auditoría de sistemas computacionales. El propósito de presentar estos dos ejemplos es que el auditor sepa como se deben archivar dichos papeles de trabajo. Aunque en la práctica, el responsable de la auditoría será quien decida el tipo de información que se debe archivar y en qué medio se puede hacer, según las necesidades de su propia evaluación.

Respaldos de bases de datos e información de la empresa

Es el respaldo periódico de información que se hace a través de disquetes (o cualquier otro medio), en los cuales se almacenan los datos de algún ejercicio, operación, o cualquier otra serie de datos que es importante conservar. El auditor de sistemas debe decidir cómo conservar esta información como parte de su evaluación.

En la práctica de la auditoría de sistemas, el auditor debe evaluar los respaldos, la periodicidad con la que se llevan a cabo, el período de duración o actualización de la información respaldada, la confiabilidad del respaldo, la manera de evitar fugas de información, entre muchos otros aspectos.

Respaldos de programas (copias de respaldo de programación)

En este caso, el auditor debe verificar que existan respaldos (periódicos o únicos) de los sistemas operativos, programas, paqueterías o sistemas realizados en la empresa, con el objeto de evaluar que dichos respaldos sean los adecuados en caso de ocurrir problemas en el sistema. Además debe verificar que los respaldos estén perfectamente custodiados, y que no existan más copias de las permitidas, para evitar la llamada piratería de programas o la fuga de información de la empresa.

7.1.10 Otros documentos que debe contener el legajo de papeles de trabajo de la auditoría

Debemos señalar que el responsable de la auditoría de sistemas es quien debe definir el contenido y la forma de guardar los papeles de trabajo, y debe hacerlo de acuerdo con las necesidades específicas de evaluación, siguiendo, de preferencia, la forma acostumbrada de captura y almacenamiento de la información recabada en la empresa o área auditada. Asimismo, es quien debe determinar las secciones, partes y documentos que se deben guardar en el legajo de papeles de trabajo. Por esta razón, a continuación presentamos algunos otros documentos que debe contener el citado legajo.

7.1.10.1 Estadísticas y cuadros concentradores de información

Este punto se refiere a todo lo relacionado con los cuadros estadísticos que utiliza el auditor para recabar y evaluar la información obtenida en la evaluación; en estos cuadros se incluyen las gráficas, datos, censos, muestras, formulas estadísticas, etc. Es de suma importancia para el auditor archivar estos cuadros en el legajo de papeles de trabajo, ya que le pueden servir para acreditar sus opiniones; además, pueden servir de referencia para los auditores novatos sobre la manera de elaborar estadísticas y obtener evidencias de una evaluación de sistemas.

Debido a la importancia de este punto, en la sección 7.3 de este capítulo analizaremos ampliamente algunos ejemplos de estas recopilaciones.

7.1.10.2 Anexos de recopilación de información

Además de la información estadística, el auditor puede obtener otro tipo de información que le es útil para realizar la evaluación de los sistemas computacionales, misma que puede ser muy variada y que debe guardar como anexos de información; a continuación presentamos algunos ejemplos de estos anexos:

- *Resultados del procesamiento de datos*
- *Descripción de puestos, funciones y actividades*

- *Resultados y pruebas de cálculos de procesamientos que se efectúan en el sistema*
- *Copias de formatos y licencias de programas y paqueterías*
- *Copias de resguardos de equipos y mobiliario*
- *Mapas de distribución de redes, instalaciones, equipos, muebles y sistemas de información*
- *Mapas de rutas de evacuación y seguridad del área de sistemas*
- *Bitácoras de reportes y servicios de mantenimiento preventivo y correctivo*
- *Resultados de inventarios y pruebas de la arquitectura de los sistemas*
- *Resultados de diseños, análisis, codificación, pruebas y liberación de sistemas*
- *Copias de programas fuente, objeto y codificación de los sistemas desarrollados en la empresa*
- *Resultados de cotizaciones y estudios de mercado para adquisiciones de hardware, software, mobiliario y consumibles de sistemas*
- *Otros documentos útiles para el auditor*
- *Diagramas de sistemas, de programación y desarrollo de sistemas*

Una de las actividades más importantes del trabajo en el área de sistemas de una empresa es el desarrollo de los propios sistemas; durante una revisión de este tipo, es responsabilidad del auditor evaluar el correcto y oportuno desarrollo e instalación de los sistemas; para ello, además de evaluar su funcionamiento, debe anexar al legajo de papeles de trabajo los documentos que contengan la información sobre el análisis, diseño, programación, pruebas e instalación de los sistemas de la empresa, como parte de una posible evidencia de su evaluación. El auditor debe incluir en estos documentos los diagramas de los sistemas, las metodologías utilizadas para el análisis y diseño de los mismos, sus codificaciones, programas objeto, fuente y todos los aspectos necesarios que estén relacionados con el desarrollo de los sistemas de la empresa.

7.10.1.3 Testimoniales, actas y documentos legales de comprobación y confirmación

En algunos casos, estos documentos pueden ser de los más importantes de una auditoría de sistemas, debido a que son el testimonio de empleados, usuarios, responsables o de las personas que por algún motivo declararon algo relacionado con los sistemas auditados o con alguna situación específica. Estos documentos deben ser recabados con toda formalidad.*

* En el capítulo 10 trataremos detalladamente las características, requisitos y formas de realizar estas actas testimoniales.

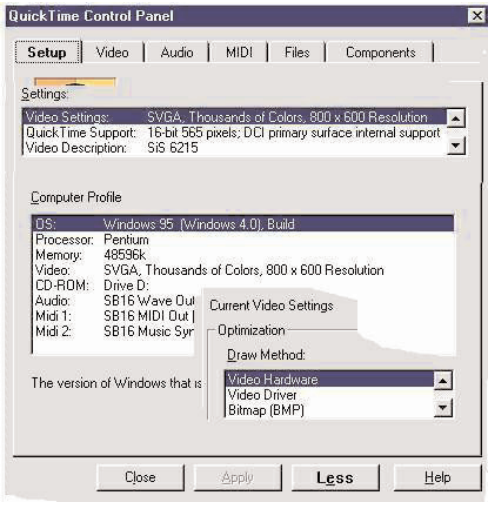
Asimismo, estos documentos son muy valiosos en cualquier tipo de auditoría, ya que sirven para corroborar desviaciones importantes, y en algunos casos pueden tener valor legal para posteriores diligencias y pueden servir como pruebas en algún litigio. Por esta razón es de suma importancia tener a la mano este tipo de documentos.

7.10.1.4 Análisis estadístico de resultados, datos y pruebas de comportamiento del sistema

Así como es necesario guardar los datos, muestras y fórmulas estadísticas indicadas, también es necesario conservar los documentos relacionados con el análisis estadístico de los resultados, ya que además de servir como evidencia de las desviaciones encontradas, también pueden servir de referencia para futuras evaluaciones; es decir, se pueden utilizar como modelo para retomar los procedimientos seguidos y obtener resultados similares o para enseñar a los auditores novatos.

Conservar por escrito estos análisis debe ser una prioridad para el responsable de la auditoría, ya que de esta manera se podrá interpretar el resultado de su evaluación, y en caso de que el auditor que hizo esos análisis no esté presente, éstos se pueden estudiar y llegar a las mismas conclusiones.

7.1.11 Otros documentos especializados de una auditoría de sistemas

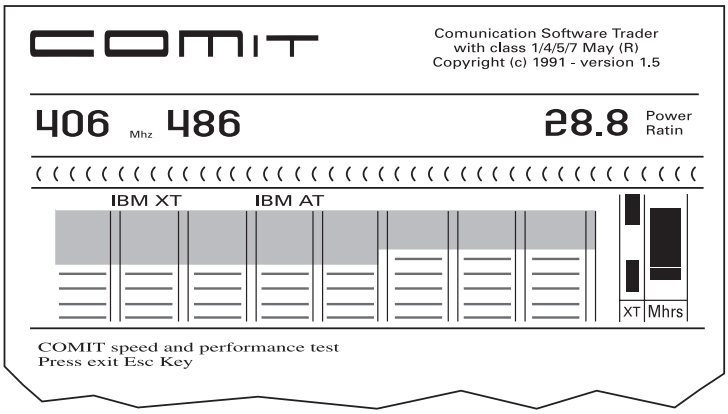


En el legajo de papeles de trabajo también se debe anexar la información (en papel o electrónicamente) relacionada con los reportes, análisis y resultados de pruebas, configuraciones y exámenes especializados del sistema computacional, de las instalaciones o de cualquier otro aspecto relacionado con el área de sistemas; también se debe anexar lo relacionado con el procesamiento de información o con cualquier otra actividad informática.

Asimismo, el auditor debe anexar cualquier otro documento que a su juicio sea de importancia para la auditoría y que necesite conservar; por ejemplo, comprobantes de viáticos, oficios de presentación, correspondencia, minutas de reuniones, nombramientos y cualquier otro tipo de documentos útiles para la auditoría.

En este ejemplo se maneja el programa especializado *QuickTime for Windows, versión 21.1.57@ de Apple Computer Inc.,* que se utiliza para verificar el contenido y funcionamiento del equipo de cómputo y de sus componentes. La composición de esta utilería se presenta únicamente para ejemplificar alguno de los muchos productos que pueden ser incluidos como documentos en el legajo de papeles de trabajo de una auditoría de sistemas computacionales.

En el siguiente ejemplo se presenta un análisis de la velocidad de procesamiento de una PC, en relación con los parámetros compatibles con IBM en AT y XT (1993). ***COMIT***@* es una marca registrada por *Comunications Software by Tradenw Inc*., y es otro ejemplo de los documentos de apoyo para el auditor de sistemas que se pueden anexar al legajo de papeles de trabajo.



7.2 Claves del auditor para marcar papeles de trabajo

Son las marcas de carácter informal que utiliza exclusivamente el auditor o el grupo de auditores que realizan la auditoría, con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor. El auditor en jefe puede imponer el uso de estos símbolos o pueden ser utilizados por acuerdo del grupo, aunque también puede suceder que no sean utilizados en una auditoría.

Su utilidad radica en que tienen un significado preciso que todos los auditores conocen y utilizan para destacar aspectos importantes de los documentos que van revisando, y en que sirven como identificadores uniformes de todas las actividades que se desarrollan durante una evaluación; así, cuando alguien del grupo de auditores encuen-

@ *QuickTime for Windows* es propiedad de *Apple Computer Inc. 1988-1996 All Rights Reserved*, y es un ejemplo de los programas útiles para auditorías de sistemas computacionales.
@* **COMIT** es propiedad de *Comunications Software by Tradenw Inc*. 1993 All Rights Reserved, y es otro ejemplo de los programas útiles para auditorías de sistemas computacionales

tra algún documento con estas marcas, sabe que éste ya ha sido revisado o que tiene una característica especial en la cual se tiene que advertir alguna observación, de acuerdo con el significado de los símbolos. Todos los auditores deben utilizar los mismos símbolos al hacer anotaciones en los documentos que evalúen.*

También ayudan al auditor a realizar un resumen de observaciones para identificar de manera rápida y sencilla las posibles desviaciones; el simple uso de estas marcas también le permite estandarizar su trabajo, siempre y cuando sean las mismas para toda la revisión.

Con el uso de estos símbolos también se evita el abuso en la recopilación de copias inútiles de papeles de evaluación y documentos oficiales, los cuales sirven para identificar los aspectos revisados, como apoyo para la evaluación o para cualquier otro aspecto similar poco importante.

Con el uso de estas marcas se hace más sencilla la revisión de documentos impresos en papel, de disquetes, bases de datos y de todo lo relacionado con los sistemas evaluados.

Es conveniente aclarar que no existe algún convenio formal respecto al tipo de marcas utilizadas entre un auditor y otro, sino que su diseño y uso es producto de las experiencias de auditorías anteriores compartidas entre los auditores. Sin embargo, por sentido común se unifican las marcas o símbolos que se utilizan en los papeles de trabajo; entre estas marcas destacan las siguientes:

Propuesta de símbolos convencionales utilizados en una auditoría de sistemas computacionales

Símbolo	*Significado o interpretación*	*Símbolo*	*Significado o interpretación*
✓	Verificado una vez	✓	Archivo verificado
✓	Verificación dos veces		Archivo con errores
✓✓	Dato correcto		Listado de resultados
✗	Dato con error		Verificado en pantalla
∅	Pendiente de checar		Errores en resultados
✓	Checado y corroborado		Transmisión interrumpida
◎	Desviación pendiente de comprobar	*com*	Comentario especial
◎	Desviación comprobada	***OBS***	Observación
¿?	Confirmar preguntas	EE	Entrevista empleado
!!	Observación importante	EF	Entrevista funcionario
ERR	No coinciden datos	EU	Entrevista usuario
VIR	Virus informático Disco contaminado	EP	Entrevista al personal
ENT	Entrevista	CUES	Cuestionario

* Al referirnos a los documentos en evaluación, también nos estamos refiriendo a los medios electromagnéticos de captura y emisión de información, así como a los demás elementos de análisis de información del área de sistemas.

Es importante destacar que los símbolos anteriormente presentados son producto de la experiencia en la aplicación de auditorías de sistemas, pero su uso no es una obligación ni pretendemos estandarizarlos, nuestra única intención es presentarlos como referencia y ejemplo a seguir. Sin embargo, por su utilidad y validez comprobadas en las evaluaciones de sistemas, sugerimos al lector que estudie y adopte aquellos que más convengan a sus intereses.

Es de suma importancia enfatizar que estos símbolos se deben diseñar en forma conjunta, se deben anotar en un mismo documento y distribuir copias entre los participantes de la auditoría; también se debe vigilar constantemente que los auditores apliquen estos símbolos con el mismo criterio. Con esto se garantizan la uniformidad y continuiad de la evaluación.

7.3 Cuadros, estadísticas y documentos concentradores de información

En esta parte se presentan todos los documentos del legajo de papeles de trabajo que servirán de soporte para presentar la información recopilada durante la auditoría y que es conveniente destacar por su importancia, por su nivel de información o por cualquier otro aspecto que resulte determinante para la evaluación y para comprobar las desviaciones plasmadas en las situaciones detectadas y en las situaciones importantes.

Por lo general estos documentos son complemento de alguna revisión y sirven para identificar y comprobar desviaciones y situaciones.

Dichos documentos pueden ser estadísticas, gráficas o cuadros en los cuales se concentran y se comparan datos tales como listados de resultados de un proceso y listados de seguimiento de las actividades, operaciones y tareas que se realizan con un sistema computacional, así como los concentrados de información estadística, las bitácoras de seguimiento y reportes, y en sí cualquier dato que pueda ser incluido en las estadísticas.

A continuación presentaremos algunos documentos que pueden ser considerados dentro de este rubro:

7.3.1 Cuadro de concentración estadística

Consumo de horas de impresión por semana

Tipo de impresora	Depto. contable	Depto. de finanzas	Depto. de ventas	Depto. de diseño	Totales
Epson 10"	5	6	8	1	20
Epson 15"	19	10	4	1	34
Inyección de tinta	2	4	4	25	35
Láser	2	4	2	20	28
Totales	28	24	18	47	117

Es un cuadro (columnas y filas) en donde se anotan datos útiles tales como operaciones aritméticas, matemáticas y/o estadísticas que le darán algún significado a la evaluación.

En el ejemplo se presenta un cuadro con el consumo de horas de impresión semanales de las impresoras de las diferentes áreas de una empresa. Con el análisis de estos datos se podrían optimizar las impresoras mediante un pool de impresión o una red con impresoras compartidas, según sea el caso que se presente en la realidad.

7.3.2 Cuadro de comparación de información

Tipo de impresora	Depto. contable	Depto. de finanzas	Depto. de ventas	Depto. de diseño	Total área	Tiempo programado	Diferencia
Epson 10"	5	6	8	1	20	40	-20
Epson 15"	19	10	4	1	34	40	-6
Inyección de tinta	2	4	4	25	35	40	-5
Láser	2	4	2	20	28	40	-12
Totales	28	24	18	47	117	160	-43
Tiempo asignado de impresión	30	30	30	70	160		
Diferencia	-2	-6	-12	-23	-43		

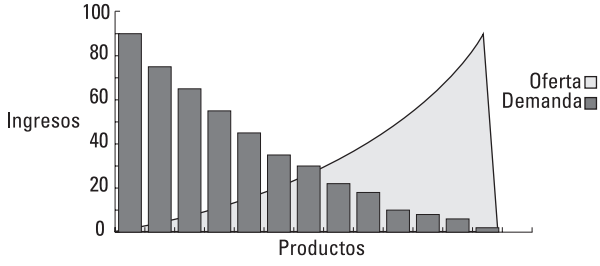
Es un cuadro de concentración estadística de datos, en el que se comparan los resultados contra parámetros normales previamente definidos; esta comparación nos dará un criterio de evaluación para esos rangos.

En el ejemplo de la tabla se hace la comparación del tiempo programado de impresión contra el tiempo real.

7.3.3 Gráficas de cualquier tipo

Es la representación gráfica de la información que proporciona un valor significativo a los datos. El propósito de estas gráficas es representar los datos en forma visual.

En el ejemplo la gráfica representa ingresos contra consumos, a fin de señalar la llamada oferta y demanda.



Éstos fueron sólo algunos ejemplos de cuadros de concentración de datos en forma estadística y gráfica; pero existen muchos tipos de cuadros y gráficas que se utilizan en una auditoría, de acuerdo a las necesidades de evaluación de los sistemas computacionales de una empresa.

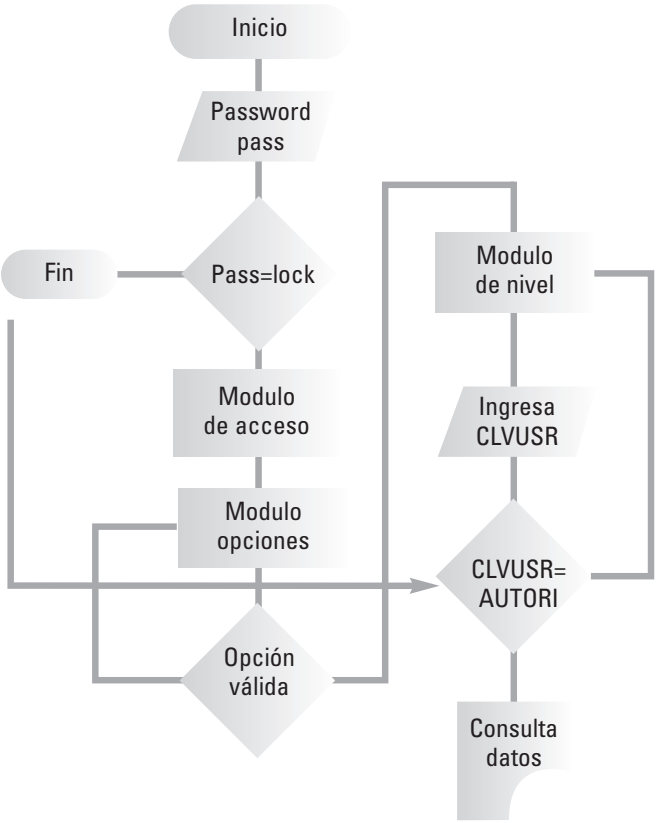
7.4 Diagramas de sistemas

Es la representación gráfica del procedimiento que se sigue para realizar una serie de operaciones y actividades debidamente coordinadas entre sí.

En el ambiente de sistemas, este diagrama es la representación gráfica de un procedimiento de sistematización, el cual está representado por líneas de flujo y símbolos que representan algún tipo de actividad, de documento o de una decisión. Esta simbología se acuerda previamente, para que quienes la vean la interpreten de la misma manera.

7.4.1 Diagrama de flujo

En este tipo de diagramas se señalan los procedimientos por medio de símbolos adoptados para ejemplificar el flujo que siguen los datos.



Cabe señalar que estos símbolos son convencionales, por ejemplo:

Para decisión se ocupa el rombo.

Para el flujo se utilizan líneas con o sin flechas que señalan el seguimiento de las aciones.

Para representar impresión se utiliza una hoja cortada.

En el ejemplo se ve un procedimiento para iniciar un sistema de consulta en el que se incluyen passwords, módulos de acceso y módulos de usuario, así como el flujo que se sigue para entrar al sistema.

El uso de los diagramas de flujo es una de las principales herramientas que utiliza un auditor para la evaluación de programas, bases de datos, programación de sistemas y cualquier otro desarrollo de sistemas de la empresa, debido a que permite seguir perfectamente los datos. En el capítulo 11 se presenta una apartado especial sobre la diagramación de sistemas.

7.4.2 Diccionario de datos

Éste es otro de los documentos importantes para el auditor, ya que le ayuda a identificar el contenido y composición de las bases de datos, su forma, el tamaño de los archivos, el número de dígitos por cada registro que ingresa a la computadora y demás características que componen una base de datos.

Diccionario de datos

CAMPO	TIPO	TAMAÑO	DESCRIPCIÓN
Cmater	Carácter	5	Clave del material.*
Cusuario	Carácter	5	Clave del usuario.*
Fprestam	Numérico	6	Fecha del préstamo.*
Flímite	Numérico	6	Fecha límite de entrega.*
Fentrega	Numérico	6	Fecha de devolución del préstamo.
Xedopres	Carácter	9	Estado del préstamo: PRESTADO, PERDIDO O DEVUELTO.*
Crespons	Carácter	3	Iniciales de la persona que modificó el registro por última vez.*

Los asteriscos indican los campos que no pueden estar vacíos, debido a la funcionalidad que se necesita del sistema.

En el ejemplo se observa un diccionario de datos que contiene la identificación del campo, su descripción, el tipo de datos que admite y el tamaño de los datos que ingresan.

Para el auditor es muy importante identificar y evaluar la correcta elaboración de las bases de datos, y una forma de realizarlo es por medio de los diccionarios de bases de datos, ya que éstos le ayudan a identificar la forma en que se realizaron estos archivos y la forma en que se utilizan.

7.4.3 Modelos

Estos documentos son muy importantes en la evaluación de los sistemas computacionales, ya que ayudan al auditor a representar la realidad de lo que va a evaluar.

Modelos
*** Son representaciones abstractas de la realidad**

Análisis	Procesos	De flujo de datos
	Gráficas de transformación	
	Datos	Entidad-Relación Modelado de datos Estructura de datos Estructura lógica
	Estado-Evento	Estado-Transición Historia de vida de la entidad
Diseño	Diseño	Gráficas de estructura
Las demás no son soportadas		

En su acepción básica, modelo es la representación gráfica o a escala de una cosa, idea, o de la realidad. Para el caso concreto de los sistemas, el modelo representa la abstracción gráfica de la realidad que el analista o programador conceptualiza para plasmarla en un documento.

De hecho, en estricto sentido, todas las gráficas y diagramas de flujo aquí mostrados son modelos que representan la realidad.

En la figura se ejemplifican las principales características de cualquier modelo utilizado en la programación orientada a objetos, incluyendo la descripción de los procedimientos presentados. Es obvio que este modelo se expresa por sí mismo.

En el capítulo 10 se amplían los ejemplos de diagramas.

Informes de auditoría de sistemas computacionales

8

Estructura del capítulo:

Objetivos del capítulo

Destacar la importancia que tiene el saber presentar profesionalmente los informes de auditorías de sistemas computacionales, a fin de que el auditor exprese su opinión y los resultados de una revisión de manera correcta, e identifique las características básicas de fondo y forma del informe, el procedimiento fundamental para elaborarlo, la estructura que deberá tener su presentación, así como los formatos que se utilizan para una óptima presentación de las desviaciones encontradas.

Introducción del capítulo

Plasmar palabras en un dictamen, en un libro, en un oficio, en un documento o en cualquier otro escrito, es dar nuestro sello personal en la comunicación de ideas, conceptos y conocimientos. En el caso específico de la auditoría de sistemas, además de reportar las observaciones encontradas, el auditor muestra su forma de ser y exhibe sus conocimientos, habilidades y experiencia en el área de auditoría de sistemas. También manifiesta un esbozo general de su cultura. A eso le llamamos estilo personal del redactor del informe.

El informe es el documento más importante de la auditoría de sistemas computacionales, debido a que a través de éste se presentan los resultados obtenidos durante la evaluación; en él se plasman, por escrito, las observaciones y el dictamen que emite el auditor, quien, de acuerdo con su experiencia, conocimientos e información recopilada, evalúa el comportamiento del sistema, la actuación y cumplimiento de su gestión informática, la realización correcta de sus objetivos, el cumplimiento de sus funciones, actividades y operaciones, o cualquier otro aspecto de los sistemas computacionales.

Precisamente por estas razones, en las siguientes páginas analizaremos los aspectos más significativos que el auditor debe tomar en cuenta para elaborar un buen informe de auditoría de sistemas. Es indiscutible que este informe debe contar con la suficiente calidad para no demeritar ni minimizar lo ahí presentado. Por esta razón es de suma importancia que el auditor reconozca y aplique el contenido de los puntos que presentamos a continuación.

8.1 Procedimiento para elaborar el informe de auditoría de sistemas computacionales

En el informe de auditoría, también llamado dictamen, se reportan las situaciones encontradas durante la evaluación,* pero también se deben incluir las causas que originan esas situaciones y las posibles sugerencias para solucionar los problemas encontrados.

Sin embargo, la elaboración del informe, el cual es el punto más importante de la auditoría de sistemas, es uno de los aspectos más difíciles para los auditores, debido a que requiere procedimientos complicados, propios de las auditorías, los cuales se tienen que llevar a cabo mediante una secuencia, como la que se propone en la figura 8.1. En ella se describe un ordenamiento general de realización del informe, el cual va desde la aplicación de los instrumentos de recopilación, hasta la presentación del dictamen final a los directivos de la empresa.

Está claro que el producto final y el más importante de una auditoría de sistemas es la elaboración correcta del informe, ya que en éste se presentan los resultados obtenidos durante la evaluación de la gestión administrativa del centro de cómputo, o de cualquier otro aspecto relacionado con los sistemas.

El procedimiento para elaborar dicho informe se compone de los siguientes pasos:

- *Aplicar instrumentos de recopilación*
- *Registrar en el formato de situaciones encontradas las desviaciones halladas durante la revisión*
- *Comentar las situaciones encontradas con los auditados*
- *Encontrar, conjuntamente con los auditados, las causas de las desviaciones y sus posibles soluciones*
- *Analizar, depurar y corregir las desviaciones encontradas*
- *Jerarquizar las desviaciones encontradas y concentrar las más importantes en el formato de situaciones relevantes*
- *Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones*
- *Concentrar, depurar y elaborar el informe final de auditoría, así como el dictamen del auditor*
- *Presentar el informe y dictamen final a los directivos de la empresa*

* En el lenguaje coloquial de auditoría, para elaborar el reporte es muy común que a los asuntos que se informan como resultados de una evaluación se les llame: **situaciones, incidencias, desviaciones** u **observaciones,** términos utilizados para indicar los problemas encontrados durante la revisión, las desviaciones que se aparten de la operación normal o cualesquier otros incidentes que se tenga que reportar. Por esa razón, en este libro se propone estandarizar estos términos por el de situaciones, para referirnos a cualesquier desviaciones, problemáticas, incidencias u observaciones que se tenga que informar. Esto obedece a que no necesariamente el auditor debe reportar sólo las desviaciones e incidencias negativas, sino también cualquier otra situación positiva que favorezca el desarrollo correcto de las actividades. El auditor también debe reportar las cosas buenas que encuentra y los aciertos en la operación.

En forma esquemática, el procedimiento propuesto debe seguir estos pasos:

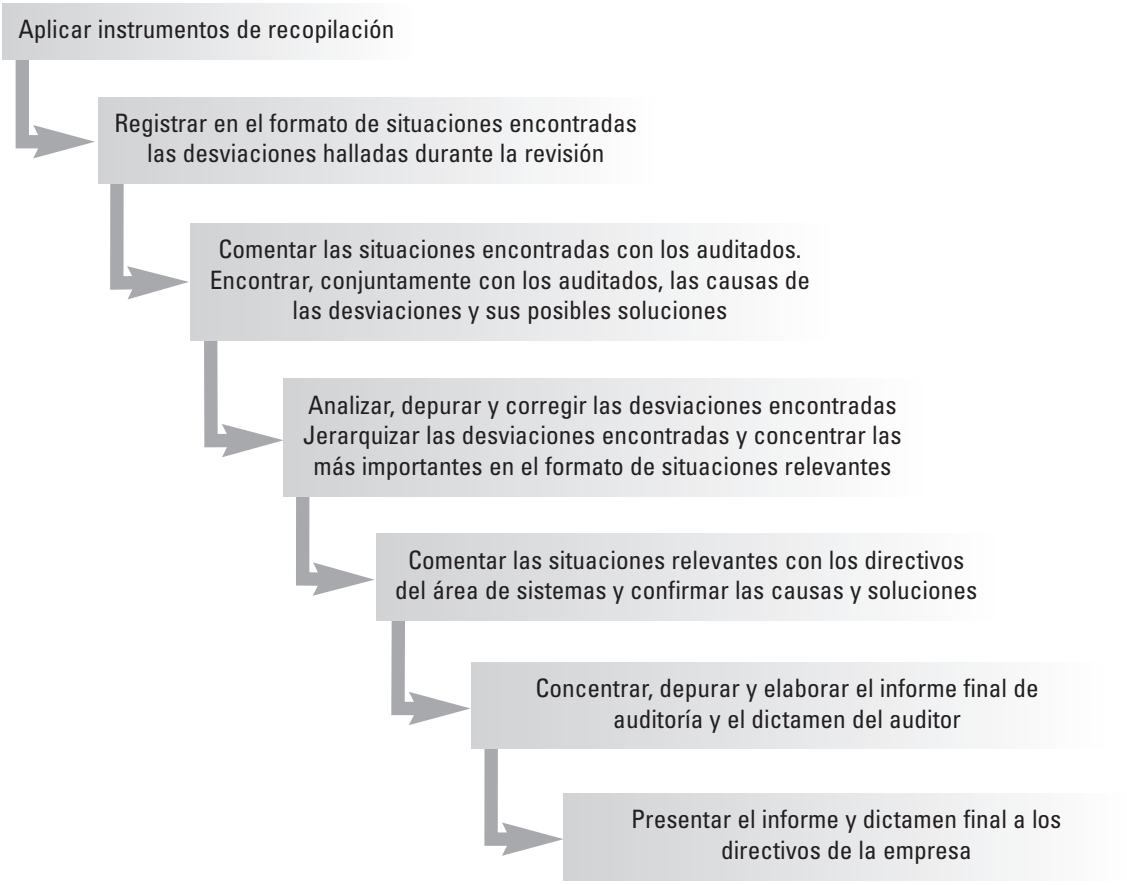


Figura 8.1 *Procedimiento para elaborar el informe de auditoría.*

Para un mejor entendimiento del proceso antes señalado, a continuación realizaremos un breve análisis de cada uno de estos puntos.

8.1.1 Aplicar instrumentos de recopilación

De acuerdo con el programa para la auditoría de sistemas, el auditor aplica los instrumentos, técnicas, procedimientos y herramientas que diseñó en la etapa de planeación,* con el propósito de realizar la evaluación a los sistemas computacionales, a las áreas del centro de cómputo o a cualquier otro aspecto.

* En el capítulo 6 se presenta la planeación de una auditoría.

Con la aplicación de estos instrumentos, el auditor detecta las posibles desviaciones a la actividad que está evaluando y, de acuerdo con sus conocimientos y experiencia, las analiza y las registra, en el formato de situaciones encontradas que analizaremos a continuación.

8.1.2 Registrar en el formato de situaciones encontradas las desviaciones halladas durante la revisión

Con la aplicación de los instrumentos diseñados en la etapa de planeación, el auditor identifica aquellas posibles desviaciones que encontró durante su evaluación, y hace un análisis comparativo de la operación normal contra la esperada. Una vez hecho este análisis, entonces puede definir aquellas situaciones que considera como desviaciones y las reporta como situaciones encontradas en su evaluación.

Las desviaciones que reporta el auditor tienen características especiales, las cuales debe plasmar por escrito en un documento de carácter formal, al que llamaremos *formato de situaciones encontradas.** Además, como requerimiento ineludible, dicho reporte debe estar perfectamente elaborado, en cuanto a su redacción, claridad, oportunidad y a otras características propias de los informes de auditoría que analizaremos en el apartado correspondiente.**

Está claro que la principal función del auditor es reportar todas las desviaciones que observó durante la auditoría de sistemas, para lo cual puede utilizar el formato que más le plazca y de la manera en que se acostumbre reportar dichas observaciones en la empresa en donde se realiza la auditoría; sin embargo, a continuación sugerimos la adopción de un formato muy fácil de elaborar por la simplicidad y sencillez para plasmar esas desviaciones. Éste es el *formato de situaciones encontradas,* el cual contiene las siguientes columnas: las situaciones, las causas, las soluciones, los responsables de la solución y las fechas de solución. En el capítulo anterior mencionamos este formato y lo trataremos más a fondo en la sección 8.4 de este capítulo.

Conviene aclarar que este primer formato de *situaciones encontradas* puede ser elaborado en borrador manuscrito, sujeto a correcciones después de comentarlo con los responsables de la operación del área auditada,*** o se puede mecanografiar, de

* Al realizar la evaluación de sistemas, el auditor encuentra desviaciones a los procedimientos, operaciones, actividades o cualesquier otras tareas normales en el área de sistemas, y esas desviaciones es lo que debe reportar, sin importar que sean sólo una mínima o una muy grande desviación. Sin embargo, no tan sólo se deben reportar las desviaciones, sino también se deben reportar todas aquellas situaciones que sean dignas de comentar, ya sea por una actividad que se está realizando en forma sobresaliente, porque en este momento no es desviación, pero puede llegar a serlo, porque merecen darse a conocer, o por cualesquier otros hechos (no desviaciones) que valga la pena reportar. Además de desviaciones se reportan los resultados, sean buenos o malos.

** En las siguientes secciones de este capítulo analizaremos todo lo que se refiere al informe de la auditoría de sistemas, incluyendo lo relacionado con los formatos de situaciones encontradas y situaciones relevantes.

*** Este primer formato se comenta con los responsables de la operación del área auditada y el siguiente formato de situaciones relevantes (que veremos adelante), con los directivos del área de sistemas.

acuerdo con la experiencia del auditor y con su costumbre de trabajo; esto es irrelevante, lo importante es que se elabore conforme a lo que señalaremos en las siguientes secciones de este capítulo.

8.1.3 Comentar las situaciones encontradas con los auditados

Una vez identificadas las situaciones encontradas, es responsabilidad del encargado de la auditoría que el auditor, o su supervisor (que puede ser el propio responsable de la auditoría), comenten cada una de esas desviaciones con el personal responsable de la operación, sistema o función auditada.

Es indispensable que cada una de estas desviaciones sean discutidas con los empleados, funcionarios o usuarios que fueron auditados, ya que, de alguna manera, éstos son los responsables de que se presenten dichas situaciones (o cuando menos están involucrados en ellas); el propósito de informarles es que ratifiquen o rectifiquen el origen de tales desviaciones; además, también le sirve al auditor para complementar la redacción de las situaciones que reporta; con ello se busca que éstas sean lo más claras posibles y más entendibles, a fin de que se reporten exactamente como se quiere señalar cada desviación.

Además, comentarlas con el auditado le permite preparar las posibles soluciones para esas desviaciones, incluyendo en esto el señalamiento de las posibles causas. En relación con esto, es indispensable recalcar lo siguiente:

> *La auditoría no es una cacería de brujas para cortar las cabezas de los auditados; es una revisión para encontrar posibles desviaciones en su actividad cotidiana y es deber del auditor comentarlas con ellos para resolverlas de común acuerdo.*

8.1.4 Encontrar, conjuntamente con los auditados, las causas de las desviaciones y sus posibles soluciones

Así como señalamos en el punto anterior la necesidad de comentar las desviaciones con los responsables de la operación, también remarcaremos que de estos comentarios se pueden obtener, de manera más fidedigna y confiable, las causas que generan cada una de las desviaciones, a fin de reportarlas en el informe de auditoría lo más apegado posible a la realidad.

Está claro que al conocer las desviaciones que se le imputan, el auditado tratará de defenderse, señalando las causas que originaron cada una de las desviaciones encontradas; con ello el auditor puede corroborar o rectificar las causas que había planteado; además le permite obtener, de manera directa y en voz de los involucrados, las posibles soluciones a estas desviaciones. Incluso hasta el responsable de llevarlas a cabo.

Éste es el verdadero trabajo del auditor, reportar las desviaciones que encontró durante su evaluación, encontrar las causas que las originaron y acordar las posibles so-

luciones conjuntamente con el auditado. *Así es como se entiende y debe entenderse la función de la auditoría de sistemas.*

Cuando se da esta retroalimentación con el personal auditado, de ellos mismos se puede seleccionar a los posibles responsables de la solución y la fecha compromiso en que se puede llegar a solucionar cada una de las desviaciones presentadas.

Es muy conveniente que el auditor obtenga la firma de enterado del auditado al finalizar los comentarios de estas desviaciones, causas, soluciones, responsables de estas soluciones y fechas de solución, aunque esto no es una norma ni un requisito indispensable para su informe. Si el auditado se negara a proporcionar su firma, al auditor no le afectaría en lo más mínimo para hacer su reporte, ya que dicha firma no influye en el resultado de la auditoría.

> *Como profesional de la auditoría, el auditor siempre reporta lo que observa con la aplicación de sus técnicas, herramientas y procedimientos de auditoría y, como parte de su trabajo, lo comenta con el auditado, sin afectarle si éste acepta o rechaza el resultado de su evaluación. Lo que avala el resultado de la auditoría es el informe y los papeles de trabajo, y no la firma del auditado.*

8.1.5 Analizar, depurar y corregir las desviaciones encontradas

Una vez que se comentaron las desviaciones con los auditados, y se obtuvieron sus causas y posibles soluciones, el responsable de la auditoría de sistemas será el encargado de analizar las desviaciones, vigilando que cada una esté perfectamente plasmada y correctamente redactada en el formato de situaciones encontradas. La redacción y presentación de estas desviaciones debe hacerse lo más correctamente posible, sin admitir ni el más mínimo error de ortografía, redacción o tipografía. Ésta es la principal responsabilidad del encargado de la auditoría de sistemas, vigilar el correcto reporte de las situaciones encontradas.

Cada auditor elabora, en borrador o mecanografiadas, las desviaciones que observó durante su evaluación, y al mismo tiempo es el responsable de comentarlas con el personal auditado para obtener de ellos sus causas y soluciones. Una vez que fueron comentadas y en su caso corroboradas o rectificadas, entonces entrega el informe al responsable de la auditoría, quien será el encargado de analizar cada una de estas desviaciones, a fin de redactarlas mejor, concentrarlas y darles una estructura jerárquica de presentación en un informe global de situaciones relevantes encontradas durante la evaluación de los sistemas.

8.1.6 Jerarquizar las desviaciones encontradas y concentrar las más importantes en el formato de situaciones relevantes

Una vez que el responsable de la auditoría de sistemas haya supervisado que el informe de desviaciones encontradas esté correctamente elaborado, debe analizar todas

las desviaciones reportadas, a fin de escoger las que considere más importantes para reportarlas en el formato de situaciones relevantes;* el propósito es enfatizar lo que considera como lo más importante de la evaluación practicada, a fin de que los directivos conozcan los aspectos más relevantes.

Las situaciones que se reportan como las más relevantes se deben redactar tal y como fueron reportadas en el formato de situaciones encontradas (*se sugiere que siempre sea así*), sin modificarlas (es propiamente una copia fiel de éstas). Esto es lo más conveniente para evitar confusiones de interpretación y errores mecanográficos o cualquier otra alteración de lo que se desea reportar como relevante. Además, así se corrobora que las desviaciones fueron comentadas con el personal auditado. Con esto no habrá lugar para ninguna mala interpretación ni evasión de responsabilidades cuando el informe de situaciones relevantes sea comentado con los directivos del área de sistemas; además, será más fácil mecanografiar dicho informe.

8.1.7 Comentar las situaciones relevantes con los directivos del área de sistemas y confirmar las causas y soluciones

Así como las situaciones encontradas se comentaron con los auditados, también las situaciones relevantes se deben comentar con los directivos del área de sistemas, a fin de que éstos las conozcan; el personal auditado puede, a juicio de los directivos, estar presente para cualquier posible aclaración sobre lo informado. Esto es lo más recomendable.

El responsable de la auditoría debe encabezar la presentación de este informe al directivo de mayor jerarquía del área de sistemas. Por lo general, esta reunión es de carácter formal y en ella se reportan todas y cada una de las situaciones consideradas como relevantes; aunque también se pueden presentar las llamadas situaciones encontradas. Además, si el encargado de la auditoría lo considera pertinente, cada auditor puede presentar el informe de la parte que le tocó evaluar, o puede hacerlo una sola persona en representación del responsable de la evaluación. Todo se hace de acuerdo con el estilo y costumbre de realizar estas presentaciones.

También es decisión del encargado que cada auditor aclare las dudas de los participantes en esta reunión.

En esta reunión se presentan los resultados obtenidos en la auditoría de sistemas computacionales, y el informe a los directivos del área auditada se debe hacer en forma abierta y preferentemente en presencia de todo el personal auditado; esto obedece a que aún podría ser posible aclarar, ratificar o rectificar las desviaciones reportadas, así como sus causas y soluciones. Aunque esto no es muy usual, ya que se debe tomar en cuenta que las problemáticas, situaciones, incidencias, desviaciones u observaciones encontradas durante la auditoría y reportadas en el formato de situaciones relevantes, ya fueron comentadas con cada uno de los auditados.

* Este formato también será analizado en la sección 8.4, y se mencionarán las características e importancia de este formato.

No obstante, como es natural, en estas reuniones muchos de los auditados tratarán de evadir o justificar su responsabilidad en las desviaciones e incluso, en algunos casos extremos, pueden hasta negar la existencia o conocimiento de la situación que se les imputa.

Recordemos que este personal está ante su jefe y difícilmente aceptará sus errores públicamente.

Como resultado de esta reunión, se pueden elaborar las modificaciones que cada caso requiera y, de ser necesario, se puede convocar a una nueva reunión para presentar las situaciones relevantes, pero no para comentar con los auditados las situaciones encontradas como se indica en el punto 8.1.3.

8.1.8 Concentrar, depurar y elaborar el informe final de auditoría y el dictamen del auditor

El siguiente paso es que el auditor responsable de la auditoría depure cada una de las situaciones relevantes reportadas, con el fin de concentrarlas en el llamado informe final de auditoría. Debido a que el informe es para el área directiva de la empresa, no debe exceder de dos a tres hojas. En este informe el auditor sólo debe señalar lo más relevante de la evaluación, incluyendo su opinión.*

La elaboración del informe es el verdadero trabajo del responsable de la auditoría, debido a que en este documento es donde realmente se muestra la importancia de su actividad, al señalar en qué situación estaba el área de sistemas antes de la evaluación practicada por los auditores a su cargo; además, debe emitir una opinión autorizada sobre el funcionamiento del centro de cómputo, sus sistemas de información, el cumplimiento del personal y usuarios o sobre cualquier otro aspecto relacionado con los sistemas computacionales de la empresa auditada.

Debemos aclarar que la razón de plasmar este informe en tan poco espacio es que los directivos de una empresa, por lo general, tienen poco conocimiento del lenguaje que se maneja en los sistemas de la institución; por lo tanto, el informe final debe ser lo más sencillo, claro y comprensible para ellos, procurando evitar, al máximo posible, el uso de términos demasiado técnicos y desconocidos para personas ajenas a la informática. Sólo se deben destacar los aspectos más importantes del área, desde el punto de vista de los directivos y no del personal que maneja los sistemas.

Cabe señalar un ejemplo de esto: *a un director general poco o nada le va a interesar que la red esté configurada en forma de estrella, con cable de par trenzado, en Frame Relay y una de las siete capas OSI no cumpla con su función, y que por eso tenga caídas constantes cuando exista saturación de transmisión y procesamiento de datos en horas pico de transmisión y procesamiento de datos*; este directivo no lo va a entender, ya que sólo le interesará saber cómo se solucionaron los problemas de emisión de información, y si la solución es oportuna y confiable.

* En el apartado relacionado con el informe de auditoría (inciso 8.3), se hacen las aclaraciones pertinentes al porqué de esta regla del informe y a la forma de elaborarlo.

8.1.9 Presentar el informe y dictamen final a los directivos de la empresa

El último paso del informe de auditoría de sistemas computacionales es la presentación oficial del dictamen (informe final de la auditoría), lo cual se puede hacer de dos maneras, ya sea en forma directa, mediante una reunión ejecutiva con los directivos de la empresa, o por envío formal del dictamen final de la auditoría al directivo mayor de la firma. Éste ya es el informe final de la auditoría practicada y, por lo tanto, no se debe admitir ningún comentario adicional que pudiera modificar lo ahí presentado; ya que es el producto final de la auditoría y, por lo tanto, ya no cabe ninguna alteración al mismo. De hacerlo, sería tanto como crear expectativas de duda sobre la veracidad y confiabilidad de su contenido.

Por lo general, a esta presentación solamente asisten el cuerpo directivo de la empresa auditada y el cuerpo ejecutivo de la empresa encargada de realizar la auditoría; aunque nada impide que estén presentes tanto el personal del área de sistemas auditada, como los auditores participantes. En el caso de una auditoría interna, sólo asisten el auditor interno y su cuerpo ejecutivo.

8.2 Características del informe de auditoría de sistemas computacionales

En la redacción del informe, el auditor señala los resultados de su investigación, sus evaluaciones, hallazgos, aportaciones y conclusiones sobre el trabajo realizado; también señala las técnicas, herramientas, métodos y procedimientos que utilizó en la obtención de datos, las observaciones, interpretaciones de los fenómenos y hechos evaluados que le sirvieron de sustento en la elaboración del documento de situaciones encontradas o relevantes que informa, así como todas las demás aportaciones con las cuales da su sello personal al informe presentado.

Evidentemente, el informe de una auditoría de sistemas computacionales es producto de la experiencia y conocimientos del auditor que lo presenta; por esta razón, además de servir para señalar las observaciones, desviaciones y resultados encontrados, este documento también sirve para que el auditor exhiba los conocimientos, técnicas y procedimientos que utilizó para evaluar el área de sistemas; asimismo, en su redacción muestra su forma de ser y de actuar profesionalmente, así como su cultura. De hecho, esto también se juzga en la presentación del informe de auditoría; no sólo el resultado, sino *quién y cómo lo presenta*. Por eso es muy importante conocer las características fundamentales de la elaboración del informe de auditoría.

Para contribuir a incrementar la calidad en la presentación del informe de auditoría, misma que se puede hacer extensiva a cualquier otro tipo de trabajos profesionales, e incluso personales o escolares, a continuación presentamos algunas de las principales características de la redacción del informe de auditoría, las cuales ayudarán al auditor de sistemas computacionales a mejorar su elaboración.

8.2.1 Características fundamentales

Inicialmente, se pueden identificar dos características fundamentales en los informes de auditoría de sistemas computacionales, las cuales siempre se refieren al contenido del informe y a la forma de presentarlo; dichas características son las siguientes:

8.2.1.1 Características de fondo

Estas características se refieren al cuidado que debe tener el auditor de sistemas al revisar que el contenido total del dictamen de auditoría sea acorde con lo que realmente tiene que señalar acerca de la revisión efectuada, refiriéndose exclusivamente al contenido del informe; para ello debe tomar en cuenta los siguientes aspectos:

- *Que la información que contiene el documento sea veraz, confiable y oportuna, y sin distorsiones ni tendencias que demeriten el trabajo realizado.*
- *Que el uso de la terminología sea exacto y objetivo, para que se entiendan e interpreten las desviaciones reportadas tal y como se quisieron plasmar.*
- *Que el contenido del informe sea congruente con lo observado, sin inventar, distorsionar o modificar lo encontrado en la evaluación.*
- *Que permita mostrar, con su simple lectura, la situación real del área auditada, a fin de identificar y solucionar la problemática señalada.*
- *Que su contenido abarque todo lo que se debe informar del área auditada, sin abundar en explicaciones inútiles, pero sin ser parco en lo que se presenta.*
- *Que el lector capte inmediatamente la problemática que reporta el auditor, así como la opinión que plasma respecto al funcionamiento del área de sistemas o de los sistemas auditados.*

8.2.1.2 Características de forma

Estas características se refieren a la manera en que el auditor debe presentar el informe, en cuanto al estilo de redacción, el contenido en partes, apartados, apéndices, tipo y tamaño de las hojas y el tipo de letra; también en lo relativo a la forma de utilizar la redacción, ortografía, sintaxis, gramática y demás componentes del lenguaje, y en sí de todo lo relacionado con la presentación del documento. Al redactar dicho informe, el auditor debe considerar los siguientes aspectos:

- *Que esté redactado en forma concisa, clara, sencilla y amena, sin exceso de tecnicismos, pero sin omitirlos cuando sean necesarios, a fin de que su lectura sea comprensible.*
- *Que al redactarlo se eviten la redundancia, repeticiones y reiteraciones inútiles que sólo abultan y entorpecen la lectura.*
- *Que la forma de presentar el informe sea profesional, mecanografiado en forma impecable y con el contenido exacto que debe tener este tipo de documentos.*

- *Que su redacción sea impecable en cuanto a ortografía y puntuación, en estilo impersonal y sin ningún error en la forma de presentarlo.*
- *Que el contenido sea acorde a las necesidades y exigencias de la empresa auditora, pero también conforme lo requiera la institución auditada.*

Las características anteriores son sólo algunas de las muchas que se pueden considerar para elaborar un buen informe de auditoría de sistemas computacionales; ya que, invariablemente se deben tomar en cuenta las características de fondo y de forma para su redacción. Sería incorrecto utilizar sólo una de ellas.

No se pueden utilizar sólo características de fondo (*contenido impecable*) en un informe de auditoría, pues adolecería de una buena presentación, pero tampoco se pueden utilizar sólo características de forma (*presentación impecable*), pues carecería de contenido real.

8.2.2 Características de la presentación del informe

Otras de las características más importantes de un informe de auditoría de sistemas computacionales son los atributos que deben tener la redacción y la presentación del informe; para lograr mejores resultados en la elaboración del citado informe, el auditor debe tomar en cuenta las características que proponemos a continuación:

Claridad	*Exactitud*
Confiabilidad	*Imparcialidad*
Propiedad	*Objetividad*
Concisión	*Congruencia*
Sencillez	*Familiaridad*
Acertividad	*Veracidad*
Ilación	*Efectividad*
Tono y fuerza	*Positividad*
Oportunidad	*Sintaxis*
Precisión	

Como parte de este punto, a continuación analizaremos cada una de estas características.

8.2.2.1 Claridad

Para el informe de auditoría, esta característica es *la clara expresión de las ideas y conceptos, de tal manera que se facilite la lectura, ya sea del dictamen, de una situación, una causa o una solución, de todo el informe, de un texto o de cualquier documento que integre el informe. Para lograr esto, es necesario redactar el informe con líneas sen-*

cillas, bien redactadas, conceptos claros y de fácil lectura para que el lector capte los juicios e ideas tal y como se quisieron expresar, cosa que a veces no es tan sencilla.

Está claro que la responsabilidad del encargado de la auditoría es vigilar que al elaborar el informe se cumpla con esta característica de la redacción; para lograr esto, es conveniente que el auditor considere los siguientes puntos:

Ordenar las ideas y conceptos en forma lógica y sencilla, conforme a un método claro y secuencial para cada uno de los puntos que se tienen que redactar, dando el mismo tratamiento a los demás puntos.

Anotar las ideas una sola vez, en forma clara y sencilla, evitando el exceso de aclaraciones y explicaciones inútiles, las cuales sólo entorpecen las ideas fundamentales. Además, evitar el uso de conceptos irrelevantes y reiterativos que sólo hacen que el lector se aleje del tema central.

Suprimir cualquier tipo de acotaciones de ideas que no vengan al caso, tales como aclaraciones entre paréntesis, corchetes o guiones, las cuales hacen que el lector del informe se salga del tema central; se debe hacer lo mismo con los temas que sean ajenos a la redacción del punto que se trate, ya que sólo enredan los conceptos.

Evitar el uso de términos ambiguos, cantinflescos[1] *y domingueros,*[2] *así como de frases redundantes, repetitivas y superfluas que sólo abultan el informe y entorpecen la lectura.*

Redactar en párrafos sencillos, claros y concretos, que contengan sólo las ideas fundamentales y los conceptos que expresen la observación que se pretende mostrar, a fin de hacer más ágil y menos engorrosa la lectura.

Utilizar un lenguaje conocido, coloquial y entendible para quien lo va a leer, evitando usar vocablos demasiado técnicos, rimbombantes, o términos de los que desconocemos su cabal significado. Es más elegante el lenguaje que se entiende y comprende sin dificultades.*

Evitar siempre iniciar cada desviación o párrafo del dictamen con frases negativas como No se encontró, No se tiene, No existe, Se carece de, No se puede, y demás frases similares. Esto crea aversión hacia la lectura del informe; por esta razón es preferible utilizar otro tipo de vocablos o suavizar lo negativo de la frase, principalmente al inicio de ésta.

Al recomendar una redacción con claridad, se busca que el auditor exprese sus ideas de manera sencilla, legible y entendible para quien leerá el informe; si dicho informe tiene algún tipo de fallas de redacción, quien lo va a leer por lo general fingirá no entenderlo; Ésta puede ser una salida que busca el auditado, a fin de evidenciar deficiencias o carencias en el auditor que presenta el informe de auditoría, para restarle

* En el ambiente de sistemas computacionales es muy común utilizar términos que solamente entienden los involucrados en dicho ambiente; sin embargo, el informe final de la auditoría de sistemas está dirigido, por lo general, a los directivos de alto nivel de una empresa, los cuales pocas veces entenderán cabalmente estos tecnicismos. Por esta razón, debemos redactar el informe en forma sencilla, con lenguaje coloquial y lo más entendible que podamos, evitando el abuso de estos tecnicismos informáticos.

credibilidad a lo que reporta. Cuando hay deficiencias de redacción, se pueden minimizar los resultados de la evaluación.

Recordemos que en el ambiente de trabajo no es muy fácil aceptar que nos digan nuestros errores y menos públicamente; así pues, un informe de auditoría se puede entender como un señalamiento público de errores detectados durante una evaluación. Está claro que ante una lectura incomprensible, el afectado fingirá no entender para así minimizar el peso de la evaluación.

8.2.2.2 Confiabilidad

Entendida como "La calidad de lo confiable. Fiabilidad"; de **Confianza***:* "Actitud de quien se fía y confía en alguien o algo. Seguridad que uno tiene en sí mismo y que puede derivarse en presunción [...]" y **Confiable**: "Se dice de la persona o cosa en que se puede confiar".[3] Para el caso del informe de auditoría de sistemas, esta característica se puede entender de la siguiente manera:

> *La calidad de la confianza que se le da a la información que reporta el auditor, derivada de las pruebas e instrumentos que aplica en la evaluación del área, sistema o actividad informática de una empresa, al confiar en que invariablemente reporta las deficiencias de las operaciones mediante un dictamen sobre el comportamiento de éstas.*

Ésta es una de las características más importantes del informe de auditoría, debido a que, cuando el auditor emite su opinión en un reporte, tanto el lector como los auditados confían en que este profesional haya aplicado todos sus conocimientos, experiencias y buen juicio para evaluar el funcionamiento de los sistemas de la empresa, así como su buen juicio para emitir una opinión al respecto, y aceptando que sus observaciones están bien analizadas y cimentadas con pruebas y procedimientos profesionales.

La plena confianza de que el auditor reporta lo que observa sin omitir datos importantes ni agregar información de más, y de que su actuación es totalmente imparcial, sin favoritismos, sesgos, distorsiones o arreglos indebidos, es lo que le da credibilidad a su actividad profesional.

Está claro que la certidumbre en la profesión de auditor se logra con esfuerzo continuo, profesionalismo en la forma de actuar, calidad en el trabajo y una total y absoluta honradez en lo que se informa acerca de las evaluaciones que se realizan.

La confianza que se deposita en la disciplina de auditoría se debe a que el auditor aplica técnicas, métodos, procedimientos y herramientas específicas para evaluar y emitir un dictamen acerca de las actividades y operaciones de una empresa o área de sistemas, la eficiencia de un sistema computacional o la confiabilidad y veracidad del uso de los recursos de una empresa, entre otros casos.

Es evidente que la base fundamental para reportar y aceptar los resultados de una auditoría es la confiabilidad; sin embargo, el auditor debe cultivar diariamente esta característica tan importante, a través de la correcta presentación de los reportes de una

evaluación, así como de una adecuada aplicación de las herramientas y procedimientos de auditoría, y del cabal cumplimiento de las normas y criterios de conducta señalados en el capítulo 3 de este libro.

> *Para el auditor es muy difícil ganar la confianza de los auditados, es todavía más difícil conservarla y puede ser muy fácil perderla por incompetencia, deshonestidad, falta de capacidad y muchas otras causas imputables al auditor poco profesional.*

8.2.2.3 Propiedad

La propiedad en la redacción de los informes de auditoría es *el uso correcto de las palabras, construyendo las frases conforme a las reglas gramaticales, empleando sólo los vocablos adecuados de acuerdo con el significado exacto de las palabras, y utilizando la escritura y pronunciación, según el sentido que se le quiere dar a la expresión empleada*.

Este estilo de redacción exige un elevado dominio del lenguaje, así como del significado y sentido de las palabras, además del uso correcto de los sinónimos, antónimos y homónimos, evitando con ello el manejo inadecuado de expresiones equivocadas, pomposas y demasiado técnicas que sólo le quitan valor y estética al informe.

Existen auditores que tienen vicios muy marcados en la elaboración de los informes de auditoría de sistemas, quienes suelen utilizar palabras inadecuadas, o vocablos que más o menos se parecen a lo que quieren expresar, pero cuyo significado desconocen o utilizan mal en el reporte; asimismo, existen quienes abusan de expresiones demasiado técnicas para aparentar una cultura informática y utilizan lenguajes que a veces el lector no entiende o desconoce su cabal significado. También se sabe de auditores cuyo lenguaje es muy limitado y deficiente y usan un número muy reducido de vocablos; aunque también pasa lo contrario, hay auditores que en su afán de aparentar ser poseedores de una elevada cultura, utilizan vocablos supuestamente elegantes y rimbombantes, con los cuales sólo muestran un gran desconocimiento y pobreza en el uso del lenguaje.

Dentro de todas estas deficiencias tenemos *la pobreza del lenguaje, el uso incorrecto de superlativos y diminutivos, el abuso de gerundios, el desconocimiento de las reglas de sintaxis, las faltas de ortografía y otras deficiencias similares en la redacción*.

Es obvio que existen muchos vicios en la elaboración de informes, no sólo en el ámbito de la auditoría, sino muchos otros, debido a que las palabras se utilizan inapropiadamente al redactar dichos informes. Por esta razón es importante analizar esta característica.

Redactar apropiadamente un informe de auditoría de sistemas significa elaborarlo con frases correctas, acordes a lo que se quiere argumentar, sin repeticiones, redundancias o reafirmaciones inútiles que sólo entorpecen la lectura y la hacen muy densa y sumamente cansada. De por sí un informe de auditoría no es muy bien recibido, y si no se redacta apropiadamente, su lectura se hace engorrosa y aburrida; además puede provocar tensión en una reunión, y más en el área de sistemas.

Un buen consejo que los supervisores de auditorías pueden dar a un auditor principiante es que, al redactar su informe, anote sólo lo estrictamente necesario, eliminando lo que esté de más, como frases repetitivas, redundantes o reiterativas. Se tienen que evitar las *tres erres: Repetitivo, Redundante y Reiterativo,* aunque tampoco se debe abusar de la cortedad del texto, ni hacer mal uso del lenguaje.

Además, también es útil aconsejarle al auditor principiante que se apegue a una de las reglas básicas al empezar a redactar su informe: *evitar frases o palabras redundantes que sólo indican la pobreza del lenguaje de quien redacta el documento, a la vez que hacen muy cansada su lectura*.

8.2.2.4 Concisión

Esta característica de la redacción del informe de auditoría *consiste en expresar los pensamientos, ideas y conceptos con el menor número de palabras, sin que por ello se le reste claridad ni precisión al contenido de dicho informe*.

Se puede decir que un informe de auditoría es conciso cuando al redactarlo se expresa su contenido total con claridad, sencillez y precisión, utilizando sólo las palabras y expresiones que sean acordes a lo que se quiere decir. Sólo las palabras necesarias para expresar el mensaje que se quiere reportar.

Conciso significa expresar el contenido en pocas palabras, pero no por ello se debe limitar su número. Conciso no quiere decir resumido, sino el uso de términos concretos, breves y precisos al expresar lo que se quiere decir de la evaluación practicada en el área de sistemas.

Evidentemente no es fácil redactar un informe de auditoría conciso; la mayoría preferimos irnos por el camino fácil de utilizar argumentación excesiva, con abundante verborrea y más palabras de las necesarias, ya que es menos problemático y evidencia menos nuestras deficiencias de lenguaje. Sin embargo, tampoco se debe abusar de la cortedad del informe, ni hacer un resumen del resultado de la auditoría. Se debe reportar exactamente, en pocas palabras y de manera precisa, lo que se observó durante la evaluación.

Es recomendable que, para poder hacer un reporte conciso, el auditor elabore borradores del informe, primero muy extensos, tal como los siente y sin ninguna restricción, y que después vaya eliminando los conceptos inútiles hasta simplificar el informe, de tal manera que escriba únicamente lo esencial de lo que quiere reportar.

Comentar el primer borrador del informe con los auditados ayudará al auditor a reducir las expresiones inútiles y a redactar dicho informe de manera concisa. Además, esto le ayudará, como ya señalamos, a ratificar, rectificar o modificar las observaciones que está reportando.

8.2.2.5 Sencillez

La sencillez en la redacción del informe estriba en expresar con naturalidad las ideas, los conceptos, hechos y observaciones sin utilizar adornos excesivos, rebuscamientos

ni tecnicismos inútiles para mostrar, supuestamente, mayor cultura; es decir, utilizar el lenguaje con franca espontaneidad, así como frases y palabras simples.

La sencillez en la redacción del informe se puede entender como el uso de un lenguaje coloquial, como si el auditor estuviera platicando lo que reporta o como si estuviera dictando una conferencia; con un lenguaje muy simple y sencillo, sin adornos ni rebuscamientos inútiles y estériles que sólo entorpecen el entendimiento del texto. La mejor forma de redactar el informe es hacerlo como si se expresara en forma de plática. De ahí la importancia de comentarlo con los auditados; si el informe se entiende en forma sencilla, entonces está correcto.

En el medio de la auditoría de sistemas es frecuente observar que muchos auditores utilizan vocablos inútiles, a veces demasiado técnicos, para presentar el informe de la auditoría, y cuando alguien les pide una breve explicación de su contenido, entonces sí lo expresan con suma sencillez. Si estos auditores entendieran que deben redactar su informe con la sencillez con que lo platican, las presentaciones de sus informes serían excelentes. Aunque esta deficiencia en la redacción también se da en los escritos políticos, laborales e incluso en muchos escritos académicos.

A continuación presentamos algunos consejos que pueden ayudar al auditor a redactar de manera sencilla un informe de auditoría de sistemas:

- *Evitar, al redactar el informe final, el uso de frases y palabras rebuscadas y sofisticadas cuyo significado se desconozca.*
- *Utilizar un lenguaje moderno, con términos actuales y propios para el entendimiento del tema.*
- *Eliminar las expresiones elevadas que supuestamente demuestran mayor cultura, cuyo significado real muchas veces se desconoce, y que sólo desvían al lector del tema central y ridiculizan el texto.*
- *Eliminar los tecnicismos innecesarios, pero no por ello limitar su uso, sino utilizar en forma adecuada los que se requieran, de acuerdo con lo que se quiere decir, a lo que demande el área involucrada o al nivel de conocimientos del lector del informe.*
- *Eliminar las palabras extranjeras que tienen un equivalente en castellano, siempre y cuando no se entorpezca ni se limite lo que se quiere plasmar en el texto.*
- *Evitar traducir al español los términos informáticos en inglés cuyo uso se haya popularizado en los ambientes de sistemas, ya que todos los usuarios los entienden.*
- *Utilizar adecuadamente la puntuación, acentuación y ortografía conforme a las reglas gramaticales. Manejándolas con suma precisión.*

8.2.2.6 Acertividad

Se dice que alguien es oportuno cuando dice o hace lo necesario, justo en el momento que se requiere, aunque no necesariamente esto sea lo más adecuado.

Se dice que alguien es acertivo cuando dice o hace lo adecuado en el momento oportuno y con ello acierta a lo que se está tratando; pero además, con esto se benefician tanto el que lo escucha como el que lo expresa. Lo mismo se dice para quien así actúa en el trabajo, en la escuela, en el hogar o en cualquier otro lado.*

Ésta precisamente es una gran cualidad de la redacción, decir en el momento justo, más bien escribir, la frase o palabra que el lector espera que se diga, exactamente en ese momento que se requiere, ni antes porque no se entendería ni después porque ya no tendría caso. Utilizando para ello las palabras adecuadas, exactas y con el significado preciso y claro a lo que se quiere indicar.[4]

La oportunidad es una de las cualidades más apreciadas de un informe de auditoría, aunque muchas veces esa llamada oportunidad se exprese con términos no muy adecuados, agradables ni exactos a lo que se informa, aunque éstos se usen cuando se tienen que usar y cuando vienen al caso. Éste es uno de los aspectos más importantes a la hora de redactar un informe; si el auditor expresa sus conceptos con oportunidad, entonces estará redactando correctamente las desviaciones que reporta. Mucho mejor si lo hace acertivamente.

La acertividad en la redacción de un informe de auditoría *consiste en que, además de expresar sus conceptos oportunamente, el auditor también los expresa con acierto y un beneficio adicional al esperado, favoreciendo el entendimiento de quien leerá el reporte. Es decir, no sólo debe escribir lo esperado en el momento oportuno y necesario, sino que también debe escribirlo con un beneficio para el lector.*

8.2.2.7 Ilación

El vocablo **ilación***, "*del latín ***illatio–onis****,* de ***inferre:*** Llevar, razonar. Deducción, inferencia."[5] "Acción o efecto de inferir una cosa de otra. Nexo lógico entre el consiguiente y las premisas. Conexión razonada entre varias ideas y un discurso.*"*[6] Se refiere a la forma en que el auditor relaciona las pruebas y procedimientos de auditoría que utiliza en su evaluación, para llegar a conclusiones específicas respecto a lo que reporta de la auditoría.

Antes de continuar, conviene aclarar las expresiones utilizadas en las definiciones anteriores:

Consiguiente

*"*Que depende y se deduce de otra cosa. En una proposición de dos términos, el segundo (consecuente), siendo el primero o premisa el antecedente.
Por consiguiente*.* Expresión consecutiva con que se señala una deducción lógica, algo que se desprende de lo dicho antes".[7]

* El vocablo acertivo, de reciente año, se deriva de acertar "atinar, dar en el blanco [...] adivinar por intuición. Hacer algo con acierto [...] opcit. Gran diccionario del Saber... pág. 16. Por esa razón se utiliza esta característica de la redacción en este sentido. El vocablo difiere de asertivo "afirmativo, que contiene una frase o una aserción" Idem. pág. 174.

Premisa

"[...] Que precede. Cada una de las proposiciones del silogismo de las que se saca una conclusión. Por extensión, base de la argumentación, discusión, etcétera."[8]

Inferir

"Conjeturar, sacar consecuencias. Llevar consigo, ocasionar, conducir a un resultado [...]."[9]

Con el solo análisis de estas definiciones bastaría para entender esta característica para la elaboración de los informes de auditoría de sistemas; sin embargo, *conviene establecer que a partir de pruebas y procedimientos para la evaluación, el auditor infiere el comportamiento de los sistemas o el cumplimiento de las actividades y operaciones del centro de cómputo, lo cual le ayuda a determinar las posibles anomalías de su operación normal, para marcarlas como desviaciones.*

Está claro que al elaborar el informe, el responsable de la auditoría será el encargado de analizar los papeles de trabajo, para hacer un estudio a conciencia de lo reportado y, a partir de deducciones lógicas, construir parámetros de evaluación que le permitan comparar cómo debería funcionar lo que está auditando y cómo funciona en realidad. A partir de ese análisis puede hacer observaciones y plasmarlas en su informe, reportándolas como desviaciones de la operación normal de lo que está auditando.

Precisamente en eso consiste el informe de auditoría, a partir de la aplicación de los métodos, técnicas, procedimientos y herramientas de auditoría, el auditor infiere el cumplimiento adecuado de la operación normal de los propios sistemas, de las actividades del área de sistemas o de cualquier otro aspecto informático que esté auditando; esto le lleva a deducir posibles desviaciones en la operación normal, y a señalarlas en el llamado informe de auditoría. Es decir, el auditor aplica esta característica de ilación, como parte sustantiva en la elaboración del informe; aunque muchas veces lo haga en forma intuitiva.

8.2.2.8 Tono y fuerza

La forma de redactar, la intensidad que se le da al escrito y la profundidad con la que se expresan los términos plasmados en un informe de auditoría, es lo que se conoce como tono y fuerza del escrito. Es decir, es la fuerza que el auditor le da a lo que está reportando, a fin de que se entienda lo que quiere expresar, justo en el tono que les quiere dar a los términos utilizados y con la fortaleza que quiere destacar.

En un informe de auditoría se pueden utilizar diversos tonos, desde los muy tenues y cálidos, otros demasiado fuertes y acalorados, algunos más tibios y temerosos, y en sí toda una gama de estilos muy distintos. Sin embargo, esta característica debe entenderse como los tonos y fortaleza con los cuales se expresarán las situaciones de los sistemas de una empresa.

Evidentemente, la forma de expresar las ideas en un reporte de auditoría muestra el estilo personal de redactar del responsable de la auditoría; esto sólo se identificará

de acuerdo con la fuerza que le dé al reporte y al tono con que maneje los conceptos y aportaciones que exprese con su dictamen de la auditoría. De paso, con ello se muestra parte de la personalidad del auditor en jefe y del grupo de auditores que realizaron la evaluación y, en algunos casos, también se muestran sus conocimientos sobre la auditoría de sistemas.

Estas características de la redacción no se aprenden en escuelas y difícilmente se pueden enseñar, debido a que la mayoría de los tipos de tono y fuerza que se les da a estos escritos se hace de acuerdo con las características y personalidad del redactor. Quizá la única forma de obtener el tono y la fuerza deseados se logre por medio de las influencias recibidas de lo que se lee en diversos informes y de las experiencias acumuladas en la elaboración de estos informes. Independientemente del carácter personal del escritor del informe.

8.2.2.9 Oportunidad

Si se tuvieran que jerarquizar las características del informe de auditoría, la oportunidad en su presentación sería quizá la más importante o de las más trascendentales para el auditor y el auditado. Es obvio que la importancia del informe será de acuerdo con la puntualidad y conveniencia con la cual se presente, ya que así se facilitará conocer las desviaciones de la operación normal para que se tomen las medidas necesarias para su solución. Si esto no se cumple, no tendría caso presentar un informe.

La oportunidad consiste precisamente en presentar a tiempo las desviaciones que fueron observadas, a fin de corregirlas de inmediato y de tomar las medidas necesarias para que no vuelvan a ocurrir. Por ejemplo, no tendría caso expresar la sospecha de sustracción del equipo y componentes del área de sistemas un año después de que esto esté ocurriendo, puesto que tal vez ya haya desaparecido todo el equipo y, por consiguiente, sería inoportuno tomar cualquier medida para evitarlo.

La esencia de la auditoría de sistemas es reportar lo que se observa durante una evaluación, a fin de que los directivos sepan cómo está funcionando la operación de los sistemas y cómo se están utilizando los recursos asignados a esta área. Pero dicho reporte debe ser hecho a tiempo y formalmente, de tal manera que al conocer las desviaciones observadas por el auditor, los directivos puedan tomar las medidas pertinentes para solucionarlas y evitar que se presenten en el futuro.

En el caso de auditorías de sistemas computacionales, oportunidad también quiere decir entregar y comentar a tiempo los resultados de la evaluación practicada: tanto la elaboración del borrador y los comentarios con los auditados, la elaboración de los reportes de situaciones encontradas y situaciones relevantes, como su presentación a los directivos del área de sistemas y la entrega del informe final a los directivos de la empresa.

8.2.2.10 Precisión

Esta característica *consiste en redactar el informe utilizando sólo conceptos completos, sin agregar datos innecesarios, pero sin omitir ninguna información que se consi-*

dere importante. Redactar con precisión significa redactar únicamente con las ideas y conceptos necesarios, sin redundancias, pero sin abusar de la brevedad de las ideas. Además, sólo se deben utilizar aquellos conceptos acordes a lo que se quiere decir; de esta manera se logra el entendimiento de lo que se quiere informar y se evitan ambigüedades y frases de más.

Se dice que una situación es precisa cuando expresa con exactitud el asunto que se está reportando; sin rebuscamientos inútiles ni información innecesaria, pero sin omisión de conceptos y datos importantes. Únicamente expresa lo necesario, con las frases y conceptos adecuados.

Adoptar un estilo sobrio y preciso no es camino fácil, ya que dentro del medio profesional de la auditoría, en el de la política empresarial e incluso en el ambiente laboral, es muy frecuente que al redactar informes y comunicados se abuse del lenguaje, exagerando a veces en el uso de frases trilladas, abundantes y que muchas veces no dicen nada y sólo engrosan el escrito. Aunque también hay informes que sólo expresan lo indispensable, redactados muy parcamente para no comprometer al redactor con lo escrito. Ambos estilos son parte de la forma de ser del ambiente de trabajo, pero se dan mucho más en los sectores gubernamental y político.

Este estilo de redacción es muy socorrido por los auditores novatos y los ***rolleros***[10] que están acostumbrados, por ignorancia o por vicio, a presentar sus informes con estas deficiencias. Existen auditores que utilizan datos e información inútiles que sólo sirven para aumentar el volumen de su informe; pero también existen auditores que presuponen que los lectores del informe ya conocen muchos aspectos de sistemas que sólo ellos comprenden, que dan por obvios y no los reportan; con ello sólo limitan la información de los resultados de la auditoría. Es evidente que en ambos casos se entorpece el entendimiento del informe de auditoría.

> Un buen informe de auditoría de sistemas computacionales debe contener sólo la información precisa, sin exceso de datos, pero sin falta de información.

A fin de ayudar al auditor a redactar mejor su informe de auditoría, a continuación presentaremos algunas preguntas que deberá contestar durante la redacción del escrito. Estos interrogantes le serán de mucha ayuda para redactar con precisión las desviaciones, causas y soluciones que presentará en su informe, así como para su dictamen. Asimismo, debe interpretar en forma personal estos interrogantes y utilizar los que más le convengan:

¿Qué?

- *¿Qué se quiere o debe informar acerca de la evaluación realizada?*
- *¿Qué se desea hacer notar acerca de la evaluación?*
- *¿Qué se debe o se puede evitar de las observaciones?*
- *¿Qué es lo importante y qué es lo irrelevante de la evaluación realizada?*
- *¿Qué estilo de redacción se utilizará en el informe de auditoría?*

- *¿Qué formatos se utilizarán para reportar las situaciones encontradas, las situaciones relevantes y el dictamen de auditoría?*
- *¿Qué criterio se debe seguir para jerarquizar las situaciones que se van a reportar?*
- *¿Qué tan importante es esta observación para reportarla?*

¿Quién?

- *¿Quién leerá este informe?*
- *¿A quién le interesará el contenido del informe?*
- *¿Quién aceptará lo escrito y quién lo rechazará?*
- *¿Quién o quiénes recibirán el informe?*
- *¿Quién será el afectado con lo que se reporte?*
- *¿Con quién comparar el informe? (O ¿contra quién compararlo?)*
- *¿Con quién consultar su contenido?*

¿Cuándo?

- *¿Cuándo se empieza a redactar la situación?*
- *¿Cuándo se terminará de redactar una situación?*
- *¿Cuándo se incluye determinada parte y cuándo no?*
- *¿Cuándo se elimina o se agrega información?*
- *¿Cuándo es borrador del dictamen?*
- *¿Cuándo brincar párrafo?*
- *¿Cuándo se entregará el informe?*
- *¿Cuándo ampliar y cuándo reducir la información?*
- *¿Cuándo utilizar información técnica de los sistemas y cuándo evitarla?*
- *¿Cuándo incluir anexos y cuadros adicionales?*

¿Dónde?

- *¿Dónde se empieza el informe?*
- *¿Dónde se termina el informe?*
- *¿Dónde va este comentario?*
- *¿Dónde se pone una cita textual?*
- *¿Dónde se anexan gráficas o cuadros estadísticos?*
- *¿Dónde dar énfasis y dónde ser sutil?*
- *¿Dónde destacar lo importante?*
- *¿Dónde va cada parte?*

¿Cómo?

- *¿Cómo redactar cada parte del informe?*
- *¿Cómo redactar todo el informe?*
- *¿Cómo jerarquizar las situaciones que se reportan?*
- *¿Cómo señalar adecuadamente el contenido del informe y del dictamen?*

- *¿Cómo determinar las partes del informe, sus capítulos, temas y anexos?*
- *¿Cómo especificar las situaciones, las causas y soluciones?*
- *¿Cómo evitar preferencias, distorsiones y desvíos de la información que se reporta?*
- *¿Cómo concentrar las situaciones en el dictamen?*
- *¿Cómo distinguir las situaciones importantes de las irrelevantes?*
- *¿Cómo supervisar la elaboración correcta del informe?*

¿Por qué?

- *¿Por qué redactar el informe?*
- *¿Por qué anotar cada situación, causa y solución?*
- *¿Por qué esta parte del dictamen va antes y aquélla después?*
- *¿Por qué esta situación va antes y aquélla después?*
- *¿Por qué se tiene que reportar esta observación o por qué no se debe hacer?*
- *¿Por qué dividir el informe en capítulos, temas y anexos?*
- *¿Por qué resumir las situaciones encontradas en situaciones relevantes?*
- *¿Por qué se redacta de determinada manera cada situación?*
- *¿Por qué se tiene que redactar el dictamen?*

¿Para qué?

- *¿Para qué redactar el informe de auditoría?*
- *¿Para qué se evaluó y revisó el área, sistema o actividad informática?*
- *¿Para qué se tiene que reportar esta observación?*
- *¿Para qué se divide el informe en situaciones, causas y soluciones?*
- *¿Para qué pulir la redacción y presentación del informe?*
- *¿Para qué concentrar las situaciones encontradas en situaciones relevantes, y éstas en el informe final y en el dictamen de la auditoría?*
- *¿Para qué elaborar el dictamen del auditor?*

Los anteriores interrogantes pueden ser apreciados como irrelevantes o demasiado obvios y, por consiguiente, no son considerados *a priori* en la elaboración del informe de auditoría de sistemas computacionales; sin embargo, la experiencia ha demostrado que al omitir muchas de estas preguntas en la redacción del informe, existen serias deficiencias en la elaboración de éste. Finalmente, lo que se pretende con esos interrogantes y los que se anexen como parte de la experiencia de trabajo, es que el auditor los analice cuando esté elaborando su informe, se interrogue a sí mismo y medite sus respuestas, para que realice de la mejor manera posible su informe de auditoría de sistemas.

8.2.2.11 Exactitud

"Del latín ***exactus:*** Acabado. Justo, conforme a la regla o a la verdad".[11] "Puntualidad y fidelidad en la ejecución de una cosa."[12]

En la redacción del informe de auditoría de sistemas, esto significa dar el sentido exacto a las palabras, a fin de hacer el texto entendible y enfocarlo justo a lo que se quiere dar a conocer al lector del informe. Es decir, lo que el auditor quiere reportar de su evaluación. Concretamente, significa plasmar las ideas, aportaciones, conclusiones y comentarios conforme se necesitan, y con la minuciosidad y escrupulosidad que se requiere de los vocablos adecuados, a fin de que el lector del informe entienda exactamente lo que se quiere expresar de la auditoría practicada.

Esta característica de la redacción es de las más importantes y, sin embargo, es una de las más descuidadas, si no es que la menos tomada en cuenta a la hora de redactar las situaciones, causas y soluciones que se van a reportar; es frecuente, ya sea por ignorancia, pobreza de lenguaje o negligencia, redactar los informes con vocablos más o menos parecidos a lo que se quiere manifestar, sin analizar si esas palabras lo expresarán realmente. En muchas ocasiones, esto se debe al desconocimiento del significado real del término utilizado, o por querer adornar el texto con vocablos técnicos y literarios que no están relacionados con lo que se informa en el escrito.

Es muy frecuente que el auditado alegue la falta de exactitud de las situaciones y comentarios plasmados en un informe de auditoría, debido a que el auditor utiliza a lo largo de su informe sólo los vocablos que son de uso más común en su disciplina, y es muy frecuente que abuse de la repetición de los mismos conceptos, aunque muchas veces estén fuera de lugar o no sean congruentes con lo que quiere testimoniar acerca de la evaluación practicada. Abundan los ejemplos de esta falta de exactitud en los reportes de auditoría; a continuación presentamos algunos de ellos:

- *El uso indiscriminado de los conceptos política, por norma, regla o lineamiento, los cuales tienen significados diferentes.*
- *El uso indiscriminado del vocablo filosofía (amor a la sabiduría), el cual se utiliza para diferentes aspectos y conceptos: la filosofía de esta auditoría, la filosofía de la empresa; así como el uso excesivo de extranjerismos o tecnicismos cuyo significado literario se desconoce, al igual que su aplicación específica en el texto.*
- *El abuso de los términos de sistemas en un informe que está destinado a directivos ajenos al área de sistemas.*

Una buena medida para corregir este vicio en la redacción, sería que el encargado de la auditoría obligara a los auditores a utilizar sinónimos cuando observe la repetición de vocablos y, si es necesario, que investiguen en algún diccionario el significado real de esas expresiones. Claro está, de acuerdo con las características y necesidades de la elaboración del informe de auditoría y de la propia disciplina de sistemas.

8.2.2.12 Imparcialidad

Uno de los requisitos más importantes que se le exigen al auditor *es que sea íntegro y profesional en la elaboración de su reporte de auditoría, anotando las observaciones*

tal y como las encontró durante su evaluación, es decir, que reporte en forma ecuánime las situaciones que informa, que no tome partido, ni para perjudicar enfatizando la gravedad de las desviaciones ni para solapar ni minimizar los errores encontrados durante su evaluación. Que sólo reporte lo justo.

Ésta es una de las características que le dan mayor solidez a la actividad de la auditoría, ya que, se supone, el auditor aplica de manera ecuánime sus herramientas e instrumentos de evaluación, lo cual le ayuda a observar, juzgar y reportar lo que ha encontrado de manera imparcial, sin ningún sesgo ni tomar partido hacia algo o alguien.

La credibilidad del informe de auditoría se fundamenta en la imparcialidad con que el auditor lo elabora, es decir, que no lo enfoque hacia el negativismo y el constante error, ni que minimice la importancia y gravedad de las desviaciones que reporta. Esto es lo que el auditor debe buscar al elaborar su informe de auditoría, que al leerlo, el destinatario capte su imparcialidad.

Respecto a la forma de elaborar los informes de auditoría de manera imparcial, no hay reglas establecidas que se puedan señalar como recetas de cocina, sin embargo, es necesario que el auditor contemple algunos de los aspectos que mencionaremos a continuación al elaborar su informe:

- *Actuar de manera imparcial invariablemente, es decir, sin una posición paternalista ni prepotente, sino justa, de acuerdo con el profesionalismo del auditor.*
- *No admitir influencias de ningún tipo, ya que podrían llegar a desvirtuar la imparcialidad del informe de auditoría.*
- *Ser equilibrado en los comentarios, no redactar como si fuera a vengar alguna ofensa, ni con benevolencia malentendida. Redactar sólo lo justo y necesario, y con los datos indispensables.*
- *Ponerse en el lugar del lector del informe, a fin de evaluar la suavidad o la dureza de lo que va a reportar, buscando ser ecuánime y equilibrado.*
- *Evitar el uso de un lenguaje áspero, impositivo, hosco y dañino que manifieste una posición de dureza, así como del tenue, dócil, condescendiente, manso y apacible que manifieste falta de carácter.*
- *Evitar ser intransigente e impositivo al redactar las desviaciones que va a reportar, así como tampoco ser sumiso ni blandengue, sino justo, equitativo e imparcial.*
- *Evitar ser sarcástico y burlón en la redacción del informe, así como manso y falto de carácter.*
- *Hacer el reporte como un trabajo profesional y no como un foro de exhibición, debate o como instrumento de venganza.*

8.2.2.13 Objetividad

Es *el entendimiento de las cosas, ideas y valores por sí mismos y no por lo que se piensa, razona e interpreta*; en el caso del informe de auditoría de sistemas es la descripción apegada a la realidad de lo que se ve; en este caso de lo que se comprueba por

medio de la evaluación, con el propósito de redactar las observaciones tal y como se presentan, describiendo los resultados de la auditoría lo más naturalmente posible.

Esta característica es una de las más valiosas para la elaboración del informe de auditoría, pues ayuda al auditor a redactar las observaciones tal y como se presentan en el sistema, en la operación o en el área de sistemas que está evaluando, sin hacer ninguna interpretación del hecho que audita, sino describiéndolo tan fielmente como se presenta en la realidad. Ésta puede ser una muy buena cualidad del informe, si se sabe aplicar a las desviaciones reportadas.

Ésta es una particularidad muy fácil de entender (*narrar los hechos tal y como se presentan*), pero muy difícil de llevar a cabo, puesto que requiere un alto dominio del arte de la redacción, así como una amplia experiencia para describir las observaciones de la auditoría tal y como se presentaron. Además exige un alto conocimiento del lenguaje y de la expresión lingüística y literaria, a fin *de no tratar de interpretar las cosas como se supone* que *deberían hacer*se, *sino presentarlas tal y como las observó el auditor*; ni más ni menos, únicamente lo captado. Esto es muy difícil para algunos auditores principiantes, ya que prefieren escribir lo que interpretan y no lo que ven en realidad.

Sin embargo, esto no quiere decir que el informe de auditoría siempre debe ser totalmente objetivo, sino que es obligación del auditor tratar de redactar las desviaciones tal y como las encontró al hacer su evaluación; pero también debe darle a cada caso la interpretación que requiera, a fin de valorar, desde un punto de vista profesional, el comportamiento y cumplimiento de lo que está evaluando.

Es necesario entender que el informe de auditoría se debe elaborar con esta característica para tratar de evitar las interpretaciones subjetivas, razonadas o caprichosas, de lo que se evalúa. El único propósito es que el auditor haga su reporte lo más objetivamente posible, pero que no por ello describa sólo la realidad que ve, sino que también pueda emitir su opinión acerca de lo que está auditando.

Lo contrario de la objetividad es la subjetividad, *entendida como lo relacionado con el modo de razonar e interpretar las cosas, no como se presentan en la realidad sino como se interpretan*. Para el caso del informe de auditoría, esto se puede entender de dos maneras; la primera es *la interpretación que el auditor hace de los resultados de la evaluación, a fin de dar su punto de vista como profesionista*, lo cual es totalmente válido. La segunda *es la interpretación sin sustento y sólo como una corazonada que un auditor hace de lo que reporta*, lo cual sólo le conduce a señalar cosas sin fundamento ni respaldo. Es decir, sólo informa por reportar algo y no porque tenga bases para ello.

Finalmente, señalaremos que la objetividad en el informe de auditoría será de acuerdo con las desviaciones que se reporten; es decir, el auditor podrá ser tan descriptivo o tan restrictivo como lo requiera la observación; pero esto en ningún momento debe limitar la libertad del auditor para emitir su opinión de la situación que reporta, de acuerdo con su experiencia y conocimientos. Evidentemente, es responsabilidad del propio auditor y del encargado de la auditoría tratar de evitar la redacción subjetiva de

lo que se auditó, a fin de evitar reportar cosas sin fundamento, nacidas sólo de una interpretación personal.

8.2.2.14 Congruencia

Congruencia *es que lo que se está reportando concuerde o corresponda con lo que en realidad está sucediendo, de tal forma que sólo se informen las cosas que el auditor conoce, siempre y cuando éstas correspondan al objeto y tema de la auditoría*. No es válido ni congruente expresar cosas diferentes a las que suceden, ya sea por desconocimiento o por falta de análisis de lo que se informa, o porque lo encontrado se parezca a lo que se quiere reportar o por cualquier otra causa que haga que el auditor informe aspectos diferentes a lo evaluado.

Esta característica adquiere significados muy especiales en el ambiente de la auditoría de sistemas computacionales, debido a que existen muchos auditores que por ignorancia o falta de experiencia en este campo tratan de evaluar la actividad de sistemas con otro tipo de auditorías, utilizando herramientas tradicionales que son buenas para otras revisiones, pero inútiles e incompletas para las auditorías de sistemas computacionales. En algunos casos tratan de adaptarlas, lo cual es bueno; pero en otros, sólo buscan obtener los mismos resultados de la auditoría anterior, aunque no haya sido de sistemas. Es obvio que esto provoca que los auditores obtengan resultados distorsionados del funcionamiento de los sistemas y, evidentemente, al emitir su informe reportan incongruencias entre la forma como, según ellos, deberían funcionar los sistemas evaluados y lo que realmente está sucediendo en ellos.

La función del auditor de sistemas consiste precisamente en aplicar las herramientas, técnicas, métodos y procedimientos específicos* que se utilizan en este tipo de auditorías, a fin de garantizar una revisión profesional. Con esto se compromete al auditor a reportar resultados congruentes con lo que auditó de los sistemas; es decir, a que informe lo que observa de manera congruente con lo que ocurre realmente.

Debemos agregar que la concordancia se debe entender como la expresión de las ideas y conceptos tal y como suceden, sin tratar de manifestar cosas fuera de lo evaluado; esto es, se deben informar las situaciones encontradas tal y como suceden en el ambiente de sistemas auditado, y no como se supone que deberían suceder, ni tampoco como acontecen en ambientes ajenos a dichos sistemas. Tampoco es válido utilizar la imaginación para suponer cosas que no suceden o que no se verificaron cabalmente, las cuales sólo llevan a reportar suposiciones. *En una auditoría no se deben reportar suposiciones, sólo se deben informar las desviaciones que hayan sido comprobadas cabalmente*.

Finalmente, la congruencia en el informe de auditoría de sistemas es reportar las cosas conforme se encontraron sin expresar nada irreal, inventado, imaginado o situaciones que no correspondan a lo auditado.

* En los capítulos 9, 10 y 11 se hace un profundo análisis de estas herramientas.

Se *deben reportar las peras como peras* (informe objetivo) *y no como figuras de chocolate en forma de pera* (informe subjetivo).

8.2.2.15 Familiaridad

Esta característica tiene mucho que ver con los conocimientos y experiencia que el auditor tenga en el área que esté auditando, debido a que debe redactar las observaciones en un lenguaje que sea familiar para quien vaya a leer el informe, evitando expresarlas en lenguajes que sean desconocidos para este último.

Se dice que algo es familiar porque se conoce mucho o porque se trata cotidianamente, o es algo en lo cual uno es experto. Familiaridad viene de familia: *"[...] Categoría taxonómica que reúne varios géneros con caracteres comunes[...]";*[13] esto nos indica que el auditor debe informar sobre lo que es familiar a los auditados, exclusivamente en el lenguaje y estilo que ellos manejan y en cuyo trabajo son expertos. No es válido ni profesional emplear expresiones distintas a las que se utilizan cotidianamente en la institución donde se realizó la auditoría. Es una obligación del responsable de la auditoría que en el informe se utilice un lenguaje que sea familiar para los auditados y no el que el auditor supone que se debería utilizar.

En el ambiente de sistemas, lo familiar también se refiere al léxico exclusivo y específico del área de sistemas al cual están acostumbrados tanto el personal del área como sus usuarios; pero se refiere específicamente al idioma informático que se utiliza en ese centro de cómputo, no al que se utiliza en otros ambientes de sistemas. El lenguaje de los usuarios de redes no es igual al de los usuarios de equipos mayores (mainframes), ni tampoco al que utiliza un usuario principiante de computadora personal. Cada uno expresa aparentemente sus vocablos en idiomas diferentes, aunque todos se refieren a los sistemas computacionales. Por eso es de suma importancia que, al elaborar el informe de auditoría de sistemas, el auditor utilice expresiones que sean familiares para los usuarios de las áreas que esté auditando.

Sin embargo, el auditor también debe evitar, lo más que pueda, el abuso de términos informáticos que dificulten la comprensión del informe de auditoría tal y como él lo trata de expresar.

Familiaridad también significa utilizar el lenguaje que se debe usar para reportar las situaciones en palabras que el lector entenderá; es decir, en el idioma coloquial que se utiliza en el ambiente de sistemas auditado. El mismo que los auditados deben y pueden entender. Esto garantiza que las inconsistencias reportadas en el informe serán captadas.

8.2.2.16 Veracidad

Como requisito indispensable para su credibilidad, el informe de auditoría debe ser veraz entre lo que se reporte como observaciones y lo que corresponda a la revisión realizada en el ámbito de sistemas; de tal manera que las situaciones que se manifiesten en el informe siempre correspondan con lo que realmente esté sucediendo en el área evaluada.

Esta característica es de suma importancia para la elaboración correcta de los informes de auditoría, debido a que es obligación del auditor informar las cosas tal y como sucedieron al momento de efectuar la evaluación o, en su caso, tal y como están sucediendo en la actualidad. Sin inventar algo que no exista, ni tampoco reportar cosas que no fueron verdaderamente evaluadas, pero de ningún modo debe ocultar las desviaciones encontradas.

Veracidad se deriva de *verdad*:

"Del latín **veritas–atis***, de* **verus***: Verdadero, cosa cierta."*[14] *"Conformidad del pensamiento o idea con la realidad de las cosas; o conformidad del pensamiento con sus propias leyes. Adecuación de lo que se dice con lo que se piensa o se siente. Propiedad de una cosa de mantenerse siempre la misma sin inmutarse. Juicio o proposición que no se puede negar racionalmente. Calidad de lo veraz (que dice o profesa siempre la verdad)[...]"*[15]

La sola definición nos permite entender esta característica tan importante para los informes de auditoría, debido a que al conferirle una gran confianza al auditor, se espera que éste exprese sus observaciones siempre con la verdad, y que las desviaciones que encuentre sean producto de una alta experiencia y conocimiento en el ramo que esté auditando, y producto de la aplicación de técnicas y procedimientos profesionales que le permitan comprobar lo que reporte. *De ahí la confianza en que sea veraz en lo que informe.*

La veracidad también debe ser una cualidad del auditor, ya que como profesional de auditoría de sistemas debe tener una ética y una moral a toda prueba y, sin lugar a dudas, siempre debe actuar con toda equidad en su trabajo. Por lo tanto, a la hora de elaborar su informe, debe reportar exclusivamente lo que encontró, sin limitar, ocultar ni minimizar las observaciones que sean necesarias. Siempre se debe apegar a una verdad que sea producto de sus pruebas y procedimientos de auditoría. En eso estriba la confianza que se le tiene al auditor.

8.2.2.17 Efectividad

La efectividad es otra de las características fundamentales que debe tener cualquier informe de auditoría, debido a que contribuye a que quien lo lea entienda mejor las situaciones que en él se informan. Esto es precisamente lo que se busca en el informe, que las observaciones estén anotadas como se presentaron realmente durante la revisión. La efectividad del informe consiste en saber expresar las observaciones en forma eficiente y eficaz.*

* **Eficaz**: "Eficiente, operativo. Se dice de la persona que lleva a cabo un proyecto, y de la cosa que contribuye a su realización." **Eficiente**: "Que realiza la función para la que se destina. Competente, capaz [...]" Opcit. Gran Diccionario... Págs. 654 y 655.

Ampliando lo anterior, *la efectividad del informe de auditoría de sistemas consiste en saber expresar, con palabras simples, completas, congruentes y en estricto sentido profesional, lo que se quiere informar; de este modo, cualquier persona que lea el informe captará de inmediato lo que el auditor reporta y podrá interpretarlo como éste quiere que sea interpretado, de tal manera que no requerirá ninguna explicación adicional para entender las desviaciones y su repercusión en la operación normal del ámbito de sistemas, así como las causas que las originaron y sus posibles soluciones.* En esto estriba la efectividad del informe.

El auditor de sistemas debe cumplir cabalmente con la característica de *efectividad*, redactando de manera eficiente las desviaciones que detectó, y también debe interpretar eficazmente el comportamiento del ámbito de sistemas que está auditando; además, como profesional de esta materia, también debe actuar eficaz y eficientemente en la evaluación que practique y, por supuesto, en la elaboración de sus informes.

En cuanto a redacción, efectividad significa saber expresar las ideas y conceptos con las palabras adecuadas, de tal manera que el lector entienda en los términos y dimensiones lo que se le quiere comunicar.

8.2.2.18 Positividad

Uno de los vicios más comunes en la auditoría consiste en elaborar el informe utilizando expresiones negativas, tales como: *no se encuentra..., no se realiza..., no se observa..., no se tiene..., no se logró..., nunca se cumple con..., nunca se procesa con... u otras negaciones*; *o también resaltando constantemente los errores, fallas y deficiencias de la operación, los retrasos e incumplimientos y una serie de expresiones de tipo destructivo que sólo provocan una gran oposición entre el auditor que informa y los responsables de la operación que lo escuchan (reciben);* es decir, que muchas ocasiones lo que reporta el auditor sea tomado como una confrontación entre él y el auditado.

Se debe tomar en cuenta que el propósito de una auditoría no es sólo reportar lo insatisfactorio de lo que se evalúa, sino informar de estas deficiencias para ayudar a corregirlas; por la tanto, el informe de auditoría de sistemas computacionales se hace para reportar la forma en que están funcionando dichos sistemas, la eficiencia de sus procesamientos y el cumplimiento de las actividades y operaciones que tienen encomendadas, así como sus deficiencias y sus aciertos. Mas nunca se debe elaborar con el malsano propósito de reportar sólo las deficiencias encontradas, y mucho menos para darlas a conocer en sentido negativo.

Para entender cómo se aplica esta característica, es necesario entender que, al realizar su evaluación, en última instancia el auditor busca y encuentra deficiencias en la operación normal que realiza un auditado, las cuales reporta en un informe; esto ocasiona frecuentemente que al auditado no le gusten los informes que le den a conocer fallas y deficiencias en el cumplimiento de su operación (*recordemos que casi nunca estamos dispuestos a recibir comentarios sobre las deficiencias de nuestro trabajo*);

por esta razón, aunque ésta es la función del auditor —*reportar las deficiencias en el trabajo*—, casi siempre se crean confrontaciones entre el auditor y el auditado, más aún si el reporte está escrito en un tono negativo y plagado del constante señalamiento de errores y deficiencias de quienes realizan la operación. De ahí la importancia de utilizar el lenguaje en forma afirmativa en el informe, o cuando menos no tan frecuentemente de manera negativa.

Esto no quiere decir que el reporte de auditoría deba ser blando, tímido o superficial, ni que sólo se informe lo bien realizado; lo que se quiere dar a entender, es que el auditor debe reportar las cosas tal y como las encontró en la evaluación, lo más objetivamente posible, pero tratando de evitar el sentido negativo en las expresiones que reporte. Recordemos que se trata de dar a conocer las desviaciones encontradas para que sean solucionadas. No se trata de evidenciar las deficiencias en un estricto sentido negativo, sino positivo para que éstas sean corregidas. Se debe hacer una crítica constructiva, no destructiva.

8.2.2.19 Sintaxis

Ésta es una de las partes elementales de la gramática; la sintaxis estudia la estructuración de las palabras, a fin de hacer congruente la composición de las frases y oraciones que integran un escrito.

Como característica del informe, podemos señalar que *es la construcción correcta de las frases, oraciones y partes específicas de un texto; la sintaxis se utiliza con el propósito de ordenar la formación de las ideas, conceptos y aportaciones que se expresan en un escrito para hacerlo entendible y apegado a lo que se quiere dar a entender.*

Esta regla elemental de la redacción, que es básica en la formación de los estudiantes desde sus primeros años de escolaridad, es uno de los principales obstáculos a los que se enfrenta un auditor cuando prepara su informe de auditoría, pues es muy frecuente que al redactar el texto de su informe, lo realice con muy serias deficiencias en cuanto a la construcción de frases, oraciones y la congruencia de los términos utilizados para expresar sus ideas en las situaciones que reporta. Hay auditores que al parecer no conocen esta regla gramatical y no la aplican en la construcción del informe. Claro está, con sus honrosas excepciones de auditores muy capacitados.

El responsable de la auditoría debe hacer recomendaciones al auditor para evitar deficiencias de sintaxis, de acuerdo con su experiencia y conocimientos, así como con la práctica constante en la redacción de estos informes; en su caso, también debe exigirle un repaso al uso elemental de cada una de las partes de la gramática.

8.2.3 Características importantes para el lector del informe de auditoría

Además de las anteriores características, el informe de auditoría se debe elaborar conservando los siguientes aspectos fundamentales de fondo y forma:

- *Que el informe tenga familiaridad*
- *Que el contenido del informe sea coloquial*
- *Que el contenido del informe sea variado*
- *Que se entregue y comente oportunamente*
- *Que su lectura sea sencilla*
- *Que su contenido esté fundamentado*
- *Que su redacción sea clara*
- *Que la información contenida sea contundente*
- *Que esté redactado en un estilo impersonal*
- *Que su contenido esté sintetizado*
- *Que su contenido sea ameno y entendible*
- *Que sea enfático en las situaciones reportadas*

Aunque la mayoría de estos aspectos parecen repeticiones de las características señaladas anteriormente, para entender la importancia de la redacción del informe conviene reiterar algunas de ellas; a continuación veremos un breve análisis de cada uno de estos puntos:

8.2.3.1 Familiaridad

Ya señalamos esto en la característica de la familiaridad, pero conviene repetir que en la redacción del informe se tiene que emplear un lenguaje que utilicen y entiendan los auditados y quienes leerán dicho informe, a fin de reportar las situaciones de modo que todos las interpreten de la misma manera.

Para el ambiente de sistemas, la familiaridad también se entenderá como el uso de los vocablos cotidianos del área de sistemas, de acuerdo con las nomenclaturas y términos exclusivos de los sistemas computacionales utilizados en la empresa.

8.2.3.2 Contenido coloquial

Además de estar escrito con un lenguaje familiar, el informe de auditoría también debe emplear un lenguaje coloquial; es decir, utilizando un estilo de redacción cotidiano, no literario, con las frases más comunes y cotidianas que se acostumbren en el área auditada, de tal manera que el informe esté hecho en forma de diálogo, como si fuera una plática entre el auditado y el auditor.

Para el caso concreto de la auditoría de sistemas, lo coloquial se entiende como el uso diario del lenguaje especializado para el área de sistemas, adaptándose a las características específicas del tipo de lenguaje, equipo y sistemas que se utilizan en la empresa auditada. Claro está, observando para ello lo señalado en la característica de familiaridad (*sección 8.2.2.15*).

8.2.3.3 Variedad

Aquí se debe entender que el informe de auditoría no debe ser monótono ni aburrido, de una sola tonalidad ni con el uso limitado de vocablos; por el contrario, se debe expresar

la variedad del lenguaje, utilizando frases diferentes y sinónimos para hacer más rico y variado su contenido. Es muy común que el auditor utilice siempre las mismas frases a lo largo del informe: *También se encontró que..., Además de..., Con base en lo anterior..., De acuerdo con la revisión efectuada a..., Se observó que..., Se descubrió que...* y otras frases similares. Cuando el auditor es repetitivo en sus vocablos, muestra una gran pobreza de lenguaje y monotonía enfadosa en lo que reporta, y pierde la categoría de auditor ante los lectores del informe. Esto, obviamente, reduce la credibilidad de lo que reporta.

Además, en el contenido del informe se deben contemplar todos los aspectos que hayan sido auditados, sin omitir ningún concepto, pero sin explayarse exclusivamente en uno solo, a fin de hacer más rico y productivo el informe.

8.2.3.4 Comentarios y entrega oportunos

Ya señalamos en la característica de oportunidad (en la sección 8.2.2.9), que el informe de auditoría se debe entregar y comentar a tiempo, a fin de que sea útil para la toma de decisiones de los directivos del área de sistemas y de la empresa. Sin este requisito, no tiene caso presentar ningún informe de auditoría.

8.2.3.5 Lectura sencilla

Para que el informe sea útil para los auditados, se debe redactar de tal manera que su lectura sea muy sencilla y ágil, a fin de que los lectores entiendan de inmediato lo que el auditor quiere reportar, y evitar que no entiendan, que mal interpreten o no acepten el informe.

Ya señalamos esto en la característica de sencillez (en la sección 8.2.2.5), pero conviene enfatizarlo.

8.2.3.6 Contenido fundamentado

Para emitir un buen informe de auditoría de sistemas, es un requisito indispensable que esté fundamentado y soportado por las pruebas, métodos y procedimientos de auditoría de sistemas, ya que eso le da validez a las observaciones del auditor.

Por esta razón, el informe de auditoría debe estar perfectamente avalado, con una clara exposición de lo que se observa, para que realmente se reporten los aspectos relevantes de la evaluación practicada. Si no existiera este fundamento, el receptor del informe no le daría credibilidad ni le daría la validez necesaria.

8.2.3.7 Redacción clara

Ya señalamos esto a lo largo de la sección anterior, sin embargo conviene resumir que la redacción del informe de auditoría de sistemas debe ser lo más clara, sencilla y veraz posible, a fin de que los lectores entiendan de manera inmediata las observaciones reportadas, sin tener la necesidad de una explicación adicional.

Además, en el caso específico de las auditorías de sistemas, los reportes de las desviaciones se deben hacer con un lenguaje cotidiano, claro y que los auditados entiendan de inmediato. También se deben utilizar los tecnicismos de sistemas con la moderación requerida, para que se comprenda claramente lo que se quiere reportar.

8.2.3.8 Información contundente

Para que el informe de auditoría sea útil para sus lectores, su contenido debe tener la suficiente contundencia y fortaleza, a fin de que las desviaciones reportadas de la operación y funcionamiento de los sistemas de la empresa se acepten de inmediato y sin necesidad de hacer comentarios adicionales. La contundencia significa no dejar lugar a dudas acerca de las desviaciones informadas, para que se entiendan de la manera como se quieren expresar.

En este caso, la contundencia significa no dejar dudas sobre lo reportado en el informe de auditoría, a fin de que el lector comprenda de inmediato lo que en realidad está ocurriendo en el ambiente de sistemas evaluado.

8.2.3.9 Redacción impersonal

Ésta es una característica muy importante para la presentación de los informes de auditoría, pues el auditor debe utilizar un estilo de redacción de tipo profesional al expresar sus observaciones; de preferencia se debe tratar en forma impersonal o en tercera persona; además, tiene que evitar el uso de un tono impositivo e imperativo en las situaciones reportadas, así como un tono de regaño o menosprecio.

Además de ser oportuno, confiable y claro, el informe de auditoría también se debe redactar impecablemente, con un estilo impersonal o en tercera persona.

8.2.3.10 Contenido sintético

El informe de auditoría no debe contener información excesiva de cada situación, lo cual lo haría tedioso; por el contrario, debe tener un contenido sintético que haga ágil y sencilla su lectura.

Además, el auditor debe evitar la abundancia de literatura que sólo hace fatigosa la lectura del informe; pero, sobre todo, debe evitar la repetitividad de las situaciones que reporta, las aclaraciones adicionales y la sobreinformación que hace demasiado abultado el informe. Sin embargo, esto no significa que deba hacer el reporte demasiado sencillo o carente de información.

8.2.3.11 Contenido ameno y entendible

El informe de auditoría tampoco debe ser muy aburrido, espeso ni solemne, aunque tampoco festivo. Debe ser redactado en un lenguaje claro y comprensible para cualquier lector, y si no es ameno, al menos no debe ser tedioso.

Al respecto se debe considerar que si bien es cierto que un informe de auditoría debe ser formal y de carácter profesional, no por ello se debe redactar en forma densa y aburrida. Es obligación del encargado de elaborar el informe buscar un equilibrio entre la formalidad y lo entendible del mismo.

8.2.3.12 Enfático en situaciones reportadas

Aunque no es válido que el informe de auditoría sea repetitivo y redundante, no por ello debe dejar de ser enfático, es decir, se debe resaltar lo realmente importante de las observaciones encontradas durante la auditoría practicada.

Enfatizar significa resaltar lo importante de las situaciones reportadas, de tal manera que el lector capte lo que el auditor quiere distinguir en la evaluación. Sin embargo, esto no implica que todo lo reportado en el informe de auditoría debe ser sobresaliente.

La finalidad de esta sección es que el auditor de sistemas analice cada uno de estos puntos, para que encuentre el estilo de redacción que le ayude a elaborar mejor sus informes de auditoría de sistemas. Para ello es indispensable que estudie y entienda cada uno de los aspectos anteriores.

8.3 Estructura del informe de auditoría de sistemas computacionales

Aunque hay muchas formas de presentar el informe de auditoría de sistemas computacionales, de acuerdo con las preferencias de la empresa o del auditor que realiza la auditoría, a continuación proponemos un modelo para presentarlo.

Esta última parte, y la más representativa de la utilidad e importancia de una auditoría de sistemas computacionales, es el llamado informe de auditoría, el cual es un documento en el que se hace la presentación formal de los resultados obtenidos durante la auditoría.

El informe de auditoría de sistemas computacionales se puede definir de la siguiente manera:

> *Es un documento formal que utiliza el auditor de sistemas para informar por escrito y de manera oportuna, precisa, completa, sencilla y clara, sobre los resultados que obtuvo después de haber aplicado las técnicas, métodos y procedimientos apropiados al tipo de revisión que realizó, para fundamentar con ellos su opinión respecto a la auditoría realizada y estar en condiciones de poder emitir un dictamen correcto sobre el comportamiento del sistema, sobre los empleados del área de sistemas y sobre los resultados obtenidos de su operación normal, a fin de que el directivo que reciba el informe conozca la situación real del área de sistemas auditada.*

Éste es el documento final, de carácter formal, en el que se presentan por escrito todos los aspectos importantes que fueron catalogados como deficiencias de las operaciones auditadas, así como el cumplimiento de las funciones y de los resultados obtenidos con las actividades evaluadas durante la auditoría. El auditor plasma su dictamen y opinión profesional en este documento, y lo sustenta con documentos de apoyo y papeles de trabajo en los que va haciendo las anotaciones de las técnicas, métodos y procedimientos que utilizó durante el desarrollo del trabajo. El informe de auditoría debe contener, como mínimo, las siguientes secciones (vea la figura 8.2):

- *Oficio de presentación*
- *Introducción*
- *Dictamen de la auditoría*
- *Situaciones relevantes*
- *Situaciones detectadas*
- *Anexos*
- *Confirmaciones en papeles de trabajo*

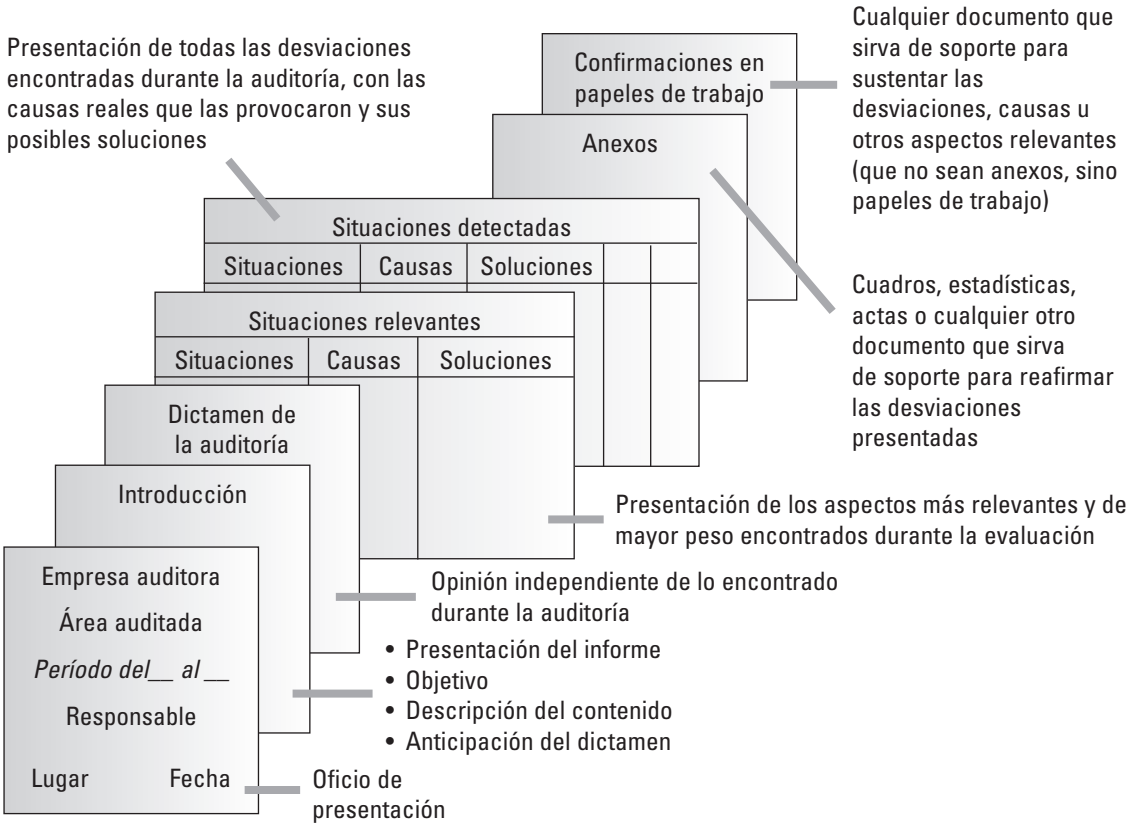


Figura 8.2 *Contenido del informe de auditoría de sistemas computacionales*

Como es costumbre en este libro, a continuación analizaremos detalladamente cada uno de estos aspectos.

8.3.1 Oficio de presentación

Es la primera parte del informe de auditoría y es un documento de carácter oficialque sirve como presentación del informe; mediante este documento se pone a consideración de los directivos de la empresa el resultado de la auditoría practicada al área de sistemas.

El contenido y presentación de dicho documento varían de una institución a otra, pero en esencia, este documento debe ser elaborado en la papelería oficial de la empresa y debe contener como mínimo los siguientes aspectos (vea la figura 8.3):

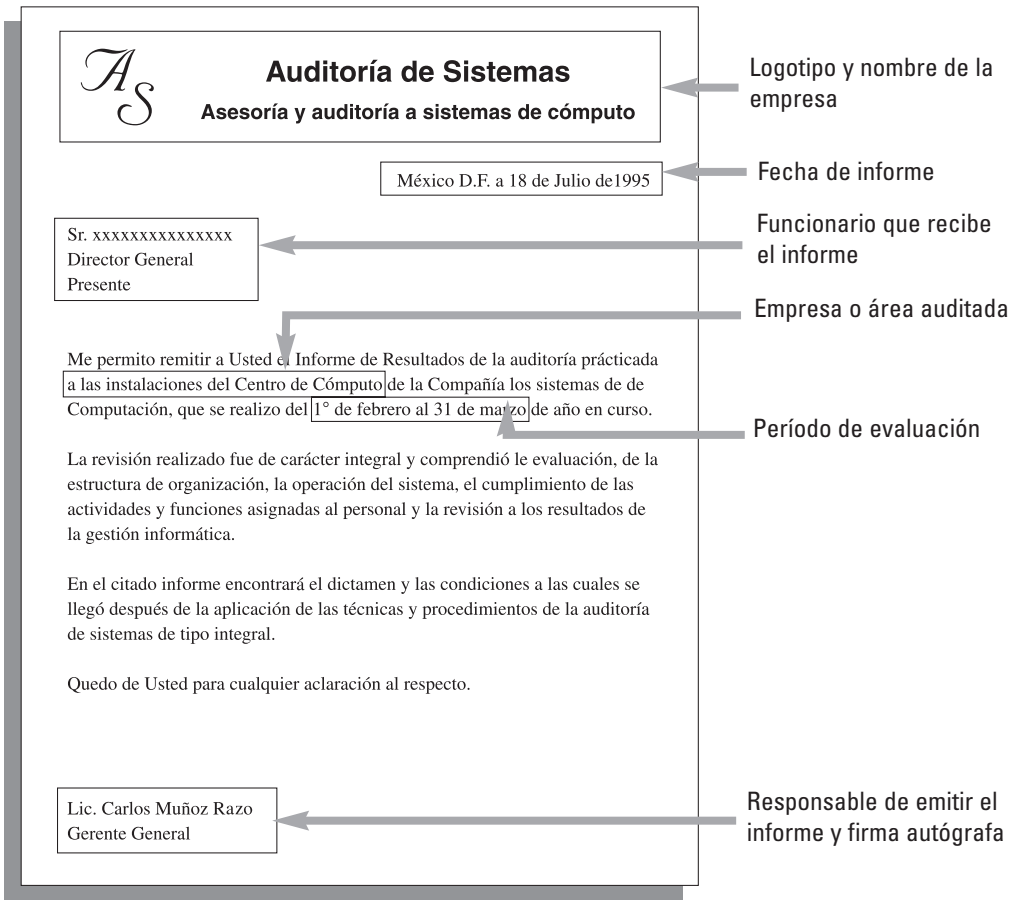


Figura 8.3 *Oficio de presentación.*

8.3.1.1 Logotipo de identificación

Si se trata de una auditoría externa, se debe poner el logotipo de la empresa que realiza la auditoría, pero si es una auditoría interna, entonces se debe ponerse el logotipo de la misma empresa y la identificación del área de auditoría interna (si existe). En cualquiera de los dos casos, el oficio de presentación siempre debe llevar el logotipo, y se debe colocar de acuerdo al diseño de la documentación oficial.

8.3.1.2 Nombre de la empresa (o área interna de auditoría)

Si es una auditoría externa, se pone el nombre y logotipo de la empresa que realiza la auditoría. Sin embargo, cuando se trata de una auditoría interna, se pone el nombre de la empresa y la identificación del área de auditoría interna responsable de hacer la evaluación. Igual que en el punto anterior.

8.3.1.3 Fecha de emisión del informe

Aquí se anota el lugar y la fecha de emisión del informe de auditoría; esto sirve para indicar la oportunidad con la que se entrega o remite dicho informe. Se debe poner la fecha con las reglas elementales de cortesía; es decir, lugar, día, mes y año o el formato que se prefiera, siempre y cuando tenga la fecha completa.

8.3.1.4 Identificación de la empresa o área auditada

En esta parte del oficio se señala, lo más detalladamente posible, el nombre completo de la empresa, del área de sistemas o del aspecto específico que haya sido evaluado.

8.3.1.5 Ejecutivo receptor del informe

Por lo general, este informe se remite a un ejecutivo de alto nivel de la empresa auditada, para su información y toma de decisiones. Algunas veces pude ser enviado al funcionario responsable de autorizar la auditoría.

Los grados académicos, puesto y nombre del ejecutivo van anotados con las reglas elementales de cortesía.

8.3.1.6 Período de la evaluación

En esta parte se anotan las fechas de inicio y terminación de la auditoría; con esto se busca darle a conocer al lector del informe el espacio de tiempo que comprendió la evaluación. El propósito de presentar este período es darle validez y vigencia a la revisión.

8.3.1.7 Contenido (o cuerpo del oficio)

Es una breve descripción de los puntos que fueron evaluados y de los aspectos que integran el informe. Se debe redactar en forma muy esquemática, con ortografía impecable y sin abusar de la extensión ni de la brevedad.

Si es necesario, se puede hacer, en forma muy breve y lo más concreto posible, un avance sobre el resultado de la auditoría, sin entrar mucho en detalles, pero con la suficiente claridad para que se entienda, de acuerdo al nivel de funciones de quien leerá dicho informe.

8.3.1.8 Responsable de emitir el dictamen

En esta parte se anota el nombre del profesional responsable de emitir el informe de auditoría, que será quien avale y responda, si es el caso, por los resultados de la evaluación, por el propio dictamen o quien hará las aclaraciones que se requieran. En el caso de una auditoría externa, se anota el nombre del responsable de la empresa encargada de realizar la auditoría, y en el caso de una auditoría interna, el nombre del responsable del área de auditoría interna.

En cualquiera de los casos, se debe poner el nombre de un profesional autorizado para emitir el informe y dictamen de auditoría.

8.3.1.9 Firma del responsable

En esta parte se pone la firma autógrafa del responsable de la auditoría, que es la persona que adquiere el compromiso de avalar lo reportado en el informe.

8.3.2 Introducción del informe de auditoría de sistemas computacionales

Es la parte del informe donde el responsable de la auditoría hace la presentación formal de su trabajo; en este apartado se manifiesta el objetivo de la auditoría, las razones que motivaron a llevarla a cabo (*en la sección 6.3 del capítulo 6 analizamos el origen de la auditoría*) y, si es el caso, los fundamentos que apoyen su realización. En algunas ocasiones también se pueden indicar la metodología y las herramientas utilizadas en la evaluación de los sistemas, aunque esto último no es forzoso.

Debemos señalar que no existen reglas específicas para elaborar esta introducción; sin embargo, se puede establecer como única regla que su redacción debe ser impecable y debe tener una excelente presentación, ya que es la primera parte que se lee del informe de auditoría. La introducción es frecuentemente la invitación a seguir leyendo el resto del informe; sin embargo, cuando esta parte está mal redactada, crea rechazo casi inmediato para seguir adelante con la lectura.

Debido a lo anterior, a continuación presentamos una serie de sugerencias que ayudarán al auditor y al responsable del informe a mejorar la elaboración de dicha introducción. Debemos aclarar que los puntos que analizaremos a continuación no son apartados de la introducción, y sólo se presentan para que el lector los identifique, pero no se deben anotar en el informe:

8.3.2.1 Aspectos generales

Iniciar la redacción de la introducción como si fuera una narración de lo que el lector encontrará en el informe; en este sentido, se recomienda comenzar con la exposición concreta del objetivo general de la auditoría, y continuar con el planteamiento de la metodología utilizada en la evaluación de los sistemas. Finalmente, si fuera necesario, concluir con un relato sintetizado de lo que el lector encontrará en dicho informe. Esto último no es tan recomendable, porque haría engorrosa la lectura.

La introducción tampoco debe ser muy amplia, sino en pocas hojas (de 1 a 3) muy bien redactadas y directamente enfocadas a los tópicos que se tratarán en el informe. Evidentemente, la ortografía y acentuación cuentan mucho en el ánimo del lector; esta parte es lo primero que lee y, por lo mismo, lo primero que juzga y le da pie para aceptar o rechazar el contenido del informe.

A continuación presentaremos algunos aspectos que el auditor puede considerar como guías en la redacción de la introducción de su informe, aclarando que estos puntos los analizaremos por separado, pero en la redacción de la introducción se deben presentar sin separaciones y sin títulos:

Prólogo

Es una breve descripción en la que el auditor presenta su trabajo, para que el lector sepa lo que encontrará en el informe; el prólogo se debe hacer en forma narrativa, sencilla y simple, y no debe ser muy extenso.

Objetivo

Es la definición del fin último que se pretende satisfacer con la auditoría; esta definición se debe redactar en forma sencilla, concreta y contemplando las siguientes reglas:

- *Iniciar el objetivo con un verbo en infinitivo*
- *Determinar primero el qué se quiere, y después el para qué se hace.*
- *Limitar la redacción a frases sustantivas.*

Se pueden plasmar varios objetivos, pero deben ser en relación a la importancia de la auditoría.

Justificación

Esto significa plantear en forma resumida y concreta los motivos por los cuales se realizó la evaluación de los sistemas computacionales, los cuales pueden ser de carácter

impositivo, por necesidad profesional, por interés de algún directivo o por cualquiera de los motivos señalados en el origen de la auditoría, mismos que analizamos en la metodología del capítulo VI.

Con esto se busca que el auditor se anticipe y conteste estos interrogantes:

- *¿Para qué? (se hizo la auditoría)*
- *¿Por qué? (se tuvo que llevar a cabo)*
- *¿Cuál fue la profundidad? (de la evaluación)*
- *¿Hasta dónde se profundizó? (en su cobertura)*
- *¿Por qué se auditó? (para analizar su alcance)*

Metodología utilizada

Aunque no es muy recomendable señalar este punto en la introducción, se puede dar el caso de que sea necesario hacer la descripción de las herramientas, métodos, técnicas y procedimientos de auditoría de sistemas utilizados durante la evaluación. De llegar a plantearlo, se debe procurar que su presentación sea lo más resumida posible, sin tanto detalle y sin hacer una descripción abultada de cada una de las herramientas utilizadas. Sólo se debe señalar a grandes rasgos lo utilizado.

Narrativa por capítulos

Esta parte de la introducción del informe de auditoría es muy poco usual; sin embargo, en caso de que se necesite, se refiere a la relatoría de lo que encontrará el lector del informe; dicha descripción tiene que ser concreta y sólo debe incluir lo más importante del contenido del informe. No es un resumen anticipado de lo que se anota en el informe, ni es la presentación breve del diagnóstico, sino la presentación de lo que encontrará el lector.

Debemos reiterar que la introducción del informe de auditoría, en caso de existir, se tiene que redactar de una forma simple y sencilla, con muy buena ortografía, evitando repeticiones inútiles y rebuscamientos que a nada conducen. Esta parte es la que hace que el lector se interese en leer lo que sigue o, por el contrario, que evite leerlo o que lo haga de manera forzada.

8.3.3 Dictamen de la auditoría de sistemas computacionales

Tal vez ésta sea la parte más importante de una auditoría de sistemas computacionales y, en muchas ocasiones, lo que más esperan los directivos de la empresa o del área auditada, debido a que es una opinión profesional respecto al comportamiento de los sistemas. Evidentemente, el dictamen está apoyado en la experiencia y conocimientos del auditor en las áreas de auditoría y sistemas, así como en la confianza del uso de las herramientas e instrumentos apropiados.

Cada empresa de auditoría o auditor que elabora un dictamen debe emitir su opinión de acuerdo con su costumbre, experiencia o según los requisitos de la empresa

auditada; sin embargo, por la importancia que tiene este informe en el área de sistemas, o en cualquier otra área, a continuación presentaremos un formato de dictamen y algunas recomendaciones para emitirlo de una mejor manera.

8.3.3.1 Presentación del dictamen

Éste es un documento de carácter formal que debe cumplir con los requisitos oficiales de presentación que ya señalamos, además de los que indicaremos a continuación (vea la figura 8.4):

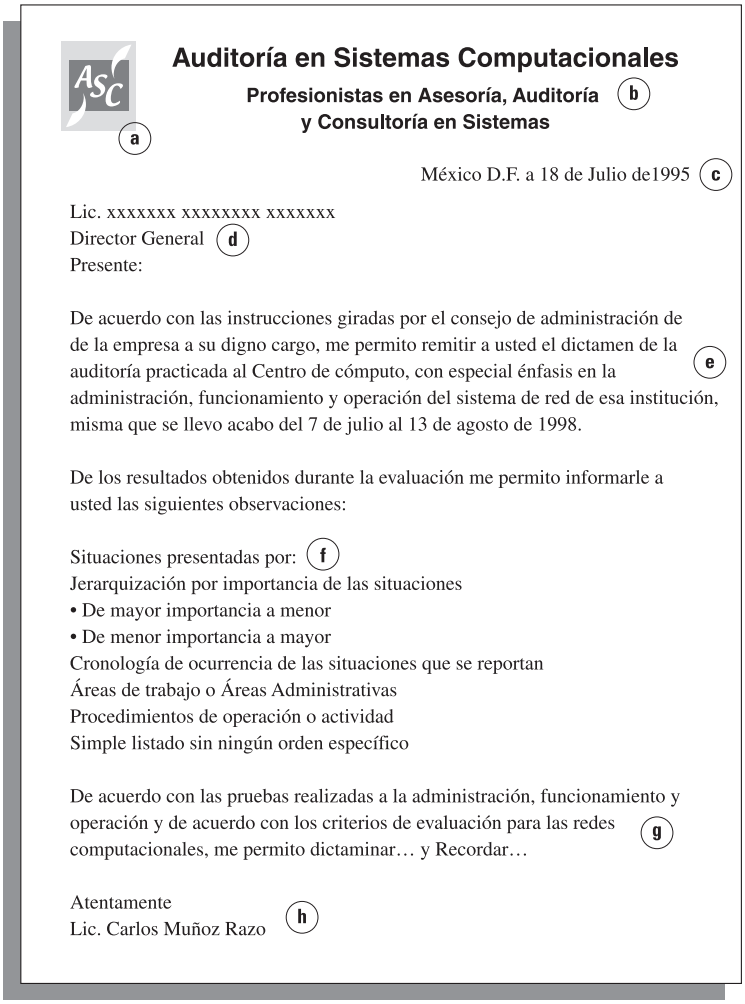


Figura 8.4 *Dictamen de auditoría.*

a) Logotipo de identificación:

En esta parte se pone el logotipo de la empresa responsable de emitir el dictamen de la auditoría, ya sea de auditoría externa o interna, como lo señalamos en la sección 8.3.1 de este capítulo. En cualquiera de los casos, este documento siempre debe llevar el logotipo, el cual se puede colocar de acuerdo al diseño de la documentación oficial.

b) Nombre de la empresa (o área interna de auditoría)

En esta parte se anota el nombre de la empresa o del área responsable de hacer la auditoría, ya sea auditoría externa o interna, y debe ir junto al logotipo de la empresa.

c) Fecha de emisión del dictamen

En este punto se anota el lugar y la fecha de entrega del dictamen, lo cual sirve para indicar la oportunidad con la que se entrega o remite dicho dictamen, conservando las reglas elementales de imposición de fechas; como si fuera cualquier otro oficio de presentación o correspondencia comercial.

d) Ejecutivo receptor del dictamen

En esta parte se anota el nombre y cargo del funcionario de alto nivel a quien se remite el dictamen. Algunas veces, el dictamen puede ser enviado al funcionario que autorizó la realización de la auditoría.

Se deben respetar los grados académicos, puesto y nombre del ejecutivo, y anotarlos con las reglas elementales de cortesía comercial.

e) Breve introdución al dictamen

En esta parte se anotan las razones que dieron origen a la auditoría, quién la ordenó, el área, sistema y actividades sujetas a evaluación, y las fechas de inicio y terminación la auditoría; con esto se busca presentar al lector todos los aspectos fundamentales del porqué de la auditoría.

f) Contenido del informe de auditoría

En esta parte del dictamen se hace una breve descripción de los puntos que fueron evaluados, describiendo en forma clara, y lo más resumida posible, los aspectos que se consideran como observaciones y desviaciones sobre los asuntos auditados. Mas específicamente, es el diagnóstico resumido del resultado de la auditoría, sin muchos detalles, pero lo suficientemente contundente, conciso, claro y comprensible para que los lectores lo entiendan. El contenido del dictamen debe ser redactado en forma impecable, debe ser muy esquemático, con ortografía intachable y no debe ser ni muy extenso ni muy corto.

El propósito fundamental de esta parte del dictamen es informar, de manera resumida, a los funcionarios de la empresa sobre las observaciones y los resultados obtenidos en la auditoría. Además, por necesidades del dictamen, se pueden presentar las

situaciones, observaciones y desviaciones encontradas, así como sus causas y soluciones; pero se deben presentar en forma muy breve y resumida, pero sin omitir lo más importante, a fin de que los lectores del informe entiendan en pocas líneas la importancia de lo que se reporta.

Las desviaciones se pueden presentar de diversas formas, de acuerdo con las necesidades del dictamen, la experiencia del auditor o la importancia de lo que se quiere reportar; lo anterior se puede hacer de las siguientes formas:

f.1) Jerarquizando las situaciones por importancia

Presentar las desviaciones, observaciones o situaciones de esta manera tiene por objeto dar una cierta jerarquía, la cual establece el auditor en forma arbitraria de acuerdo a su conveniencia, buscando con ello hacer la presentación de esas situaciones más entendible y con un mayor impacto, y buscando que el lector del informe capte la importancia de la información que reporta. Esta organización se puede hacer de dos formas:

De mayor importancia a menor
Es cuando se jerarquizan las situaciones reportadas, iniciando por las de mayor importancia para terminar con las de menor importancia, de acuerdo al criterio del auditor.

De menor importancia a mayor
Es cuando se jerarquizan las situaciones reportadas en forma inversa, iniciando por las de menor importancia para concluir con las de mayor importancia.

f.2) Cronología de ocurrencia de las situaciones reportadas

Otro criterio para presentar las situaciones encontradas, es siguiendo un cierto orden cronológico de ocurrencia de las desviaciones; aquí se sigue un criterio de sucesión ordenada de acontecimientos concretos, considerados como desviaciones, conforme éstos se fueron presentando; otro criterio es atendiendo la forma en que se fueron detectando estas desviaciones; igual puede ser el ciclo de eventos informáticos que se presentan como deficiencias de la operación normal, o cualquier otro tipo de ordenamiento de carácter cronológico que el auditor aprovecha para establecer un orden de presentación de las desviaciones que detectó.

f.3) Áreas de trabajo o áreas administrativas

Las situaciones reportadas también se pueden ordenar utilizando la estructura de organización establecida en las áreas de sistemas de la empresa auditada.

En este acomodo se sigue el mismo ordenamiento que tienen las áreas de sistemas, de acuerdo al mismo criterio que se adoptó para su establecimiento, pudiendo presentar las desviaciones con alguno de los criterios analizados anteriormente.

f.4) Procedimientos de operación o actividad

También se puede hacer una presentación de las situaciones reportadas siguiendo el mismo orden en el que se desarrollan las actividades, funciones u operaciones norma-

les del centro de cómputo auditado; para esto, el auditor informa las desviaciones de acuerdo al proceso que se sigue en la operación normal del área y, dentro de este mismo, también puede utilizar otros criterios. Un criterio que sirve como ejemplo para esta presentación es el ciclo de vida de los sistemas:

- *Análisis del sistema actual*
- *Diseño del nuevo sistema*
- *Codificación del sistema*
- *Pruebas y correcciones*
- *Instalación y liberación del sistema*
- *Mantenimiento*

f.5) Simple listado sin ningún orden específico

En esta forma de presentación no se sigue ningún orden específico, sino que las situaciones que se reportan se presentan una tras otra, sin mediar ningún criterio, sin jerarquizar ni ordenar de manera alguna, sólo se presentan en un simple listado. Esto, aunque no es lo usual, también es válido y muy socorrido por los auditores principiantes.

f.6) Otros criterios de presentación

Aquí el auditor utiliza su propio criterio, de acuerdo con un ordenamiento elaborado, basándose en su experiencia, conocimientos, en las necesidades de la empresa auditada o en cualquier otro criterio de presentación diferente a los señalados anteriormente.

g) Dictamen y recomendaciones del auditor

Después de haber señalado en forma resumida cada una de las situaciones que se reportan como desviaciones, el siguiente apartado del dictamen de la auditoría corresponde a la opinión que el del auditor emite sobre los sistemas computacionales auditados. En este espacio asienta su opinión profesional, de manera objetiva, libre de cualquier influencia y con estricto apego a las pruebas y resultados observados durante la evaluación.

Esta parte es quizá la más importante de la auditoría y, en muchas ocasiones, lo que está esperando el receptor del informe, ya que es donde el responsable de la auditoría emite su juicio profesional a fin de dictaminar sobre el funcionamiento de los sistemas evaluados.

Aquí existen reglas bien claras y específicas cuando se trata de auditorías de tipo fiscal y financiero, pero en el caso de la auditoría de sistemas computacionales, aún no hay regulaciones concretas que normen la actividad de este especialista de la auditoría; sin embargo, es bueno repasar lo señalado en las normas, obligaciones y criterios ético-profesionales del auditor (*tratados en el capítulo 3*).

Lo que sí conviene recordar y recalcar, es que el dictamen emitido por el auditor conlleva una responsabilidad profesional y de carácter legal y penal; además, es la parte más importante de una auditoría de sistemas computacionales.

h) Responsable de emitir el dictamen

La última parte del dictamen de auditoría lleva el nombre, puesto y título del responsable de emitir el dictamen, además de su firma autógrafa.

Conviene finalizar la exposición del dictamen de auditoría señalando que no existe un límite específico para su tamaño; sin embargo, es recomendable que no pase de 4 páginas y que su contenido esté muy sintetizado, destacando sólo lo más sustancial de la evaluación, pero sin ser parco ni restringido. *Recordemos que este documento es la presentación formal del informe final de la auditoría y la opinión profesional del auditor*. Sobra decir que la ortografía, redacción, presentación y mecanografía deben ser impecables y sin un solo error.

8.3.4 Situaciones relevantes

Parte fundamental del informe de auditoría son los formatos de *situaciones relevantes;** éstos son los documentos oficiales donde el responsable de la auditoría reporta las desviaciones que, según su criterio, son las más importantes encontradas durante el desarrollo de la auditoría.

Estos formatos se anexan para posibles aclaraciones y consultas de las desviaciones que se reportan en el dictamen; aunque, cabe recordar, el auditor ya debió comentar este documento con los directivos del área de sistemas, como indicamos al principio de este capítulo (sección 8.1).

Aquí solamente mencionamos la existencia de este formato en el informe, ya que en la siguiente sección analizaremos su contenido, así como la forma de elaborarlo.

8.3.5 Situaciones encontradas

Como parte complementaria del formato anterior, también se puede integrar en el informe de auditoría de sistemas computacionales el *formato de situaciones encontradas,*** que es donde se concentran todas las desviaciones encontradas durante la evaluación. Su inclusión en el dictamen es a criterio del responsable de la auditoría, debido a que sería muy improbable que los receptores del informe final, generalmente altos funcionarios de la empresa, tomen en cuenta el análisis de este documento. Además, este formato dio origen al de situaciones relevantes y este último dio pie a la elaboración del dictamen de auditoría. Por ello se consultaría muy esporádicamente.

También debemos recordar que el auditor ya debió comentar este documento con los responsables directos de la operación, actividad o área auditadas; incluso convie-

* En la sección 7.1.4, del capítulo 7, mostramos el formato para estas situaciones, y en la siguiente sección de este capítulo lo analizaremos detalladamente.

** En la sección 7.1.5, del capítulo 7, mostramos el formato para estas situaciones, y en la siguiente sección de este capítulo lo analizaremos detalladamente.

ne recordar que esos comentarios le sirvieron al auditor para ratificar o rectificar las observaciones emitidas.

Aquí tampoco indicamos ejemplos ni mayor información sobre este formato, debido a que también lo analizaremos en la siguiente sección.

8.3.6 Anexos

Una última parte que puede contener el informe de auditoría de sistemas computacionales son los anexos, los cuales son documentos en forma de gráficas, cuadros, declaraciones o cualquier otro formato que servirá de soporte para las desviaciones reportadas en el informe final. No es obligatorio incluirlos, pero sí es conveniente, debido a que se podría necesitar de estas aclaraciones significativas, pues a veces el lector del informe no capta lo que se informa y, para su buen entendimiento, requiere de apoyos ilustrativos, gráficos y cuadros, donde se enfatizan o aclaran las desviaciones reportadas.

Cabe señalar que no existe ningún criterio establecido para la presentación de estos anexos; sólo el criterio del responsable de la auditoría, así como su experiencia en la elaboración del informe. Éstos serán los principales parámetros que deberá seguir el auditor.

8.3.7 Confirmaciones en papeles de trabajo

Este documento no se debe integrar al informe final de la auditoría, sin embargo, al presentar el informe a los directivos, es muy conveniente que el auditor tenga a la mano *el legajo de papeles de trabajo*, ya que podría necesitar hacer aclaraciones importantes de lo reportado; entonces puede recurrir a las pruebas documentadas en este legajo. De ahí la importancia de llevarlo.

8.4 Formatos para el informe de auditoría de sistemas computacionales

Existen muchas formas de reportar las desviaciones que se detectaron durante una auditoría de sistemas computacionales, que se presentan de acuerdo con las preferencias, experiencia, conocimientos y necesidades del responsable de hacer la auditoría. Incluso, en muchas ocasiones las empresas externas dedicadas al trabajo de auditoría, tienen establecidas sus propias formas de reportar las observaciones, estandarizando así la forma de elaborar sus informes de auditorías.

Para este libro hemos adoptado dos formatos que, a criterio de este autor, son los más funcionales, tanto por la forma en que ayudan a reportar las situaciones encontradas en la auditoría, como por la facilidad con que el lector entiende lo que se está informando en estos documentos. Debo aclarar que durante mi entrenamiento inicial como auditor y posterior responsable de esta especialidad, así como en la frecuente

exposición de esta materia en aulas universitarias y conferencias, siempre he constatado comprobar la utilidad de dichos formatos. Además, he comprobado que facilitan la forma de reportar las desviaciones observadas en la evaluación. También sirven para enseñar a los auditores principiantes a elaborar informes de auditoría, pues son fáciles de llenar y comprender. A continuación presentamos dichos formatos:

- *Formato de situaciones encontradas*
- *Formato de situaciones relevantes*

8.4.1 Formato de situaciones encontradas

Este documento, que es uno de los documentos más importantes para el desarrollo de cualquier auditoría de sistemas, es un formato especial para la recopilación de situaciones o desviaciones encontradas, el cual está formado por una serie de hojas (formatos individuales) en las cuales el auditor anota en manuscrito o tipografía todas las desviaciones que encuentra durante su evaluación.

Este formato, en forma individual, tiene seis columnas básicas en las que se anotan los siguientes asuntos:

- **La referencia:** *es un número consecutivo, combinado o marca especial, mediante el cual se identifica la situación a tratar.*
- **Las situaciones detectadas:** *específicamente, es la descripción de lo que se encontró en un determinado punto de la evaluación, según las pruebas, procedimientos o técnicas de evaluación utilizados para hacer la revisión; cada una de estas desviaciones es parte importante del documento.*
- **Las causas:** *es la presentación de los motivos e imputaciones que originaron la desviación y puede ser una sola causa o varias las que ocasionaron esta desviación, todas se anotan, a criterio del auditor.*
- **Las posibles soluciones:** *son sugerencias del auditado o del auditor para solucionar las desviaciones reportadas. Casi siempre corresponde una solución para cada una de las causas reportadas.*
- **Fecha de compromiso:** *es el período o la fecha tentativa para implantar la solución acordada. Se anota una fecha para cada solución propuesta.*
- **Responsables de las soluciones:** *son los funcionarios, empleados o cualquier persona responsable de implantar las soluciones. También se acostumbra anotar un responsable por cada solución, aunque a veces parezca repetirse el mismo responsable.*

A continuación veremos un formato de presentación para las situaciones encontradas (vea la figura 8.5), el cual servirá de base para las aplicaciones que haremos de una auditoría de sistemas computacionales:

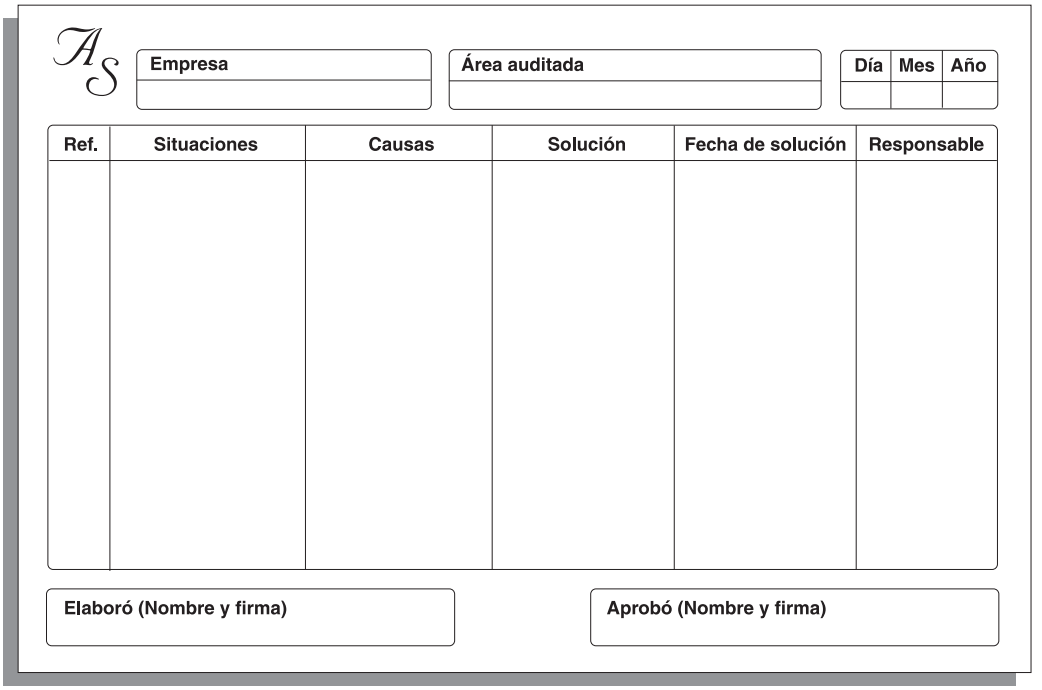


Figura 8.5 *Formato de situaciones encontradas.*

8.4.1.1 Identificación (en la parte superior izquierda del formato)

Es el lugar en donde se anota el nombre de la empresa auditora, ya sea el de la empresa que hace la auditoría, si es auditoría externa, o el de la institución, si es auditoría interna. Si es necesario, también lleva el logotipo, cargado en la parte superior izquierda.

8.4.1.2 Área auditada (en la parte central del formato)

Es el lugar en donde se anota la dependencia, área de informática, sección o unidad administrativa de sistemas evaluada. Lo que se pretende con esta identificación, es que se tenga bien claro cuál es el ambiente de trabajo donde se presentaron las desviaciones.

8.4.1.3 Fecha de evaluación (en la parte superior derecha)

En este espacio se anota la fecha en que se presenta la evaluación, con el formato día, mes y año. En algunos casos puede ser el día, mes y año en que inicio el período de la evaluación, y el día, mes y año en que concluyó. Ambos son válidos, pero deben llevar el año con cuatro dígitos.

8.4.1.4 Número de referencia (columna 0)

Es el número progresivo que se le asigna a la desviación reportada; de preferencia se asigna en forma continua, para que sirva como referencia para localizar cada desviación. Esta columna también se podría modificar, de acuerdo con las necesidades de presentación de las observaciones, e incluso se podría eliminar, según el criterio del auditor. También se puede adoptar una numeración especial, que puede ser por importancia de las desviaciones, por área de evaluación (este último punto conforme al ejemplo del índice señalado en la sección 7.1.2 del capítulo 7) o cualquier otra numeración, de acuerdo con las características de presentación de dicho documento.

8.4.1.5 Situaciones encontradas (columna 1)

En esta primera columna se anotan, una por una y de manera clara, sencilla, y completa, aquellas situaciones o desviaciones encontradas en el punto que se está evaluando. Presentado el asunto lo más concreto, directo, preciso y descriptivo posible.

El objetivo es señalar, de la mejor manera posible, los aspectos que se han encontrado en la evaluación, y describir la desviación o la situación anormal que se observa.

En dicha columna es preferible anotar, una a una, todas las situaciones y desviaciones encontradas, por mínimas que sean, sin importar su relevancia, frecuencia o cualquier otro concepto; lo importante es señalar todas las posibles desviaciones. Recordemos que son papeles de trabajo y que el auditor seleccionará posteriormente las desviaciones más relevantes. También se pueden anotar las situaciones positivas, si el auditor lo considera importante; esto último es recomendable.

8.4.1.6 Causas de la situación (columna 2)

En la siguiente columna, a la altura de la presentación de cada situación, se anotan las posibles causas que originan la desviación; las causas deben ser reales y deben estar plenamente identificadas y comprobadas, es decir, se deben presentar los antecedentes que sean los verdaderamente causantes de la desviación reportada. No es válido inventar causas sin tener su soporte ni evidencia.

Cada situación detectada puede tener una o varias causas. Lo realmente importante es que el auditor resalte las causas que originan la desviación encontrada. Esto es lo que se busca con la auditoría, presentar las desviaciones y lo que las originó, a fin de corregirlas.

Como ya señalamos, es requisito indispensable presentar las verdaderas causas de las situaciones detectadas durante la auditoría, sin emitir, inventar ninguna, ni tampoco hacer suposiciones, sino presentar sólo las realidades que han sido previamente comprobadas; el propósito es que, al contar con las verdaderas causas, se puedan emitir soluciones acordes a la problemática presentada. Si se parte de orígenes supuestos,

entonces se enmendarán problemas supuestos, no reales, y las verdaderas desviaciones no se podrán solucionar y seguirían las mismas observaciones.

8.4.1.7 Soluciones propuestas (columna 3)

Una vez analizadas las situaciones detectadas y las causas que las originan, se podrá emitir la posible o posibles soluciones a esas situaciones. Pueden existir muchas soluciones para cada situaciones y todas se anotan en esta columna.

Cabe hacer notar que la presentación de las soluciones es opcional para el auditor, ya que se recomienda que éstas sean determinadas por el propio auditado, ya sea el responsable directo de la situación detectada, por alguno de sus superiores inmediatos o, en algunos casos, por su personal subordinado; todos ellos están más en contacto con la problemática presentada y, en consecuencia, tienen mejores elementos para solucionar esa problemática.

Cabe destacar que cada situación presentada puede tener una o más soluciones, y que le corresponderá al auditado proponer la solución o soluciones para resolver las situaciones; el auditor sólo se limitará a destacar la situación, detectar las causas que las originaron y presentar las soluciones que le proponen. No es válido ni ético que el auditor imponga soluciones y mucho menos que establezca compromisos de solución a nombre del auditado o de cualquier otra persona. *Se puede sugerir una solución, pero nunca imponerla*.

8.4.1.8 Fecha de compromiso para la solución (columna 4)

Es la formalización del compromiso contraído por el responsable de la solución. Dicha fecha se expresa en formato DD, MM, AAAA o en el que el auditor elija. Lo importante es que se determine una fecha compromiso, con un plazo más o menos razonable, dependiendo del alcance de la situación detectada.

8.4.1.9 Responsable de la solución (columna 5)

Aunque esta columna no es obligatoria, es preferible anotar lo más claramente posible al o los responsables de solucionar la situación presentada. Con ello se trata de ubicar y definir la responsabilidad en la solución; en caso de ser necesario, se determina quiénes serán los encargados de elaborar las alternativas de solución del problema presentado.

Tampoco es obligatorio seguir un formato específico para la presentación de los responsables de las soluciones, pero se recomienda que sea el de más alto rango del área auditada, ya que con ello se evita que se diluya la responsabilidad y un subordinado tiene menos posibilidades de tomar decisiones sustantivas que permitan solucionar la problemática presentada.

8.4.1.10 Elaboró la hoja de situaciones, nombre y firma (parte inferior izquierda)

Aquí se anota el nombre completo, el puesto y la firma autógrafa del auditor encargado de hacer la recopilación de la información y, por supuesto, de cada una de las situaciones reportadas, causas y soluciones presentadas en el formato. Esto se hace con el propósito de responsabilizar al auditor de sus opiniones, y de recurrir a él con facilidad cuando se necesite que haga cualquier aclaración sobre dichas observaciones. Es indispensable que siempre se cumpla este requisito; en caso de ser necesario, el nombre del auditor se puede cambiar por el del responsable de toda la auditoría.

8.4.1.11 Aprobó la hoja de situaciones, nombre y firma (parte inferior central)

Se anota el nombre del responsable de avalar, previo análisis, presentación y comprobación, las evidencias presentadas por el auditor subordinado. Con esto se busca verificar el trabajo del auditor y, de ser necesario, que el auditor y el responsable de la auditoría se hagan responsables de los resultados de la revisión practicada.

Para una mejor presentación de las situaciones, causas y soluciones planteadas, aunque sean documentos de uso exclusivo del auditor, y para evitar dudas sobre ellas, es necesario escribirlas a la misma altura en cada columna, sin importar su tamaño o extensión, también es preciso, por orden y comodidad, empezar cada nueva desviación un renglón abajo de la última frase que se haya escrito en cualquiera de las seis columnas.

Se hace énfasis en que este documento tiene que estar redactado en forma impecable y puede ser escrito a mano, en máquina o con impresora; lo esencial es que en su contenido se establezca en forma precisa la desviación que se observó, así como sus causas y sus posibles soluciones, sin aumentar conceptos ni minimizar lo encontrado; asimismo, el punto señalado debe ser claro, oportuno y exacto.

Para una buena redacción de este documento, sugerimos consultar lo relacionado con las características del informe de auditoría (*sección 8.2*) y aplicar los conceptos ahí señalados.

8.4.2 Formato de situaciones relevantes

Este documento es una réplica simplificada del formato anterior, sólo que en éste únicamente se anotan las situaciones consideradas como relevantes, resultado del análisis al documento anterior, es decir, sólo se incluyen aquellas observaciones que a juicio del auditor o del responsable de la auditoría son realmente importantes para el desarrollo de las actividades del área de sistemas evaluada.

Debemos insistir que en este documento sólo se presentan las situaciones más significativas detectadas durante la evaluación.

Es recomendable que las situaciones relevantes incluidas en este documento sean las mismas que las establecidas en el documento anterior, incluso con las mismas palabras, pero aquí no deben aparecer a mano sino impecablemente mecanografiadas. También se sugiere seguir el mismo orden planteado en el documento anterior. A continuación presentamos una propuesta del formato de situaciones relevantes, el cual servirá de base para las siguientes aplicaciones de auditoría de sistemas que haremos (vea la figura 8.6).

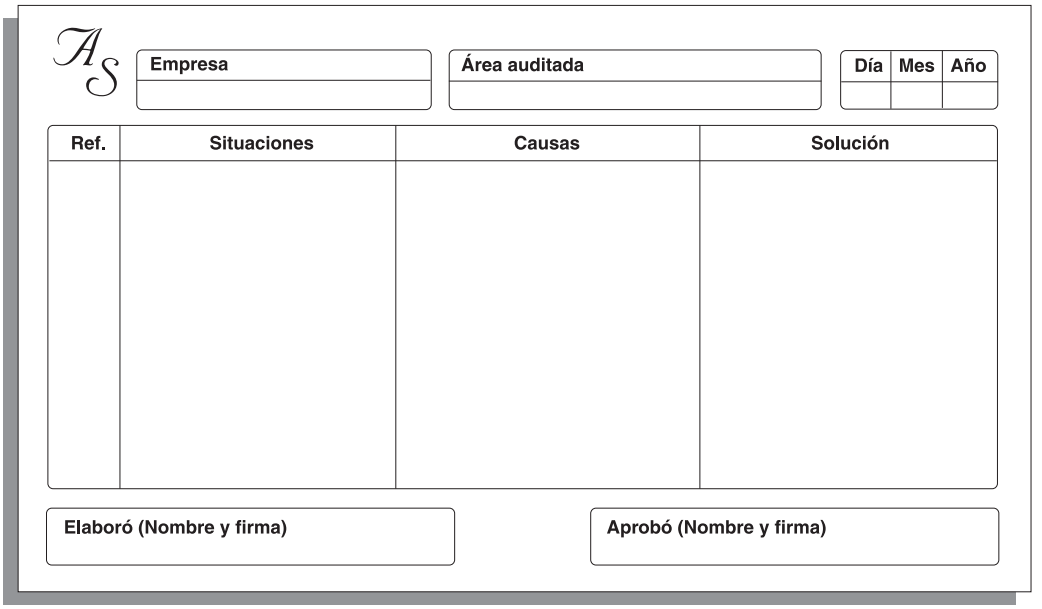


Figura 8.6 *Formato de situaciones relevantes*

Este formato, que también se elabora en forma individual, tiene tres columnas básicas en las cuales se anotan, exclusivamente en computadora o a máquina, los siguientes aspectos:

- **Las situaciones relevantes,** *que son lo que más se destacó en el documento anterior y que se determinó como lo más importante de destacar, según las pruebas, procedimientos y técnicas utilizados para hacer la evaluación.*
- **Las causas,** *que son los motivos de las desviaciones.*
- **Las posibles soluciones,** *que son las posibles soluciones para las desviaciones.*

8.4.2.1 Identificación (en la parte superior izquierda del formato)

Es el lugar en donde se anota el nombre de la empresa que hace la auditoría, si es auditoría externa, o el de la institución, si es auditoría interna. Si es necesario, también se pone el logotipo, cargado a la extrema izquierda.

8.4.2.2 Área auditada (en la parte central del formato)

En esta parte del formato se anota la dependencia, área de informática, sección o unidad administrativa de sistemas evaluada. El propósito de esto es que se tenga bien identificado el lugar de trabajo donde se detectaron las desviaciones.

8.4.2.3 Fecha de evaluación (en la parte superior derecha)

En este espacio se anota la fecha en que se presenta la evaluación, con el formato día, mes y año. En algunos casos se pueden poner las fechas de inicio y finalización de la auditoría.

8.4.2.4 Número de referencia (columna 0)

Es el número progresivo que se le asigna a la desviación, de preferencia en forma continua, para que sirva como referencia para localizar el punto deseado. Esta columna puede ser modificada de acuerdo con las necesidades de presentación de las desviaciones relevantes, y si fuera necesario se puede eliminar.

8.4.2.5 Situaciones relevantes (columna 1)

En esta primera columna se anotan las situaciones que, a criterio del auditor, son las más importantes de destacar de las presentadas en el documento anterior. Su redacción debe ser sencilla, objetiva y debe ir directamente al asunto que se encontró como desviación, presentando el asunto lo más claro, preciso y descriptivo posible.

La idea central de este punto es señalar, punto por punto, los aspectos más importantes encontrados durante la evaluación, y anotar (exclusivamente a máquina) la desviación o situación anormal observada.

Aquí es preferible anotar todas las situaciones y desviaciones consideradas como relevantes, por mínimas que sean su relevancia y sin importar su frecuencia ni cualquier otro concepto. Recordemos que este formato, al igual que el anterior, también es parte de los papeles de trabajo y que el auditor seleccionará de todas estas desviaciones las que le servirán para fundamentar su opinión profesional y elaborar su informe final de auditoría.

Es recomendable que la redacción de estas situaciones relevantes sean una copia fiel de las mismas situaciones identificadas en el formato de situaciones encontradas, a fin de no modificar ningún concepto ni permitir ningún error o alteraciones a éstas.

8.4.2.6 Causas de la desviación (columna 2)

En la siguiente columna se anotan las causas que originaron las desviaciones a la altura de la presentación de cada desviación; dichas causas deben ser las reales y estar plenamente identificadas y comprobadas. No es válido inventar causas ni hacer suposiciones, es decir, solamente se presentan las causas que realmente originaron la desviación.

Cada situación relevante puede tener una o varias causas. Lo realmente importante es destacar las causas que originan la desviación encontrada. Esto es lo que se busca con la auditoría, presentar las desviaciones y lo que las originó, a fin de corregirlas.

Al igual que en las situaciones relevantes, se recomienda anotar el mismo texto de las causas que se reportaron en el formato de situaciones encontradas, a fin de evitar posibles errores y alteraciones de estas causas.

8.4.2.7 Soluciones propuestas (columna 3)

Una vez analizadas las situaciones relevantes y las causas que las originaron, se podrá emitir la posible o posibles soluciones a esas desviaciones. Pueden existir muchas soluciones para cada desviación, y todas se deben anotar en esta columna, de la misma manera que en el *formato de situaciones encontradas*.

Cabe hacer notar que la presentación de las soluciones es opcional para el auditor, pues recomienda que éstas sean determinadas por el propio auditado, ya sea el responsable directo de la desviación detectada, por alguno de sus superiores inmediatos o, en algunos casos, por su personal subordinado, porque todos ellos están más en contacto con la problemática presentada y, en consecuencia, tienen mejores elementos para solucionarla.

Es muy importante recalcar que sólo se deben presentar las desviaciones que a criterio del auditor sean las más relevantes, tratando de destacar únicamente aquello que sea realmente sustantivo; también se pueden resaltar los aspectos positivos, según el criterio del auditor.

Al igual que en las situaciones relevantes y las causas de las mismas, se sugiere que las soluciones que se reportan en el presente formato sean una copia fiel de las mismas soluciones que se presentaron en el formato de situaciones encontradas.

9

Instrumentos de recopilación de información aplicables en una auditoría de sistemas computacionales

Estructura del capítulo:

Objetivos del capítulo

Identificar los principales instrumentos, técnicas, herramientas y métodos utilizados en la recopilación de información útil para realizar una auditoría de sistemas, fundamentados en las herramientas y métodos tradicionales de recopilación de información de las auditorías tradicionales; también utilizados en el análisis y diseño de sistemas, y las ciencias sociales, a fin de conocer su forma de aplicación y funcionamiento en las auditorías de sistemas computacionales y adaptarlos a las necesidades específicas del ambiente de sistemas que se requiere auditar.

Introducción del capítulo

El auditor debe aprovechar las técnicas, procedimientos y herramientas tradicionales de auditoría aplicables en el área de sistemas computacionales; el propósito es que las diseñe y las utilice para hacer una evaluación correcta del funcionamiento de dicha área, de la operación del propio sistema o de su gestión informática, beneficiándose con ello debido a la ya probada eficiencia y eficacia en otros tipos de auditorías, en las cuales se han conseguido buenos resultados.

Al utilizar estas herramientas, métodos y procedimientos en la auditoría de sistemas, lo que se hace es utilizar lo mejor de ellas para adecuarlas a las necesidades específicas de evaluación requeridas en el ambiente de sistemas; ya sea para evaluar la operación de los sistemas, en cuanto al hardware, software, instalaciones, comunicaciones, etcétera, o la gestión administrativa del área de sistemas, las metodologías de desarrollo de proyectos, entre otros muchos aspectos relacionados con los sistemas.

Es por ello que el auditor de sistemas, como profesional especializado en la rama de informática, debe saber cómo utilizar esta serie de técnicas específicas de las auditorías tradicionales que le ayudarán a evaluar mejor los diferentes aspectos del área que tenga que auditar. Además, estos métodos tradicionales no sólo se utilizan para evaluar el área de informática, sino también cualquier otra área ajena al ambiente de sistemas.

Para este libro, vamos a clasificar estas técnicas, métodos y procedimientos de revisión para el área de sistemas en tres grandes grupos:

Técnicas, herramientas y métodos útiles en la recopilación de información conveniente para la auditoría de sistemas computacionales (que trataremos en este capítulo).

Técnicas, métodos y procedimientos especializados para la evaluación de sistemas computacionales (que analizaremos en el siguiente capítulo).

Técnicas, métodos y procedimientos de apoyo para emitir los diagnósticos sobre los sistemas computacionales (que analizaremos en el capítulo 11).

9.1 Entrevistas

La principal actividad de un auditor, sin importar el tipo de auditoría que realice, es la recopilación de información sobre el aspecto que va a auditar, pues concentra y tabula esa información en cuadros y estadísticas, analiza sus resultados y emite un juicio sobre el aspecto que evaluó.

Una de las técnicas más utilizada por los auditores es la entrevista, ya que a través de ésta obtienen información sobre lo que auditará; además, bien aplicada, les permite obtener guías que serán importantes para su trabajo, e incluso, muchas veces se entera de *tips* que le permitirán conocer más sobre los puntos que puede evaluar o *debe analizar* y mucha más información.

La entrevista podría entenderse como *la recopilación de información que se realiza en forma directa, cara a cara y a través de algún medio de captura de datos,* es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando; en la aplicación de esta técnica, el auditor utiliza una guía de entrevista, la cual contiene una serie de preguntas preconcebidas que va adaptando conforme recibe la información del entrevistado, de acuerdo con las circunstancias que se le presentan y en busca de obtener más información útil para su trabajo.

9.1.1 Ciclo de la entrevista de auditoría

Es conveniente señalar que para realizar una entrevista adecuada es indispensable entender y seguir un procedimiento bien estructurado, cuya eficacia en las auditorías tradicionales y en las ciencias sociales, donde es muy utilizada esta técnica, está plenamente comprobada. Esto le servirá al auditor de sistemas computacionales para llevar a cabo una buena investigación, apoyado en una serie de preguntas previamente establecidas y enfocadas al objetivo de la entrevista; con este método se busca captar una mayor información sobre lo que se auditará; además, esta información es más valiosa que la que se puede obtener por medio de un cuestionario, una observación o cualquier otra técnica de auditoría.

El siguiente procedimiento es indispensable para realizar una buena entrevista:

Inicio
Apertura
Cima o clímax
Cierre

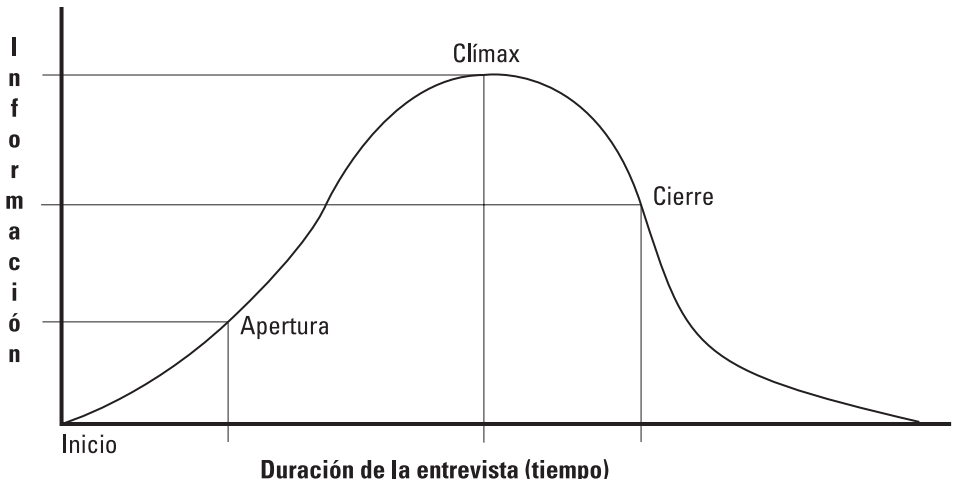
9.1.1.1 Inicio

Aquí es donde se inicia la entrevista, a través de una breve presentación con la cual se busca *romper el hielo*, y con una corta explicación del objetivo de la entrevista; si es necesario, aquí se hace la solicitud de cooperación por parte del entrevistado (personal auditado) para que éste proporcione la información requerida por el auditor.

En un ambiente puramente práctico, ésta es quizá la misión más difícil del auditor, ya que por la misma naturaleza de la misión que debe realizar (la de evaluar), lleva implícito el rechazo por parte de la persona a quien va a entrevistar; evidentemente, la apertura es un camino muy difícil bajo estas condiciones, pero es indispensable para el éxito en la aplicación de esta técnica. Algunas veces es importante iniciar con una breve plática informal o con algún tema de interés mutuo.

9.1.1.2 Apertura

También conocida como el inicio formal de la entrevista o despertar el interés del entrevistado, es la parte donde el auditor inicia formalmente su interrogatorio, con preguntas breves, simples y de sondeo, sin profundizar sobre algún tema en especial; el propósito básico de este punto es obtener posibles respuestas para iniciar la conversación, tratando de concentrar la plática sobre un tema de interés común entre el auditado y el auditor, de preferencia relacionado con el aspecto que se pretende evaluar.



Este punto, *la apertura de la entrevista*, es de suma importancia para el trabajo del auditor, pues aquí es donde inicia la conversación formal con el entrevistado, en el cual se busca evitar cualquier posible rechazo y resistencia de su parte; debemos tomar en cuenta que muchas veces el auditado está a la *defensiva, es evasivo y frío,* por lo que suele responder en forma vaga, evitando, hasta donde le es posible, proporcionar alguna información comprometedora para él o sus compañeros. Saber aplicar esta técnica de auditoría es quizás el trabajo más difícil para el auditor, ya que requiere de una amplia experiencia y habilidad, además de sólidos conocimientos sobre sus características, uso y formas de aplicación.*

9.1.1.3 Cima o clímax

Ésta es la parte de la entrevista en donde el auditor, con base en su habilidad y experiencia, obtiene la información medular para la investigación, la cual se va propiciando conforme el tema objeto de la entrevista adquiere mayor interés.

Con una buena aplicación de este punto, el auditor obtiene la información necesaria para evaluar las opiniones, comentarios y datos arrojados en la entrevista.

9.1.1.4 Cierre

Ésta es la parte final de la entrevista, en donde el auditor proporciona una absoluta libertad al entrevistado por si *puede* o *quiere* agregar algo que le permita complementar los datos antes recopilados; en muchas ocasiones, y más en la aplicación de una auditoría, ésta es una parte sustantiva, pues el entrevistado supone que la entrevista ya terminó; entonces, libre de presión, proporciona al auditor la información de mayor utilidad que le permite a este último confirmar, avalar o rectificar lo captado anteriormente. Además, mediante una hábil conducción del cierre, el auditor consigue *tips*, *comentarios* y *orientaciones* que le serán de mucha utilidad para continuar con la evaluación del aspecto auditado.

Evidentemente, en esta etapa se debe agradecer la participación del entrevistado.

La entrevista, a diferencia de otras técnicas y métodos de recopilación, requiere una amplia capacitación, conocimientos y experiencia por parte del auditor, así como un juicio sereno y libre de cualquier influencia para poder captar las verdaderas opiniones del entrevistado, y no agregar ni quitar nada de la información obtenida.

Además, a diferencia del cuestionario, la observación, el muestreo y otras técnicas y métodos de auditoría, en la entrevista no es fácil obtener datos cuantitativos medibles y tabulables, y después concentrar e interpretar dichos datos, debido a que se requiere un profundo análisis de los resultados obtenidos. Aunque en muchos casos, esta información verbal es más valiosa que la obtenida con otras herramientas.

* Para ampliar este punto, es recomendable analizar las formas de realizar la entrevista que aparecen más adelante en este capítulo.

La aplicación de esta herramienta exige una gran habilidad y experiencia del auditor, ya que el entrevistado siempre estará a la defensiva durante su desarrollo y, en muchas ocasiones, si no es adecuadamente conducida, será difícil que se obtenga información suficiente sobre algún tema relacionado con el trabajo del auditado.

9.1.2 Tipos de entrevistas para una auditoría

Hay dos tipos de entrevistas, las que se hacen de manera libre y espontánea, sin formalidades ni limitaciones, y las destinadas a la participación del entrevistado, mediante un método previamente establecido. Para el caso de la auditoría también podríamos agregar otros tipos de entrevistas, por ejemplo, las utilizadas para iniciar una evaluación, otras que sirven para corroborar y comprobar aspectos detectados con anterioridad o las empleadas para que el auditor informe o confronte los hechos y actores en determinadas situaciones. Concretamente, los tipos de entrevistas para la auditoría de sistemas computacionales serán los siguientes.

9.1.2.1 Entrevistas libres

Son las entrevistas en las que se sigue un guión básico para obtener la información requerida, pero la participación del entrevistado es libre y sin ninguna atadura. Con este tipo de entrevistas se pretende dar libertad al entrevistado para que se explaye; el propósito es tener una mayor intimidad en la plática para que la información sea más verídica y con más profundidad; aunque se corre el riesgo de que el entrevistado se aparte del tema central y pueda perderse en temas intranscendentes.

Es bueno utilizar este tipo de entrevistas para cualquier evaluación de sistemas, pues ayudan a que el auditado se extienda libremente en comentarios y aportaciones sobre lo que se está investigando, aunque se corre el grave riesgo de desviarse del tema sustantivo, deliberada o inconscientemente y que el entrevistado actúe casi siempre a la defensiva.

9.1.2.2 Entrevistas dirigidas

En estas entrevistas siempre se dirigen las opiniones del entrevistado, forzando sus respuestas dentro de un parámetro o guión prestablecido, sin admitir ni permitir ninguna variación significativa. Aquí, de acuerdo con la habilidad del auditor para conducir la entrevista, la participación del entrevistado puede llegar a tener mayor profundidad y la calidad de los datos, aunque se puede variar en cuanto a contenido y la utilidad de la información para la evaluación del auditor.

Este tipo de entrevistas es recomendable para rectificar o ratificar datos con el entrevistado, siempre que se establezca perfectamente el guión a seguir durante la entrevista.

9.1.2.3 Entrevistas de exploración

En una auditoría de sistemas es recomendable que el primer contacto con los auditados sea a través de este tipo de entrevistas, pues por lo general son de carácter libre y pueden ser muy útiles para buscar algún punto de partida para la evaluación. Además, ayudan al auditor a obtener información importante para explorar el contorno y apreciar los alcances que pudiera tener la revisión; también le ayudan a conocer el ambiente en el que se desarrollará la auditoría y como será la participación del entrevistado en la misma.

Las entrevistas de exploración también se hacen con la intención de familiarizar al auditor con los sistemas que va a evaluar, debido a que existen muchos tipos de sistemas, programas y paqueterías, utilizados en una institución de acuerdo con sus necesidades específicas; por esta razón, el auditor debe entender dichos sistemas para poder evaluarlos, y le ayudan a identificar el mejor punto de partida de la auditoría.

9.1.2.4 Entrevistas de comprobación

Estas entrevistas son de mucha utilidad para el auditor, ya que se realizan para comprobar la veracidad de la información recopilada durante la evaluación y permiten corroborar o rectificar los datos y percepciones sobre las observaciones encontradas con las pruebas e instrumentos aplicados en la auditoría; además, ayudan a profundizar en la evaluación, a reforzar su orientación o a cambiar el rumbo de la evaluación.

Este tipo de entrevistas requiere una amplia experiencia y conocimientos sobre las técnicas de entrevista, pues cuando se da este tipo de conversaciones, por lo general el auditado está a la defensiva y es difícil conducirlas, sin embargo, cuando se conducen bien, son muy útiles para ratificar o rectificar datos de una auditoría.

9.1.2.5 Entrevistas de información

En la metodología propuesta para desarrollar una auditoría de sistemas hablamos de la necesidad de comentar las observaciones con los auditados o con los funcionarios responsables del área de sistemas, según sea el caso; para eso se utiliza este tipo de entrevistas, para que el auditor comente cada una de las desviaciones que reporta en su informe, y con ello obtiene información valiosa del entrevistado que le sirve para rectificar o ratificar las situaciones que está informando, además le ayudan para recopilar datos útiles para encontrar las causas y soluciones que complementen sus observaciones.

No es fácil llevar a cabo este tipo de entrevistas, ya que requieren de mucha habilidad y experiencia por parte del auditor; recordemos que no es nada fácil comentar con el auditado las desviaciones de su trabajo o su responsabilidad en el manejo de los sistemas auditados. Sin embargo, es indispensable llevar a cabo estas entrevistas y realizarla de la mejor manera posible.

9.1.2.6 Entrevistas informales

Estas entrevistas son de suma importancia aunque propiamente no sean entrevistas de trabajo, ya que cuando el auditor las aplica de manera correcta, le ayudan a conocer algún tipo de problemática que sólo se expresa cuando no existe la presión de una entrevista formal como las indicadas anteriormente.

Por lo general, estas entrevistas son totalmente ajenas al ambiente de trabajo, casi personales y casi siempre son conversaciones informales que se dan entre personas para tratar temas sin importancia, sin embargo, el auditor aprovecha estos encuentros para conocer algún problema específico que pueda influir en la evaluación y que de otra manera no conocería.

9.1.3 Tipos de preguntas para entrevistas

Así como señalamos los tipos de entrevistas que se pueden realizar, también es necesario que demos a conocer los tipos de preguntas y la manera en que se pueden plantear éstas durante una entrevista; estas preguntas se hacen de acuerdo con las necesidades y características de cada entrevista, y se pueden agrupar en los siguientes tipos.

9.1.3.1 Preguntas abiertas

Las entrevistas realizadas con este tipo de preguntas son aquellas donde el entrevistado tiene la libertad absoluta para expresar su opinión sin ningún límite, aunque a veces se salga del tema que se le plantea.

El auditor de sistemas que aplique esta técnica debe saber aprovechar este tipo de preguntas, pues si las emplea correctamente, puede obtener información muy valiosa para su evaluación; además, si sabe motivar al entrevistado, éste le puede proporcionar información valiosa que puede validar posteriormente con otro tipo de herramientas de auditoría de sistemas.

9.1.3.2 Preguntas cerradas

Las entrevistas desarrolladas con preguntas cerradas (o concretas) se realizan con el propósito de centrar las respuestas del auditado hacia el objeto de la entrevista, sin dejarlo salir del tema. Este tipo de preguntas puede ser de mucha utilidad para el auditor, pues le ayudan a limitar las respuestas hacia el tema central de la entrevista.

9.1.3.3 Preguntas de sondeo

Este tipo de preguntas se puede hacer al inicio o durante el desarrollo de la entrevista, y se utiliza para determinar el grado de cooperación y participación del auditado durante la misma; el propósito es averiguar la manera en que el auditado colabora en

responder a estos interrogantes. El auditor debe utilizar este tipo de preguntas principalmente para comprobar la veracidad de las respuestas del auditado y así estar en condiciones de medir su grado de cooperación, o también las puede utilizar para obtener mayor información.

9.1.3.4 Preguntas de cierre

Antes de concluir la entrevista es importante realizar las llamadas preguntas de cierre, las cuales se hacen para terminar con el interrogatorio y como una forma de obtener información adicional de último momento; esta información surge al cerrar la entrevista, cuando el entrevistado, libre de la presión de la misma, proporciona información muy útil para normar criterios de evaluación o corroborar datos.

Debemos hacer notar que estas preguntas pueden ser de las más trascendentales en la recopilación de la información necesaria para la evaluación de los sistemas, pues el auditor puede aprovechar que el entrevistado deja de estar a la defensiva porque cree que la entrevista ya terminó, y puede proporcionar información muy valiosa para la evaluación.

9.1.3.5 Preguntas mixtas

Es la combinación de dos o más de los tipos de preguntas anteriores, para tratar de hacer más ágil y eficiente la recopilación de la información necesaria para la auditoría. El auditor debe saber elaborar este tipo de preguntas para aprovechar las posibilidades de la entrevista.

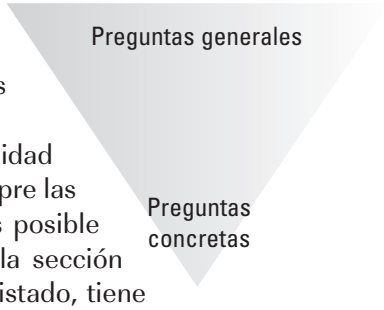
Conviene finalizar el tratamiento de este tema, haciendo énfasis en la aplicación de estos tipos de preguntas, a fin de que el auditor pueda obtener información valiosa que pueda corroborar posteriormente con otras herramientas de auditoría, pero lo importante es que sepa utilizar dichos tipos de preguntas como un eficaz instrumento de captación de información.

Es muy aconsejable que el auditor inicie la recopilación de información para una evaluación mediante una entrevista, sea formal o informal, y que después compruebe la información que obtuvo en esa entrevista, y posteriormente haga una nueva entrevista para corroborar cada observación importante.

9.1.4 Formas de realizar una entrevista para una auditoría de sistemas

La entrevista es una de las herramientas que más ayudan al auditor en una evaluación, debido a que le permite obtener la llamada información de primera mano y, en muchos casos, facilita la comprobación de fenómenos ya contemplados con anterioridad. Sin embargo, la entrevista debe aplicarse mediante una estructura concreta y una adecuada técnica de conducción. Básicamente hay cuatro técnicas de conducción, mismas que presentamos a continuación.

9.1.4.1 Entrevistas tipo embudo



El auditor inicia este tipo de entrevistas con preguntas de carácter general (abiertas), y conforme avanza la plática va haciendo preguntas más concretas (cerradas), enfocadas hacia el tema que le interesa.

En este tipo de entrevistas se requiere cierta habilidad y experiencia por parte del auditor, debido a que siempre las debe iniciar con preguntas de carácter general, si es posible alejadas del tema central (la apertura señalada en la sección 9.2.1), y conforme va logrando la apertura del entrevistado, tiene que centrar las preguntas hacia aspectos más concretos que sean de su interés; como si fuera un embudo o pirámide invertida, que inicia con lo más general y termina con lo particular y concreto.

Es recomendable utilizar este tipo de entrevistas para vencer la resistencia de los auditados que están a la defensiva. Además, se pueden utilizar para corroborar información captada con anterioridad.

9.1.4.2 Entrevistas tipo pirámide

Estas entrevistas también son fundamentales para recopilar información en la auditoría de sistemas, pero se estructuran en forma inversa a la anterior, es decir, inician con preguntas cerradas (concretas) y conforme avanza la charla se van haciendo las preguntas de carácter general con las cuales se obtiene abundante información. Cuando se utiliza esta técnica siempre se debe finalizar con una pregunta abierta.

El auditor siempre comienza la entrevista tipo pirámide empleando una pregunta cerrada muy concreta y a veces directa, con la que, de acuerdo con su experiencia, conocimientos y habilidad, obtiene datos útiles para la evaluación, y conforme recibe cada respuesta formula las siguientes preguntas y dirige la entrevista hacia el tema que le interesa, como si fuera una pirámide, iniciando desde la cúspide, con preguntas precisas y concretas, y conforme avanza la entrevista continúa con preguntas de carácter general hacia los intereses del auditor.

Este tipo de entrevistas también se puede utilizar para obtener información, partiendo de algo concreto, de algo ya especificado y, dependiendo de la habilidad del auditor para llevar a cabo la entrevista, se va dejando en libertad al entrevistado para que informe sobre los aspectos generales que se quieren indagar. Esto es muy similar a lo que dice el dicho popular: *meter aguja para sacar hilo*.

9.1.4.3 Entrevistas tipo diamante

El auditor inicia este tipo de entrevistas con preguntas cerradas enfocadas hacia un tópico que le interesa, y conforme avanza la entrevista dirige las preguntas hacia cuestiones más abiertas (con preguntas generales). Ya casi para finalizar la entrevista, de acuerdo con el transcurso de la plática, vuelve a hacer preguntas concretas enfocadas al tema que le interesa

Estas entrevistas son una combinación de las entrevistas anteriores, ya que inician con la modalidad de la entrevista de pirámide, pero en lugar de terminarlas con preguntas abiertas, se continúa como en la entrevista de embudo, es decir, concluyen con preguntas cerradas (concretas).

Su utilidad es muy variada, ya que se pueden utilizar en forma indistinta para cualquier tipo de entrevista que requiera el auditor.

9.1.4.4 Entrevistas tipo reloj de arena

El auditor inicia las entrevistas de este tipo con preguntas de carácter general (abiertas), y conforme avanza la plática, va haciendo preguntas más concretas (cerradas) enfocadas hacia temas que sean de su interés; después, para finalizar, vuelve a hacer preguntas de carácter general, buscando que el entrevistado le proporcione la mayor cantidad de información posible.

En este tipo de entrevistas también se da la combinación de las entrevistas anteriores, iniciando como en la modalidad de la entrevista de embudo, pero en lugar de terminar la entrevista con preguntas cerradas, se termina como en la entrevista tipo pirámide, es decir, con preguntas abiertas.

Con estas entrevistas se puede obtener información muy útil para una auditoría de sistemas, dependiendo de la experiencia y habilidad del auditor que las aplique.

Hemos presentado las anteriores clasificaciones de entrevistas como un complemento de las técnicas de recopilación de información que se utilizan en el análisis y diseño de sistemas; asimismo, proponemos estas entrevistas como una herramienta auxiliar que le servirá de apoyo al auditor para obtener información relacionada con la auditoría de sistemas computacionales.

Otra de las grandes ventajas de este instrumento es que le permite al auditor definir el planteamiento más adecuado para abordar el tema que desea investigar, mediante la técnica de la entrevista con los auditados, conforme a su propio albedrío y conveniencia.

Conviene recordar que entrevistar a los auditados es muy difícil, pues la mayoría, si no es que todos, suelen ocultar, disimular o fingir respuestas, y en algunos casos evitan responder directamente o lo hacen tratando de no comprometerse con lo que dicen. Muchas veces estos auditados sienten que son interrogados y se ponen a la defensiva, pues suponen que lo que comenten será utilizado en su contra. Éstos son algunos de los motivos de su falta de cooperación para responder las preguntas que se les formulan.

Ésta es la razón por la que se deben conocer distintas técnicas y métodos para realizar entrevistas. Es evidente que al seguir estas técnicas de entrevistas para la recopilación de información del área auditada, las aportaciones del entrevistado serán más confiables y acordes con los requerimientos del auditor.

9.1.5 Formas de recopilar la información en las entrevistas de auditoría

Ya destacamos la importancia y formas de realizar las entrevistas de auditoría, sin embargo, ahora debemos hacer algunas recomendaciones para obtener la información del entrevistado; al respecto, debemos señalar que no es fácil capturar la información que proporciona el entrevistado, pues existen ciertos impedimentos físicos o personales que dificultan esta tarea, además de que se necesita de mucha habilidad y experiencia por parte del auditor, así como de la aplicación de técnicas especiales.

A continuación presentamos algunas de las principales formas de recopilar la información.

9.1.5.1 Entrevistas grabadas

En estas entrevistas se hace la recopilación de la información por medio de algún instrumento electromagnético o de video, a fin de registrar todos los detalles de la entrevista, para posteriormente hacer un análisis de las aportaciones que hace el entrevistado. En algunos casos, esta información se puede utilizar como evidencia de algunas situaciones reportadas.

Aunque este tipo de captura de datos es el más sencillo y quizás el más recomendable, para los entrevistados es el menos favorable, pues les atemoriza saber que los están grabando porque suponen que los datos que proporcionan se pueden utilizar como evidencia en la auditoría.

9.1.5.2 Tomar notas

Otra de las modalidades más socorridas para recopilar información en una entrevista es recopilar los datos tomando notas en forma directa, es decir, cuando el auditor toma notas personalmente de lo que dice el auditado.

Para aplicar esta técnica de recopilación de información, el auditor requiere de una gran habilidad, experiencia y, en muchos casos, del uso de técnicas especiales como taquigrafía, toma de dictado o alguna otra herramienta que le permita tomar notas eficientemente.

La principal ventaja de esta técnica es que crea menor resistencia en el entrevistado y se puede interpretar la información al momento de capturarla; por otro lado, su principal desventaja es que se puede malinterpretar la información y perder datos valiosos cuando no se tiene mucha práctica en esta técnica.

9.1.5.3 Captar lo esencial sin notas

Una de las formas más utilizadas de captar información en la auditoría de sistemas es sin tomar notas en forma directa, o cuando menos sin que sea tan evidente como en el caso anterior; aunque es indudable que en esta técnica también se requiere de una gran experiencia y habilidad por parte del auditor, además de una gran memoria, concentración y capacidad de síntesis, entre otras muchas habilidades.

El auditor aplica esta técnica de manera natural en la práctica cotidiana de la auditoría, a cada momento y con la intensidad que le demanda la recopilación de la información, ya que al consultar e interrogar al entrevistado sobre algún tópico que está auditando, al mismo tiempo está tomando nota mentalmente de lo consultado, obteniendo así la información que requiere sin la formalidad de una entrevista. Obviamente, obtener buenos resultados con esta técnica dependerá de la experiencia y habilidad del auditor.

9.1.5.4 Otras formas

En la auditoría de sistemas existen otros tipos de entrevistas para recopilar información, pero cada auditor las aplica de acuerdo con sus necesidades; por esta razón, sólo mencionaremos algunos posibles ejemplos:

Entrevistas de segunda mano, realizadas a personas que no están involucradas directamente en el aspecto auditado, pero que aportan información relacionada.

Entrevistas ocultas*, en las que otra persona entrevista al auditado y éste no sabe que se está recopilando la información que proporciona.*

Entrevistas disfrazadas *de plática informal sobre cualquier aspecto que aparentemente no tiene relación con el trabajo, pero en las que se está recopilando la información que proporciona el entrevistado.*

9.2 Cuestionarios

Los cuestionarios son una de las formas de recopilación de información de mayor utilidad para el auditor; por esta razón, a continuación presentamos una definición de cuestionario:

Es la recopilación de datos mediante preguntas impresas en cédulas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, el auditor obtiene información útil que puede concentrar, clasificar e interpretar por medio de su tabulación y análisis, para evaluar lo que está auditando y emitir una opinión sobre el aspecto investigado.

El cuestionario tiene la gran ventaja de que puede recopilar una gran cantidad de información, debido a que contiene preguntas sencillas cuyas respuestas no implican ninguna dificultad; además, como en otros métodos, su aplicación es de carácter impersonal y libre de influencias y compromisos para el entrevistado. También tiene la ventaja de poder seleccionar los tipos de preguntas que se deben realizar, los cuales señalaremos a continuación.

9.2.1 Preguntas abiertas

Son las preguntas donde el encuestado es libre de responder de acuerdo con su criterio, o en las que tiene múltiples opciones para responder sin ninguna limitación, ni en tamaño ni en profundidad y le permiten que la expresión de sus ideas y opiniones fluya sin limitaciones.

La ventaja de este tipo de preguntas es que se puede obtener más información de la esperada; también dejan abierta la posibilidad de profundizar sobre tópicos no contemplados inicialmente, aunque tienen la desventaja de que dificultan la tabulación de los datos, e incluso pueden provocar que se desvíe la atención del encuestado.

Estas preguntas son de mucha utilidad en una auditoría de sistemas computacionales, principalmente para iniciar la recopilación de información, debido a que se obtiene mucha información, aunque se corre el riesgo de desviar la atención hacia temas ajenos al objeto de la auditoría.

No hay un formato específico para este tipo de preguntas; por esta razón, el auditor de sistemas puede emplear libremente la forma de preguntas abiertas que le sea útil, de acuerdo con sus necesidades de información.

9.2.2 Preguntas cerradas

Con este tipo de preguntas el encuestado tiene la oportunidad de elegir la respuesta que sea acorde con su opinión de entre las opciones presentadas. Hay varias formas de preguntas cerradas, entre las cuales tenemos las siguientes.

9.2.2.1 Preguntas dicotómicas

Estas preguntas sólo tienen dos posibles respuestas, que por lo general son opuestas entre sí, por ejemplo:

( ) Sí ( ) No

( ) Masculino ( ) Femenino

( ) Presente ( ) Ausente
( ) Hardware ( ) Software

9.2.2.2 Preguntas tricotómicas

Son aquellas que tienen tres opciones de respuesta, por ejemplo:

( ) Sí ( ) No ( ) Sin respuesta
( ) Redes ( ) Equipo mayor ( ) PCs

¿Cuál es su nivel de responsabilidad en el centro de cómputo?

( ) Operador ( ) Líder de proyecto ( ) Gerente

9.2.2.3 Preguntas de opción múltiple

También conocidas como preguntas *peine* o *ítems,* presentan varias respuestas de entre las que se puede elegir sólo una; por lo general, estos ítems tienen una gama de respuestas que varían de un extremo a otro, por ejemplo:

Elija la respuesta marcando con una "x"

Soltero	( )	Excelente	( )	Empleado	( )
Divorciado	( )	Bueno	( )	Usuario	( )
Viudo	( )	Regular	( )	Proveedor	( )
Unión libre	( )	Malo	( )	Asesor	( )
Casado	( )	Deficiente	( )	Directivo	( )

9.2.2.4 Preguntas de opción de rangos o grupos

Son las preguntas cuyas respuestas se encuentran comprendidas en ciertos rangos o grupos, dentro de los cuales el encuestado puede elegir sólo una de las respuestas, por ejemplo:

Elija su tiempo de trabajo en computadora de entre alguno de los siguientes rangos:

Menos de 2 horas al día ( )
De 2 a 4 horas al día ( )
De 4 a 6 horas al día ( )
De 6 a 8 horas al día ( )
Más de 8 horas al día ( )
Nunca la utiliza ( )

9.2.2.5 Gradación (preguntas de grados opuestos)

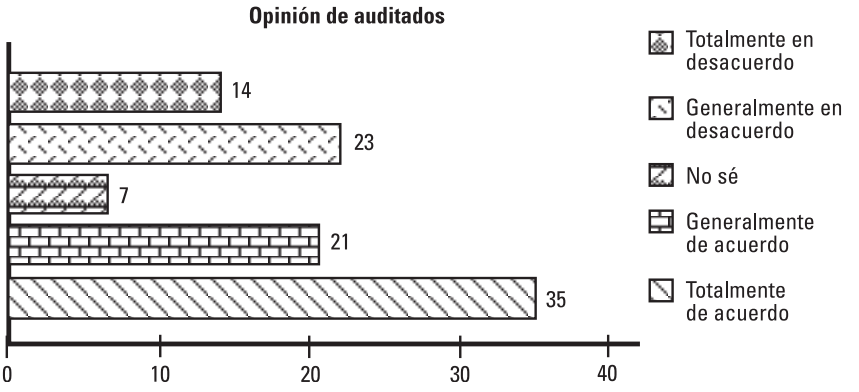
También conocida como gradación de Likert; en este tipo de preguntas cerradas, las respuestas se emplean para recopilar las opiniones, intereses o actitudes de los entrevistados, concentrando gradualmente cada una de las respuestas, una por una, hasta obtener porcentajes representativos de ellas, por lo general estas preguntas se hacen bajo cinco grados o tipos de respuestas, donde los extremos son totalmente opuestos entre sí, por ejemplo:

La empresa pretende modificar el sistema actual de procesamiento de datos por un sistema de redes. ¿Qué opina?

Totalmente de acuerdo	( )
Generalmente de acuerdo	( )
No sé	( )
Generalmente en desacuerdo	( )
Totalmente en desacuerdo	( )

Las respuestas a los cuestionarios aplicados se agrupan, una a una, y se concentran en cuadros estadísticos o gráficas que arrojan información fácil de interpretar, por ejemplo, para 100 cuestionarios, independientemente de los aspectos estadísticos, se obtendrían los siguientes datos:

Preguntas	**Casos**
Totalmente de acuerdo	35
Generalmente de acuerdo	21
No sé	7
Generalmente en desacuerdo	23
Totalmente en desacuerdo	14



9.2.2.6 Preguntas testigo

Son las preguntas que se hacen para comprobar la veracidad de las respuestas a otras preguntas hechas con anterioridad, en otra forma y en otra parte del cuestionario; su aplicación es opcional, sin embargo, son muy útiles para comprobar la veracidad de las respuestas que emiten los encuestados. Además, estas preguntas se pueden hacer bajo cualquiera de los formatos analizados anteriormente.

9.2.2.7 Preguntas matriz

Estas preguntas tienen la peculiaridad de que se elaboran en cualquier medio, en cuadernillo, en grupo, en hojas sueltas u otro medio, pero son contestadas en una hoja en forma de matriz, logrando con esto mayor congruencia, una rápida tabulación y mayor veracidad en las respuestas.

Además, tienen la gran ventaja de poder agruparse en obtención de datos aparentemente distintos y desconectados entre sí, pero que le pueden ayudar al auditor a conocer aspectos especiales que desee auditar, por ejemplo:

	Edad	**Antigüedad**		**Nivel de ingresos**	**Funciones que realiza**			
		Puesto	**Área**		**directivo**	**decisión**	**supervisor**	**operación**
Gerente								
Líder de proyecto								
Analista								
Programador								
Operador								
Administrativo								

El propio auditor puede elaborar estas preguntas para poder validar las respuestas en el momento que las recibe, y las puede elaborar en grupo o de manera individual; pero es él quien debe anotar las respuestas de los encuestados.

Es recomendable elaborar las preguntas previamente y efectuar pruebas piloto antes de aplicarlas, además pueden aplicarse de manera grupal o individual.

9.2.2.8 Ventajas y desventajas de los cuestionarios

Los cuestionarios son los instrumentos más populares para la recopilación de información, sobre todo para la información relacionada con las auditorías de cualquier tipo.

Por esta razón son muy utilizados y tienen muchas ventajas para obtener grandes volúmenes de datos, aunque también tienen grandes desventajas que limitan su aplicación. A continuación presentamos algunas de las ventajas y desventajas más comunes de los cuestionarios.

Ventajas

- *Facilitan la recopilación de información y no se necesitan muchas explicaciones ni una gran preparación para aplicarlos.*
- *Permiten la rápida tabulación e interpretación de los datos, proporcionándoles la confiabilidad requerida.*
- *Evitan la dispersión de la información requerida, al concentrarse en preguntas de elección forzosa.*
- *Por su diseño, los cuestionarios son muy rápidos de aplicar y ayudan a captar mucha información en poco tiempo.*
- *En el ambiente de sistemas es fácil capturar, concentrar y obtener información útil a partir de las respuestas, mediante el uso de la computadora. Incluso se pueden proyectar los datos y hacer gráficas.*
- *Hacen impersonal la aportación de respuestas; por lo tanto, en una auditoría ayudan a obtener información útil y confiable, si se plantean bien las preguntas.*

Desventajas

- *Falta de profundidad en las respuestas y no se puede ir más allá del cuestionario.*
- *Se necesita una buena elección del universo y de las muestras utilizadas.*
- *Pueden provocar la obtención de datos equivocados si se formulan deficientemente las preguntas, si se distorsionan o si se utilizan términos ilegibles, poco usados o estereotipados.*
- *La interpretación y el análisis de los datos pueden ser muy simples si el cuestionario no está bien estructurado o no contempla todos los puntos requeridos.*
- *Limitan la participación del auditado, ya que éste puede evadir preguntas importantes o se puede escudar en el anonimato que dan los cuestionarios.*
- *Hacen impersonal la participación del personal auditado, por lo que la aportación de la información útil para la auditoría es limitada.*
- *Denotan la falta de experiencia y pocos conocimientos del auditor que las aplica, si éste no plantea ni estructura correctamente las preguntas, lo cual puede provocar que su trabajo sea rechazado.*

9.2.3 Método para diseñar y aplicar los cuestionarios

Ya señalamos al principio de este punto que el cuestionario es uno de los instrumentos más utilizados en la recopilación de información para cualquier tipo de auditoría; por esta misma razón, en la auditoría de sistemas computacionales este valioso instru-

mento se puede aprovechar para la recopilación de información sobre algunos aspectos concretos de los sistemas computacionales, sin embargo, para aplicarlo correctamente se necesita un procedimiento específico que permita utilizar eficientemente este tipo de instrumentos de auditoría; basándonos en ello, a continuación proponemos los siguientes pasos:

Determinar el objetivo del cuestionario
Elaborar un borrador del cuestionario
Aplicar una prueba piloto
Elaborar el cuestionario final
Determinar el universo y la muestra
Aplicar el cuestionario
Tabular la información del cuestionario y elaborar gráficas y cuadros
Interpretar los resultados
Elaborar las observaciones

A continuación analizaremos brevemente cada uno de estos puntos, a fin de entenderlos mejor.

9.2.3.1 Determinar el objetivo del cuestionario

Lo primero que debe hacer el auditor es determinar los objetivos que pretende alcanzar con la aplicación del cuestionario, es decir, tiene que establecer el fin que persigue; para ello se tiene que hacer las siguientes preguntas: ¿Qué información pretende obtener con la aplicación del cuestionario? ¿Para qué aplicarlo? ¿Qué información obtendrá? ¿Cómo la utilizará? ¿La aplicación del cuestionario satisface sus necesidades de información? Y todo lo relacionado con la recopilación de información para la auditoría por medio de este instrumento.

Es importante que el auditor defina perfectamente los objetivos de recopilación de datos y los resultados que espera obtener con este instrumento.

9.2.3.2 Elaborar un borrador del cuestionario

Una vez definidos el objetivo y los resultados que espera obtener con este instrumento, el auditor debe elaborar el borrador mecanografiado del cuestionario, definiendo la cantidad y el tipo de preguntas, así como la forma de aplicarlas para obtener mejores respuestas sin perder de vista el objetivo de la evaluación.

El auditor puede elaborar la cantidad de borradores que necesite, lo importante es que haga el cuestionario lo mejor posible.

9.2.3.3 Aplicar una prueba piloto

Después de elaborar el borrador del cuestionario, el siguiente paso es probarlo; para ello, el auditor puede hacer la recopilación inicial de información en forma de experimento, es

decir, puede aplicar el cuestionario a determinadas personas, observando la manera en que lo contestan y las dificultades que hubiese; posteriormente, analizar las respuestas, el auditor puede comprobar si el cuestionario cumple adecuadamente con los objetivos de recopilación de información y su utilidad para capturar la información que requiere.

El resultado obtenido con esta prueba piloto sirve para corregir, modificar o ratificar la forma en que están planteadas las preguntas, a fin de recopilar eficientemente la información.

Esta prueba se puede hacer tantas veces como sea necesario, y se puede utilizar de muchas maneras, pero lo fundamental es hacerla para perfeccionar las preguntas antes de aplicar el cuestionario final.

9.2.3.4 Elaborar el cuestionario final

Con los resultados de la prueba piloto se perfeccionan todos los detalles del cuestionario para elaborarlo de manera definitiva, a fin de reproducirlo y aplicarlo de acuerdo con las necesidades y características de la recopilación de datos que demanda su evaluación.

Es muy importante que el auditor haga las pruebas piloto necesarias, a fin de elaborar correctamente el cuestionario final.

9.2.3.5 Determinar el universo y la muestra

Éste es uno de los principales aspectos que se deben estudiar en la aplicación del cuestionario y de cualquier instrumento de recopilación de información, ya que la validez estadística de la recopilación de datos para la auditoría de sistemas dependerá de su correcta elección.

El auditor debe determinar el universo en el que aplicará el cuestionario, de acuerdo con sus necesidades específicas de recopilación de información y, si es necesario, también debe calcular la muestra que utilizará en la aplicación de los cuestionarios, de acuerdo con las fórmulas estadísticas correspondientes y las necesidades concretas de la evaluación.

Debido a la importancia del tema, en la sección 9.6 de este capítulo haremos un análisis sobre la importancia de las muestras, su uso estadístico y la manera de aplicarlas.

9.2.3.6 Aplicar el cuestionario

El siguiente paso es aplicar el cuestionario a la muestra o personal seleccionado; para esto se puede utilizar cualquier técnica de aplicación, ya sea por correo, directamente, mediante encuestadores, en forma grupal o individual, o por cualquier otro método.

9.2.3.7 Tabular la información del cuestionario y elaborar gráficas y cuadros

Una vez que han sido recopilados todos los cuestionarios, el siguiente paso es capturar los datos de cada cuestionario y concentrarlos en cuadros estadísticos o gráficas,

por medio del método estadístico o programa de cómputo elegido para tabular la información, de acuerdo con lo determinado en la planeación de la auditoría, el universo y las muestras.

Debido a que existen muchos métodos y programas de cómputo para la concentración de información y presentación de cuadros estadísticos y gráficas de interpretación, en la sección 9.6 de este capítulo también haremos un análisis sobre estos tópicos.

9.2.3.8 Interpretar los resultados

El siguiente paso y quizás el más importante para el auditor de sistemas computacionales, es analizar la información concentrada en los cuadros estadísticos y gráficas de presentación, con el propósito de interpretarla y evaluar el comportamiento del aspecto de sistemas auditado; esto también le ayuda a identificar las posibles desviaciones que reportara.

Después de la elaboración del cuestionario, la interpretación de la información recopilada con este instrumento es la función más importante del auditor y del responsable de la auditoría, ya que sólo si tienen la experiencia y los conocimientos necesarios podrán interpretar correctamente dicha información, para así emitir una explicación adecuada del comportamiento del ámbito de sistemas auditado con este instrumento.

9.2.3.9 Elaborar las observaciones

Una vez interpretada la información recopilada, el auditor puede determinar las posibles observaciones sobre el funcionamiento del aspecto de los sistemas evaluados, para reportarlas en su informe. Aquí es donde el auditor establece las desviaciones encontradas.

Cabe señalar que el cuestionario se puede aplicar en forma individual o general para todos los que trabajan en el área de sistemas y para las personas involucradas en la misma; también se puede aplicar en cualquier tipo de auditoría, de acuerdo con las necesidades concretas de cada evaluación, con el tiempo programado y con los recursos disponibles para realizarla.

9.3 Encuestas

Las encuestas constituyen otra de las técnicas más populares y de mayor uso en una auditoría de sistemas computacionales, y son útiles principalmente para averiguar opiniones sobre aspectos de la informática tales como el servicio, el comportamiento y utilidad del equipo, la actuación del personal y los usuarios, la oportunidad de la presentación de los resultados, entre otros juicios sobre la función informática.

Existen muchas técnicas y métodos para aplicar las encuestas, no sólo en la auditoría sino también en las ciencias sociales, en donde tienen muchas aplicaciones y sus resultados son cada vez más confiables y aceptados, tanto por las técnicas y procedimientos que se utilizan para su diseño, como por la elección del universo y deter-

minación estadística de las muestras. También por la forma de captar las opiniones, concentrar los datos y emitir los resultados en cuadros estadísticos y gráficas, además de muchos otros aspectos que las han hecho cada día más populares. Incluso en la actualidad ya tienen más aceptación que otras herramientas para auditorías de sistemas computacionales, ya que son parte fundamental de una investigación sobre la recopilación de opiniones, y sus resultados son razonablemente aceptados.

Podemos definir una encuesta de la siguiente manera:

> *Es la recopilación de datos concretos sobre un tema específico, mediante el uso de cuestionarios o entrevistas diseñados con preguntas precisas para obtener las opiniones de los encuestados, las cuales permiten, después de hacer una rápida tabulación, análisis e interpretación de esa información, conocer su punto de vista y sentimientos hacia un tópico específico.*

Las encuestas son un complemento muy valioso para la información que obtiene el auditor con los cuestionarios y entrevistas debido a que con ellas consigue comentarios, opiniones, interpretaciones y datos a través de preguntas sencillas y simples; asimismo, puede concentrar esas opiniones a través de técnicas estadísticas para cuantificarlas y darles una interpretación sobre el fenómeno de sistemas estudiado.

Además, haciendo primero las encuestas y después entrevistas aleatorias, el auditor puede corroborar la información recopilada de un área y compararla con la que tiene de esa misma área o de otra. Esto le ayuda a hacer una mejor evaluación de los sistemas que está auditando.

Las encuestas también son un valioso auxiliar para obtener información abundante, útil y confiable sobre el comportamiento, la utilidad y oportunidad con la cual se proporcionan los servicios del sistema o del área de sistemas de la empresa. Además permiten recopilar, cuantificar, tabular e interpretar fácilmente, en estadísticas, cuadros y gráficas las tendencias de opiniones y comentarios de los encuestados.

Por estas razones, aparte de su creciente importancia, es muy conveniente conocer la manera de utilizar esta herramienta que ayuda al auditor en la recopilación, tabulación y análisis, de información, no sólo para auditorías de sistemas, sino para la auditoría en general.

No existen reglas para el uso de las encuestas en el área de auditoría de sistemas; quizá las únicas son las que regulan los aspectos técnico-estadísticos en la elección del universo y la muestra; pero éstas se pueden contemplar dentro de la aplicación de métodos probabilísticos y estadísticas para hacer la mejor elección de las muestras, así como la selección de los métodos de recopilación de opiniones.

Con la aplicación de encuestas en las auditorías de sistemas se busca que la forma de recopilar las opiniones sea ágil, sencilla y poco complicada para los encuestados; esto se logra mediante preguntas claras, sencillas y de fácil entendimiento, a fin de que las respuestas de los encuestados sean concretas y enfocadas hacia el tema de estudio. Con las encuestas también se hace más sencilla la tabulación de la informa-

ción obtenida y, consecuentemente, se vuelve más confiable la concentración de esas opiniones. Además, permiten al auditor analizar e interpretar los resultados con mayor facilidad para fundamentar sus opiniones.

Esta herramienta no es de uso exclusivo para la auditoría sino que también se aplica, con mucho éxito, en el análisis y diseño de sistemas, el campo de las ciencias sociales y, principalmente, en los sondeos de opinión. Respecto a su aplicación, existen muchas técnicas y métodos; sin embargo, a continuación haremos un breve análisis de las principales características de las encuestas y de cómo se aplican en la auditoría de sistemas.

9.3.1 Clasificación de la encuesta por la forma de obtener la información

Esta clasificación atiende a la manera de obtener la recopilación de información, ya se sea de las opiniones, comentarios, sugerencias o de cualquier otro dato importante para la auditoría de sistemas; dicha recopilación se puede realizar de tres formas distintas, mismas que analizaremos a continuación.

9.3.1.1 Encuestas escritas

En estas encuestas se recopila la información mediante algún tipo de cuestionario que el encuestado responde directamente con su puño y letra, quien, además, puede responder a estas encuestas de manera anónima o proporcionar sus datos de identificación, según las necesidades de la evaluación.

La aplicación de estas encuestas le puede proporcionar grandes ventajas al auditor de sistemas, debido a que le permite tabular y analizar la información fácilmente, y con ello fundamentar sus comentarios, sin embargo, también puede haber serias dificultades para su aplicación, ya sea por resistencia de los encuestados, por su falta de cooperación o porque proporcionan información limitada e insuficiente; esto puede limitar la utilidad de esta herramienta.

9.3.1.2 Encuestas verbales

En la aplicación de estas encuestas, el auditor plantea las preguntas directamente al encuestado y obtiene sus respuestas de manera verbal, registrando sus opiniones y comentarios a través de algún medio magnético o tomando nota él mismo. En este caso, el encuestador registra las aportaciones del encuestado, sin embargo, en estas encuestas no se debe tratar de interpretar ni tratar de traducir las opiniones del encuestado, solo debe captarlas.

Ésta es una de las herramientas más valiosas en la auditoría de sistemas para obtener las opiniones y comentarios de los auditados, ya que ayuda a vencer su resistencia y es de fácil aplicación; siempre y cuando sea bien utilizada y estén bien definidos los objetivos que se pretenden alcanzar con ella.

9.3.1.3 Encuestas mixtas

Estas encuestas son una combinación de las dos técnicas anteriores y se aplican de acuerdo con las necesidades específicas de información del auditor y de acuerdo con las características de los encuestados.

9.3.2 Clasificación de la encuesta por la forma de realizarla

Esta clasificación obedece exclusivamente a las diferentes formas de obtener las opiniones y comentarios de los auditados; estas formas de obtener la información se clasifican de la siguiente manera.

9.3.2.1 Encuestas dirigidas

Son las encuestas en donde un auditor induce al encuestado para que centre sus opiniones y comentarios hacia temas concretos sobre la evaluación, sin embargo, este tipo de encuestas no se debe confundir con encuestas manipuladas. Lo fundamental de estas encuestas es que se deben dirigir hacia un objetivo específico de la evaluación, pero no se deben manipular ni desviar intencionalmente hacia un resultado.

A continuación presentamos algunas aplicaciones para esta herramienta:

Para conocer las opiniones sobre el servicio que prestan los sistemas de la empresa; en estas encuestas todas las preguntas están enfocadas a obtener opiniones y comentarios de los usuarios sobre cómo sienten este servicio, y únicamente se deben hacer sobre este tópico, no se pueden hacer para obtener información sobre algún otro tema.

Para conocer la utilidad de un programa desarrollado en la empresa; en este caso, todas las preguntas se enfocarán a que el usuario del programa opine sobre la utilidad de éste, sus beneficios y defectos, pero nada más sobre este programa y no sobre otros similares.

Para las prestaciones que se otorgan a los trabajadores del área de sistemas; aquí se busca saber lo que opinan los trabajadores sobre las prestaciones, en dinero y en especie, que reciben como complemento de sus ingresos, pero sólo sobre este tema, no se pueden utilizar para otros temas.

Éstos son sólo tres ejemplos que sirven para que el auditor entienda cómo funciona este tipo de encuestas y para que pueda diseñarlas de acuerdo con sus necesidades específicas de evaluación.

9.3.3 Clasificación de la encuesta por la forma de las preguntas

Por lo general, las encuestas se realizan con preguntas concretas (cerradas) o de carácter general (abiertas) que se centran en temas de interés para el auditor, buscando

obtener respuestas en sólo dos sentidos; para el mejor entendimiento de esta forma de elaborar las preguntas para una encuesta, conviene aplicar lo señalado en la sección 9.2.2 de este capítulo, pero adaptándolo a las encuestas. A continuación haremos un breve repaso de lo señalado en las preguntas de tipo cerrado.

9.3.3.1 Preguntas dicotómicas

Este tipo de preguntas sólo tienen dos posibles respuestas, por lo general opuestas entre sí, por ejemplo:

( ) Sí	( ) No
( ) Masculino	( ) Femenino
( ) Presente	( ) Ausente
( ) Hardware	( ) Software

En las encuestas se puede utilizar este tipo de preguntas, pero tendrían muy pocas aplicaciones y la obtención de opiniones sería deficiente.

9.3.3.2 Preguntas tricotómicas

Son las preguntas que tienen tres opciones de respuesta, por ejemplo:

¿El sistema de cómputo instalado en la empresa funciona adecuadamente?

Sí ( ) No ( ) Sin respuesta ( )

Se va a implantar la capacitación obligatoria en el manejo de Internet, ¿cuál es su posición al respecto?

A favor ( ) En contra ( ) Sin opinión ( )

La emigración de sistemas que llevará a cabo la empresa requiere la actualización de los lenguajes; el primer lenguaje que se pretende implantar es Java. ¿Qué opina?

De acuerdo ( ) En desacuerdo ( ) No opina ( )

Aquí las aplicaciones son más amplias al obtener tres posibles respuestas, sin embargo, aunque se obtiene una mayor gama de opiniones, también se pueden considerar pobres y limitadas para las necesidades de una auditoría de sistemas.

9.3.3.3 Preguntas de opción múltiple

También conocidas como preguntas peine o ítems, tienen varias respuestas de entre las que se puede elegir una sola; por lo general, estos ítems tienen una gama de respuestas que varían de un extremo a otro, de mayor a menor o viceversa, por ejemplo:

¿Cómo calificaría el funcionamiento del sistema de red instalado en la empresa?

Excelente ( )
Bueno ( )
Regular ( )
Malo ( )
Pésimo ( )

¿Cómo calificaría la solución de los problemas relacionados con el mantenimiento de los sistemas computacionales?

( ) Muy buena ( ) Suficiente ( ) Mala ( ) Inexistente

¿La actualización del sistema de procesamiento de nómina cumple con los objetivos trazados?

Sí cumple en su totalidad ( ) Desconoce si cumple ( )
Apenas y cumple ( ) Se abstiene de opinar ( )
No cumple en lo más mínimo ( )

En una auditoría de sistemas, este tipo de preguntas puede llevar a conclusiones importantes sobre el funcionamiento actual y futuro de los sistemas.

9.3.3.4 Preguntas de opción de rangos o grupos

Son las preguntas cuyas respuestas se encuentran comprendidas en ciertos rangos o grupos que van desde un extremo mínimo hasta otro extremo máximo, dentro de los cuales el encuestado puede elegir sólo una respuesta que satisfaga su opinión. Generalmente se buscan grupos homogéneos que representen aspectos graduables para medir con mayor facilidad las opiniones de los encuestados, por ejemplo:

¿Cuál es, en su opinión, el tiempo óptimo de trabajo en computadora para las actividades que realiza? Seleccione sólo uno de los siguientes rangos.

Menos de 2 horas al día ( )
De 2 a 4 horas al día ( )
De 4 a 6 horas al día ( )
De 6 a 8 horas al día ( )
Más de 8 horas al día ( )
Nunca la utiliza ( )

¿Cuánto tarda (en días hábiles) en capturar los datos para hacer el procesamiento de la nómina del personal?

Menos de dos días a la quincena ( )
De tres a cinco días a la quincena ( )

De cinco a ocho días a la quincena ( )
Más de ocho días a la quincena ( )

Estas preguntas pueden ser de mucha utilidad para el auditor, ya que las puede aplicar en múltiples campos y en formas muy variadas, por su facilidad para estimar rangos más o menos homogéneos en los que el encuestado tiene que opinar sobre uno solo. Todo dependerá de los objetivos que el auditor pretenda alcanzar.

9.3.3.5 Gradación de Likert

En este tipo de preguntas, las respuestas se emplean para recopilar las opiniones, intereses o actitudes de los entrevistados, concentrando gradualmente cada una de las respuestas para conseguir porcentajes representativos de la mayoría de las opiniones; por lo general estas preguntas se hacen bajo cinco grados o tipos de respuestas, en donde los extremos son opuestos entre sí, por ejemplo:

La empresa pretende modificar el sistema actual de procesamiento de datos por un sistema de redes. ¿Qué opina de esta decisión?

Totalmente de acuerdo ( )
Parcialmente de acuerdo ( )
No puedo opinar ( )
Parcialmente en desacuerdo ( )
Totalmente en desacuerdo ( )

¿Cómo es, en su opinión, la seguridad en el acceso a los sistemas computacionales de la empresa, en cuanto a la satisfacción de las necesidades de protección de sus datos?

Absolutamente confiable ( )
Confiable ( )
Aceptable ( )
Poco confiable ( )
Absolutamente desconfiable ( )

Las respuestas a estas preguntas se agrupan, una a una, y se concentran en cuadros estadísticos o gráficas que arrojan información fácil de interpretar. En la sección 9.2.2 de este capítulo presentamos un ejemplo de cuadro estadístico y una gráfica.

9.3.3.6 Preguntas testigo (variables de control)

Son las preguntas que se hacen para comprobar la veracidad de las respuestas a otras preguntas hechas anteriormente; con estas preguntas se verifica la honradez en las respuestas; un claro ejemplo sería el caso de la edad; si vemos al encuestado maduro

(entre 36 y 50 años) y éste pone la edad de un joven (entre 18 y 27), está claro que si miente en esta respuesta, también puede mentir en otra parte del cuestionario; aquí lo mejor es desechar estas respuestas. Una variante es hacer la misma pregunta en otra parte de la encuesta, pero cambiando el formato, mas no el fondo; teóricamente, la respuesta debe ser similar; en caso de ser contraria, habría que valorar si se desecha la encuesta o si estas opiniones se toman con reservas.

El uso de estas preguntas es opcional; sin embargo, son muy útiles para comprobar la veracidad en las respuestas de los encuestados. Además, este tipo de preguntas, también llamadas variables de control, se puede hacer bajo cualquiera de los formatos que indicamos a continuación.

Sexo

Esto no se pregunta, *sólo* se observa y se anota.

Masculino ( ) *Femenino* ( )

Edad

( ) Joven [entre 18 y 27]
( ) Adulto [entre 28 y 35]
( ) Maduro [entre 36 y 50]
( ) Mayor [entre 51 y 65]
( ) Anciano [mayor a 66]

Una variante es no preguntar la edad sino el año de nacimiento; de esta manera se puede calcular automáticamente la edad y observar la apariencia del encuestado.

Lugar de nacimiento

Se recaban el estado y municipio.

Esta pregunta puede ser muy importante en una auditoría de sistemas, ya que la respuesta puede indicar cierto tipo de comportamiento del encuestado, según su lugar de origen; no es el mismo comportamiento en el sur, que en el centro o en el norte. Este criterio sería muy subjetivo en grandes ciudades y de acuerdo con el tiempo de residencia, sin embargo, se debe tomar en cuenta cuando sea necesario diferenciar algunas respuestas.

Educación

Se mide en años completos de estudio y se busca identificar el grado de conocimientos y participación del encuestado en el ambiente informático. No es lo mismo preguntar a un usuario con pocos conocimientos de sistemas qué opina acerca de la instalación de una red, que plantear la pregunta a un usuario con estudios especializados en sistemas. Las respuestas y opiniones son diametralmente opuestas. Para medir

el grado de educación sugerimos utilizar los siguientes rangos, los cuales son aplicables sólo al ambiente de sistemas, ya que en las ciencias sociales puede haber otros parámetros de educación que aquí no señalaremos:

1. *Educación básica (para los empleados que tienen primaria o secundaria)*
2. *Educación media superior (para los empleados que cursaron la preparatoria o similar)*
3. *Educación secretarial con apoyo de sistemas*
4. *Educación técnica ajena al área de sistemas*
5. *Educación técnica con especialidad en sistemas*
6. *Profesional sin conocimientos de sistemas (o con conocimientos elementales)*
7. *Profesional en sistemas*
8. *Especialidad en sistemas (maestría, diplomado, certificado)*
9. *Otros estudios con manejo de sistemas*

Manejo de la computadora

¿Cuál es su trabajo en el área de sistemas y qué equipo maneja?

( ) Usuario	( ) PC	( ) Red	( ) Equipo mayor
( ) Operador de sistemas	( ) PC	( ) Red	( ) Equipo mayor
( ) Desarrollador de sistemas	( ) PC	( ) Red	( ) Equipo mayor
( ) Programador de sistemas	( ) PC	( ) Red	( ) Equipo mayor
( ) Administrador del sistema	( ) PC	( ) Red	( ) Equipo mayor
( ) Directivo de sistemas	( ) PC	( ) Red	( ) Equipo mayor
( ) Asesor	( ) PC	( ) Red	( ) Equipo mayor
( ) Desarrollador externo	( ) PC	( ) Red	( ) Equipo mayor

Ésta es otra de las preguntas que ayudan a valorar la profundidad de las encuestas sobre el dominio de los sistemas por parte del entrevistado, e incluso a rechazarlas. Es obvio que no es igual la opinión de un usuario inexperto en el manejo de una PC, que la de un experto en redes; la diferencia de conocimientos informáticos entre uno y otro es abismal, por lo tanto, la diferencia en sus comentarios también lo es.

Puesto en la empresa

Otra de las preguntas que sirven de apoyo para validar la veracidad de la encuesta, así como para calificar la importancia de la información recopilada en ella, es lo relacionado con el puesto que ocupa el entrevistado en el área de cómputo, debido a que su respuesta indica su responsabilidad, autoridad y nivel de toma de decisiones. Esto ayuda al auditor a diferenciar las opiniones y comentarios del auditado.

Es obvio que la opinión del más alto directivo del área de sistemas para autorizar el desarrollo de un nuevo proyecto no es igual a la del operador del sistema, ni a la del

líder de proyectos encargado de desarrollar dicho proyecto, ni a la del programador del sistema. Está claro que cada quien opinará desde su particular punto de vista, de acuerdo con el nivel de estructura y a su responsabilidad en la empresa.

Qué revistas y periódicos especializados lee el auditado

¿Cuáles son los libros, revistas y periódicos especializados en sistemas que lee?

( ) Periódicos ¿Cuáles? _____
( ) Revistas ¿Cuáles? _____
( ) Libros ¿Cuáles? _____
( ) Otros ¿Cuáles? _____

Esta pregunta sirve para establecer el grado de cultura informática y actualización que tiene el entrevistado, con el propósito de valorar sus comentarios y opiniones.

9.3.3.7 Encuestas no dirigidas

Al aplicar este tipo de encuestas, el auditor deja que el auditado exprese libremente sus opiniones y comentarios, sin interferir en éstos, sobre un tema específico de la evaluación.

9.3.4 Clasificación de las encuestas por el universo que abarcan

Es la clasificación de las encuestas según el método que se sigue para recopilar las opiniones, ya sea que éstas se obtengan de una sola persona, de un grupo o de una área en especial; esta clasificación incluye los siguientes tipos de encuestas.

9.3.4.1 Encuestas individuales

Son las entrevistas que hace el auditor de manera individual a cada uno de los encuestados, utilizando cualquiera de las técnicas de entrevista anteriores.

9.3.4.2 Encuestas de grupo

Son las encuestas que el auditor aplica a un mismo grupo de auditados, concentrando de manera estadística la información obtenida y registrándola en grupos, ya sea por mayoría simple, por grupos de opinión o por cualquier otro tipo de gradación.

La aplicación de este tipo de encuestas no es fácil ni tan común, debido a que se requiere el concurso de un grupo de auditados, los cuales muchas veces no están dispuestos a cooperar o tratan de minimizar sus comentarios para no comprometerse, sin embargo, ahorran mucho tiempo de recopilación y cuando son bien aplicadas se obtiene información homogénea y resultados confiables.

9.3.5 Clasificación de la encuesta por la forma de manejar la información

Esta clasificación se hace tomando en cuenta la forma de manejar las opiniones y comentarios de los encuestados, debido a que se busca ligar la forma de compilar los datos con la forma de comprobar su veracidad, oportunidad y suficiencia, así como la forma de establecer un método confiable para accesar la información en forma más congruente.

9.3.5.1 Encuestas unidas

Son las encuestas que se aplican con preguntas hechas especialmente para ligar las posibles respuestas, opiniones y comentarios de los encuestados, con el fin de obtener una secuencia lógica y confiable.

Este tipo de preguntas se debe realizar de manera simple, sin repetirlas y lo más transparentemente posible, ya que se busca verificar la confiabilidad de las respuestas de los encuestados. Además, estas preguntas son de gran utilidad para cualquier tipo de auditoría, ya que ayudan a recopilar la información de manera más sencilla.

9.3.5.2 Encuestas transversales

Estas encuestas se hacen con preguntas que se cruzan entre sí para obtener cierto grado de veracidad en las respuestas de los encuestados, es decir, se hace una pregunta en algún lugar y de una manera muy específica, y después se hace otra pregunta relacionada con la primera, pero en distinto lugar; el propósito es obtener respuestas más o menos secuenciales de un mismo tema; con ello se puede verificar la confiabilidad de las respuestas de los encuestados.

Estas preguntas son muy importantes en una auditoría de sistemas para comprobar la confiabilidad de las respuestas, incluso para eliminar las que no sean tan confiables o para tomarlas con las reservas del caso.

9.3.5.3 Encuestas de candado

Son las encuestas que se hacen con preguntas que tienen el mismo contexto pero planteadas de diferentes formas y en distintas partes de la encuesta, con el fin de determinar la validez de las respuestas, opiniones y comentarios de los auditados es decir, a través de preguntas aparentemente diferentes, formuladas en diferentes partes de la encuesta, se obtienen respuestas, comentarios y opiniones similares. En caso de que las respuestas sean diferentes, el auditor puede dudar de la veracidad de éstas. Esto permite que el auditor valore la utilidad de estas encuestas.

9.3.6. Clasificación de la encuesta por la forma de participación de los encuestados

Esta clasificación permite desarrollar un tipo especial de obtención de información, la cual se concentra sobre un objetivo específico, de acuerdo con lo que el auditor quiera analizar; a continuación presentamos algunos ejemplos.

9.3.6.1 Encuestas de panel

Son las encuestas que permiten obtener la opinión de un grupo de auditados seleccionados por alguna característica, conocimientos sobre un tema en especial o necesidad de la auditoría, a fin de ir conformando sus opiniones (iguales o diferentes); como si fuera un panel de libres aportaciones, en donde cada participante va opinando hasta llegar a consensos o diferencias que ayudan al auditor a captar la información que requiere.

Estas encuestas también se aplican con otras técnicas de manejo de grupos, como tormenta de ideas, corrillos, mesa redonda, Phillips 66 o cualquier otra técnica de manejo de decisiones grupales, según la habilidad del auditor para aplicarlas y los resultados que espera obtener con este tipo de encuestas.

9.3.6.2 Encuestas de análisis

Son las encuestas que se realizan para conocer las opiniones de los auditados y de los supuestamente expertos en algún tema especializado de sistemas, partiendo de un examen previo de los temas que interesa investigar, con lo cual se busca comprobar o en su caso refutar un tema en estudio.

Este tipo de encuestas es muy útil para analizar bajo una óptica específica los datos, la información especializada o algún tema de interés especial para el auditor. Claro está, tomando en cuenta las opiniones y comentarios de los auditados y de los especialistas encuestados.

9.3.6.3 Encuestas de libre albedrío

Son las encuestas en las que la opinión del encuestado se analiza sin ningún plan ni método concreto, y se utilizan para que el auditor pueda examinar posibles opiniones y comentarios expresados libremente y sin limitaciones. En algunos casos, estas encuestas sirven para saber hacia dónde enfocar la auditoría.

9.3.6.4 Encuestas de confirmación

Ese tipo de encuestas sirve para que el auditor confirme, valide o rechace información obtenida previamente sobre algún tema en especial, ya sea aplicando la encuesta a los responsables directos de algún fenómeno o a las personas que pueden validar esa información.

Estas encuestas son muy similares a las que tratamos en la sección 9.1.3.3; sección 9.2.2.6 y sección 9.3.3.6.

9.3.6.5 Encuestas de investigación

Este tipo de encuestas sirve para que el auditor obtenga información sobre algún aspecto que desconoce del área o tema que va a evaluar, con la colaboración, forzada o

libre, del encuestado; además, estas encuestas le ayudan a indagar, corroborar o reafirmar algún punto concreto con las opiniones y comentarios de los encuestados.

Podríamos seguir explicando los tipos de encuestas que se pueden utilizar en una auditoría de sistemas, pero sería ocioso y a la vez inoperante, ya que el auditor debe aplicar estas técnicas y métodos de encuesta de acuerdo con sus necesidades específicas de información, con su experiencia y conocimientos en el manejo de esta herramienta, y con su habilidad para el manejo de opiniones. Por tal razón dejaremos hasta aquí el análisis de esta herramienta.

9.4 Observación

Una de las técnicas más populares, de mayor impacto y más utilizadas para examinar los diferentes aspectos que repercuten en el funcionamiento del área de informática o del propio sistema, es la aplicación de diversas técnicas y métodos de observación que permiten recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas.

Con el propósito de entender esta herramienta de la auditoría de sistemas, a continuación presentaremos algunas definiciones de observación, y después propondremos algunos enfoques concretos sobre su uso en la auditoría de sistemas.

Observación

"Acción y efecto de observar [...] Atención que se presta a ciertas cosas [...] Reflexión [...] Explicación de algo [...] Estudio notable sobre algunas cosas [...] Estudiar la marcha de [...]"[1]

"Es la acción de observar, de mirar detenidamente [...] La observación puede ser estudiada desde el investigador que observa, que mira detenidamente y desde lo observado, lo mirado detenidamente [...] significa también el conjunto de cosas observadas, el conjunto de datos y el conjunto de fenómenos..."[2]

Observar

"Del latín Observare: *Ejecutar lo prescrito [...] Considerar con atención [...] Espiar [...] Notar [...] Advertir, reparar [...] Percibir [...] Atisbar [...] Mirar."*[3]

"Examinar con atención, analizar [...] Advertir, reparar [...] Mirar con atención y recato, observar [...] Observar y cumplir lo mandado."[4]

Arias Galicia aporta

"A fin de recolectar datos suficientes, se hace necesario, precisamente, observar los fenómenos en cuestión con objeto de determinar si existe [...] la palabra observación porque en última instancia los sentidos del investigador deben percibir los eventos directamente o por medio de registros realizados por algún aparato o los efectos del pro-

pio sujeto [...] En las ciencias de la conducta nos observamos a nosotros mismos y a otras personas. En el primer caso háblese de introspección (ver hacia adentro) y en el segundo de extrospección (ver hacia afuera). Ambas no necesariamente excluyentes sino, en realidad, se complementan en muchos casos."[5]

Como podemos deducir a partir de las definiciones anteriores, la acción de observar es el hecho de examinar, analizar, advertir o estudiar algo; en este caso, cuando el auditor de sistemas aplica esta técnica, lo que hace es observar todo lo relacionado con los sistemas de una empresa, con el propósito de percibir, examinar o analizar lo relacionado con los eventos que se presentan en el desarrollo de las actividades de un sistema, de un centro de sistematización, de la operación de la computadora o el desempeño de cualquiera de las actividades que le permitirán evaluar el cumplimiento de las operaciones del sistema.

La observación se puede hacer desde diferentes puntos de vista y con diversas técnicas y métodos que analizaremos a continuación.

9.4.1 Observación directa

Es la inspección hecha directamente en el contexto donde se presenta el hecho o fenómeno observado, a fin de contemplar todos los aspectos inherentes al comportamiento, conducta y características de ese ambiente. En este caso, el observador (el auditor de sistemas) entra en contacto directo con el fenómeno observado, analizando su comportamiento de dos maneras; por un lado permanece aislado al observar el comportamiento del hecho o fenómeno (*sistema*) que va a estudiar, y por otro lado participa en dicho fenómeno al observarlo. Lo importante es observar en forma directa lo que acontece en el sistema o área de sistemas auditada. A continuación presentamos algunos ejemplos de observación:

Observar la forma en que ingresan los usuarios al centro de cómputo, a fin de conocer las medidas de seguridad establecidas para el acceso a esta área.

Observar el comportamiento de los usuarios de un sistema, a fin de evaluar su forma de utilizarlo.

La observación (monitoreo) hecha por el administrador de una red acerca del trabajo que están realizando los usuarios del sistema, a fin de validar las bases de datos que éste está utilizando, sus privilegios y restricciones en el sistema, siempre que la observación no sea oculta, es decir, que el usuario sepa lo que hacen él y el administrador. En caso contrario, sería una observación oculta.

Este tipo de observaciones se aplica espontánea e intuitivamente en cualquier tipo de auditoría; recordemos que la principal función del auditor es observar el funcionamiento de lo que evalúa; en este caso, lo que observa del ambiente de sistemas en forma franca, abierta y concisa.

9.4.2 Observación indirecta

Es la observación del hecho (gestión informática) o fenómeno (sistema) en estudio, pero sin que el observador (auditor) entre en contacto directo con el aspecto observado, sino que lo examina por medios indirectos, ya sea por referencias o comparaciones; para lograr lo anterior, el auditor se vale de observaciones ajenas al hecho, sin entrar en contacto ni participar por ningún motivo en su comportamiento, actividades o características.

En estos casos, la función del auditor está encaminada a observar las repercusiones del fenómeno contemplado, pero no estudia el propio fenómeno sino su repercusión, comparando lo observado con otro fenómeno similar o con las características que debería tener, tomando como referencia otra manifestación similar.

Este tipo de observación es muy utilizado en una auditoría de sistemas para evaluar el comportamiento de un sistema. A continuación presentamos algunos ejemplos:

El monitoreo de las actividades de los usuarios en una red de cómputo; aquí no se observa directamente el sistema, sino su operación.

El seguimiento de las fases de desarrollo de un nuevo sistema; aquí no se evalúa el desarrollo de los sistemas, sino las fases terminadas de los proyectos de sistemas de la empresa.

La prueba de escritorio para corroborar la programación adecuada de un sistema. Aquí se siguen las instrucciones del sistema pero en el escritorio, como si el sistema estuviera funcionando, pero no se siguen en el sistema cuando éste está funcionando.

Un estudio paralelo de mercado para la adquisición de equipo de cómputo. Es hacer un estudio igual al que se lleva a cabo, pero sin que se note que se está realizando.

Éstos son algunos de los muchos ejemplos de observación indirecta, la cual no debemos confundir con la observación oculta, ya que aquí se observa el fenómeno pero no se oculta que se está observando, e incluso en algún momento se puede comparar con el fenómeno que se está estudiando.

9.4.3 Observación oculta

Es cuando el observador (auditor), por las necesidades propias de la evaluación, permanece oculto para observar el fenómeno que está auditando (sistema o gestión informática), sin que los involucrados noten su presencia; con este tipo de observación se pretende estudiar el comportamiento y las características del fenómeno en su ambiente natural, sin que sufra ninguna alteración ni influencia exterior. La presencia del auditor siempre interfiere, aunque no participe en el fenómeno observado.

Este tipo de observación es muy útil en una auditoría de sistemas, ya que es muy similar al señalado en el punto anterior, salvo que aquí nadie sabe que el auditor está

observando, entonces éste puede observar con absoluta libertad el comportamiento del hecho o fenómeno auditado, logrando así identificar el verdadero comportamiento de los sistemas.

9.4.4 Observación participativa

En este tipo de observación, el observador (auditor) tiene la oportunidad de formar parte del fenómeno observado (del sistema o la gestión informática) como si fuera un integrante del mismo. Esta participación le permite observar más de cerca las características, costumbres, comportamiento y actuación del fenómeno observado; además, como pertenece a su ambiente, puede comprobar las modificaciones y variaciones determinadas previamente del comportamiento y conducta de los hechos.

Este tipo de observación es muy útil cuando se pretende probar el comportamiento del sistema, debido a que el auditor diseña algunos experimentos con el único propósito de conocer el comportamiento de dichos sistemas bajo ciertas condiciones. A continuación presentamos algunos ejemplos:

Procesamiento del sistema actual con datos ficticios. A fin de evaluar su comportamiento, pero con datos que no pueden alterar el sistema.

Modificación de las operaciones y rutinas básicas del proceso. Para que el auditor evalúe la repercusión de los cambios en el sistema; siempre que se hayan tomado las medidas pertinentes, como el respaldo del programa original y los cuidados debidos.

Cualquier otra transformación programada de la operación normal del sistema. A fin de saber cuál es su comportamiento bajo otras condiciones.

También se pueden alterar otros aspectos del área de sistemas, como el desarrollo de proyectos, la codificación de instrucciones, las instalaciones físicas de energía eléctrica, voz y datos, las actividades de los usuarios y muchos otros aspectos, siempre que el auditor participe directamente en estos experimentos, a fin de valorar la conducta, características y alteraciones que sufre el sistema, su operación e incluso los usuarios y empleados del área de informática con esos cambios.

9.4.5 Observación no participativa

En ésta, el observador (auditor) evita participar en el fenómeno bajo estudio (el sistema o la gestión informática), a fin de no impactar o contaminar con su presencia el comportamiento, características y desenvolvimiento normal del fenómeno observado. El propósito de este tipo de observación es saber, de una manera más confiable y veraz, cómo se comporta el fenómeno.

No debemos confundir este tipo de observación con la observación indirecta ni con la oculta, pues aquí el auditor observa el fenómeno sin tener ninguna participación en el mismo, es decir, puede haber alteraciones en el sistema, pero no son producto

de la evaluación sino de la propia operación, sólo que aquí el auditor observa el fenómeno y toma nota de las alteraciones en el comportamiento, pero él no las provoca. A continuación presentamos algunos ejemplos:

El comportamiento en los simulacros y pruebas del plan de contingencias. El auditor observa las pruebas y puede tomar nota de las alteraciones que sufren, pero se abstiene de participar e inclusive de opinar.

Las pruebas de instalación de programas y paqueterías. Aquí sólo observa las variaciones y cambios que se van realizando en la instalación, y aunque nota deficiencias en esas pruebas, sólo observa y evita opinar y participar en ellas.

Las modificaciones en la aplicación de los presupuestos del área de sistemas. Aquí sólo valora que se apliquen correctamente los presupuestos, pero si hay cambios y alteraciones en dicha aplicación, sólo toma nota pero no hace comentarios ni sugerencias. Si es el caso, lo anota en su informe, pero no en la observación.

Lo fundamental de este tipo de observación es que el auditor sólo capta posibles cambios en los que él no sugiere ni participa, sino que sólo observa cómo se presentan y cual es su comportamiento.

9.4.6 Introspección

En las ciencias sociales la introspección se entiende como el examen interno del comportamiento y actuación del sujeto observado (sistema); en una auditoría se entiende como la observación interna del fenómeno, es decir, es la investigación en la que se observa desde el interior del propio hecho en estudio. Su propósito es entender mejor el comportamiento del fenómeno, sus características y su desenvolvimiento.

En este caso el auditor observa el hecho o fenómeno (sistema, gestión informática u operación) desde su interior, a fin de conocer su comportamiento y sus posibles alteraciones desde lo íntimo del fenomeno. Con lo anterior puede hacer una evaluación más directa y profunda. A continuación presentamos algunos ejemplos:

Asistir a los cursos de capacitación de los usuarios. Aquí puede participar en los cursos o sólo estar como observador; de esta manera puede saber desde el interior cómo se da la capacitación en el área de sistemas.

Estar presente en el análisis del sistema actual para un nuevo diseño de sistemas. Aquí sólo se dedica a observar el comportamiento de los analistas, evitando alterar con su presencia el desarrollo de esta fase del diseño de sistemas. Con ello puede observar, desde el mismo proceso, qué tan oportunamente se cumple esta fase, y si se emplean las herramientas y metodologías adecuadas en los nuevos proyectos de sistemas de la empresa.

Monitorear las aplicaciones y actividades de los usuarios. Aunque ésta también puede ser una observación oculta, aquí el auditor observa, desde lo más profundo del sistema, el comportamiento de los usuarios y el aprovechamiento del sistema.

Modificar la nómina de cualquier empleado. En este tipo de pruebas, que deben ser planeadas previamente y estar documentadas perfectamente, el auditor altera algún ingreso, sueldo o cualquier otro aspecto de la nómina (que supuestamente no podría alterar), a fin de evaluar las repercusiones de estos cambios. Con ello conoce la seguridad y confiabilidad del sistema desde el interior de éste.*

*Accesar a los niveles y privilegios que se pueda de una red. En estos casos, el auditor evalúa las restricciones, contraseñas y la seguridad de los sistemas de red, y evalúa de paso la protección y confiabilidad de los datos y las restricciones de acceso a los niveles permitidos según los privilegios de los usuarios.***

Los niveles más comunes de acceso para los usuarios de sistemas son los siguientes:

***Consulta**: en este nivel, el usuario sólo puede entrar a consultar la información.*

***Captura de datos**: en este nivel, el usuario sólo puede alterar los datos que permite el sistema.*

***Modificación de programación y datos**: en este nivel, el usuario tiene el privilegio de modificar datos sustanciales del sistema, e incluso del programa.*

***Administrador de la red**: en este nivel, el administrador tiene todos los privilegios para alterar libremente los datos, programas, niveles de privilegios y demás acciones del sistema.*

Los anteriores son sólo algunos de los muchos casos en los que el auditor puede valorar los fenómenos que estudia desde el interior de éstos; esto le permite captar la esencia de sus operaciones y su comportamiento real.

9.4.7 Extrospección

En este tipo de observación, el observador (auditor) realiza la inspección desde un punto de vista totalmente externo al fenómeno que está analizando, es decir, hace la observación sin entrar en contacto con el interior del hecho observado (el sistema). El propósito es comprender la actuación del fenómeno en relación con otros fenómenos similares que le servirán de parámetro para compararlo.

Estas pruebas son muy útiles para el auditor, ya que le permiten valorar el comportamiento de los sistemas (programas, paqueterías, gestión administrativa, gestión informática, operación, instalaciones, etc.) comparándolo con el comportamiento de otros sistemas similares. Con ello puede opinar sobre el comportamiento del sistema,

* Teóricamente, estos sistemas son inviolables y nadie, ni siquiera el auditor, puede entrar en ellos, mucho menos hacerles cambios si no existe la debida autorización para ello.

** En teoría, el auditor sólo puede accesar a los niveles que le permita el administrador; por ningún concepto puede accesar a otros niveles sin esa autorización. La prueba consiste en entrar hasta donde pueda sin la aprobación de los directivos; en cada caso debe documentar los niveles de acceso y la posible alteración que haga en el sistema de red, para después reportar lo anterior en su informe.

no desde el punto de vista de cómo funciona, sino desde el punto de vista de cómo debería funcionar.

Sin embargo, debemos tomar en cuenta que el fenómeno observado es el que está siendo auditado y que tiene un comportamiento específico de acuerdo con las características de operación de la empresa, y aunque otro sistema esté mejor aplicado, se debe comparar el comportamiento de ambos para sugerir mejoras en la operación del sistema observado, y no sólo para criticar sus deficiencias.

9.4.8 Observación histórica

Este tipo de observación se basa en el registro de los hechos pasados, a fin de analizarlos y proyectar hacia el futuro los resultados obtenidos, además, el observador (auditor) inspecciona los registros de operaciones y actividades pasadas, históricas, para estudiar su comportamiento pasado. A continuación presentamos algunos ejemplos:

La revisión de la bitácora de los servicios de mantenimiento correctivo o preventivo que se realizan durante un periodo determinado. En este caso, las observaciones que se realizan son propiamente la revisión a las observaciones obtenidas de quienes se registraron en las bitácoras.*

De hecho, esto es muy similar a la auditoría financiera, en la que se observan los hechos registrados con anterioridad.

9.4.9 Observación controlada

En este tipo de observación, el observador (auditor) tiene libre acceso para manipular, de manera controlada, las variables que afectan al fenómeno estudiado (procesamiento del sistema, programas, paqueterías, forma de realizar las operaciones, etc.), a fin de analizar los cambios de conducta, los resultados y las características que se presentan al variar esas condiciones. El propósito de esta técnica es observar directamente el impacto que tienen las variaciones que se dan en el fenómeno, es decir, manipulando los cambios que se van dando en el hecho estudiado. Es indispensable documentar estas variaciones y, después de que se hayan presentado, regresar el fenómeno a su estado natural.

Esta observación es muy similar a las mencionadas anteriormente, sólo que en ésta el auditor debe planear perfectamente las modificaciones que va a realizar, con el propósito de no alterar permanentemente el sistema en estudio. Lo ideal es probar las modificaciones de manera simulada sin alterar para nada el sistema.

* En el ambiente específico de informática, al mantenimiento de sistemas se le ha clasificado en dos partes: el llamado **mantenimiento preventivo,** el cual pretende evitar que se presenten problemas en los sistemas, aplicándose las medidas preventivas por medio de un programa, previamente establecido. Mientras que, el **mantenimiento correctivo,** corrige los desperfectos del sistema cuando éstos ya ocurrieron. Se supone que el primero es mantenimiento para prevenir y el segundo es para corregir desperfectos.

9.4.10 Observación natural

En esta observación, a diferencia de la anterior, el observador (auditor) sólo propone las variaciones que va a estudiar, pero no las manipula de ninguna manera, ya que sólo busca observar la conducta, los resultados y características del fenómeno en estudio, pero en su ambiente natural, con sus propias variaciones, sin alterarlas voluntaria o involuntariamente. Es decir, es la observación de la conducta del fenómeno estudiado tal y como es, sin alterarlo.

En un aspecto más práctico, la observación, en cualquiera de sus variaciones antes estudiadas, es una de las principales herramientas que se pueden utilizar en una auditoría de sistemas, debido a que por medio de las técnicas y métodos de observación, el auditor puede examinar todos los aspectos que intervienen en el funcionamiento de un sistema, de su gestión administrativa y en el comportamiento del área de cómputo; ya sea en la operación del propio equipo, en el desarrollo de las actividades y el cumplimiento de las funciones del personal del área de sistemas, en el desarrollo e implantación de nuevos sistemas, en las medidas de seguridad y previsión de contingencias del centro de información, o para estudiar cualquiera de los demás aspectos de la actividad del área de informática susceptibles de auditar.

Es evidente que con la aplicación de esta técnica, el auditor de sistemas recolecta información muy valiosa que le ayuda a emitir un juicio sobre el funcionamiento de cada uno de los aspectos que debe auditar.

Como parte del análisis de este punto, a continuación señalaremos algunos de los aspectos más relevantes de los sistemas de información en los que se puede utilizar la técnica de observación, buscando cubrir algunos de los aspectos más concretos para evaluar en dichos sistemas. Cabe aclarar que el uso de esta herramienta básica para la auditoría de sistemas es sólo una sugerencia, ya que, como hemos citado a lo largo de estas explicaciones, las técnicas y métodos de observación se aplicarán de acuerdo con las necesidades y características propias de cada centro de información.

La observación del comportamiento del sistema, en cuanto al funcionamiento del equipo de cómputo, sus periféricos y equipos asociados, así como de su operación y uso de éstos.

La observación de la operación del sistema de procesamiento de datos y el uso de sus lenguajes, programas, paqueterías e información.

La observación de la existencia y aplicación de las medidas de seguridad establecidas en el centro informático para controlar el acceso del personal informático, los usuarios y de personas ajenas al sistema, a los programas, a la información y al propio sistema.

Observar los sistemas, protección y prevención de contingencias que repercuten en los sistemas de cómputo, los equipos, instalaciones, programas e información.

Observar la existencia y cumplimiento de los planes de contingencias para salvaguardar los sistemas, archivos y la información procesada en ellos.

Observar el desarrollo y cumplimiento de las funciones y actividades de los funcionarios, del personal del área y de los usuarios del sistema.

Observar la administración y control de proyectos, el desarrollo e implantación de los nuevos sistemas y el uso de las metodologías para su análisis y diseño.

Éstos son sólo algunos de los muchos ejemplos de la aplicación de esta herramienta de auditoría, adaptándola a las características y variaciones que hemos visto, y usándola de acuerdo con las necesidades de la auditoría de sistemas.

9.5 Inventarios

Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando, a fin de saber la cantidad existente de algún producto en una fecha determinada y compararla con la que debería haber según los documentos en esa misma fecha. Consiste propiamente en comparar las cantidades reales existentes con las que debería haber para comprobar que sean iguales o, en caso contrario, para resaltar las posibles diferencias e investigar sus causas.

Esta técnica se utiliza principalmente en las auditorías de carácter financiero, operativo y administrativo, aunque también se utiliza en otros tipos de auditorías. Sin embargo, su realización consume muchos recursos, ya que es necesario conocer los bienes existentes, los cuales deben ser contabilizados físicamente y registrados en documentos formales para compararlos con algún registro formal de los bienes que debería haber.

Con la aplicación de esta herramienta de la auditoría tradicional, el auditor de sistemas también puede examinar las existencias de los elementos disponibles para el funcionamiento del área de informática o del propio sistema, contabilizando para ello los equipos componentes de los sistemas de cómputo, la información y datos de la empresa, los programas, periféricos, consumibles, documentos, recursos informáticos y los demás aspectos cuya existencia real se quiere conocer, a fin de comparar dicha existencia (cantidad) con registros formales de la existencia que debería haber.

En la auditoría de sistemas, este método de recopilación de información ayuda enormemente a realizar una evaluación adecuada de la gestión administrativa del área de sistemas, así como del aprovechamiento, custodia y control de los bienes informáticos que hay en dicha área. Sin embargo, por lo *supuestamente técnico* del ambiente de sistemas, así como por la poca importancia que se suele dar a estos aspectos *considerados como administrativos*, la realización de estos inventarios de bienes asignados al área de sistemas se deja en segundo plano, a pesar de su importancia para saber lo que tiene la empresa para realizar las actividades de cómputo, tanto por su monto y forma de uso, como por lo valioso de los recursos y lo que representan como bienes de la misma empresa.

Con el propósito de entender cómo se utiliza esta herramienta, a continuación presentamos algunas definiciones de inventario:

Inventario

"Lista ordenada de las cosas de valor de una persona o sociedad [...]"[6]

"El inventario incluye todos los stocks de artículos y materiales que posee una compañía y utiliza en el proceso de manufactura de productos o para ofrecer un servicio [...] No obstante, numerosos autores incluyen los suministros de equipos, maquinarias, oficinas, cantina, bienestar, y de hecho todo lo que sea propiedad de la empresa [...]"[7]

En el caso de la auditoría de sistemas, definiremos el inventario de la siguiente manera:

> *Es la recopilación de todos los bienes y materiales que posee una empresa, a fin de comparar las existencias reales con los registros contables.*

En un plano más práctico para la auditoría de sistemas, a continuación presentamos los principales tipos de inventarios aplicables en el ambiente de sistemas computacionales, asimismo, debido a su importancia, los analizaremos para saber cómo utilizarlos adecuadamente y obtener buenos resultados.

Inventario del software
Inventario del hardware
Inventario de consumibles
Inventario de documentos
Inventario de inmuebles, instalaciones, mobiliario y equipos de sistemas
Inventario del personal informático
Inventario de bases de datos e información institucional

9.5.1 Inventario del software

Uno de los documentos fundamentales para una auditoría de sistemas es el inventario de programas, lenguajes, paqueterías, sistemas operativos y cualquier otro software utilizado en la institución para el procesamiento de su información y la operación de sus sistemas computacionales. El propósito de este inventario es evaluar la existencia del software, su uso adecuado, su resguardo y aprovechamiento en el área de sistemas, incluyendo las licencias para su uso, registros y demás características.

Este inventario se realiza mediante un documento formal en el que se detalla todo el software que está instalado en los sistemas de la empresa, incluyendo todas sus características, versiones, formas de presentación e incluso número de licencias para su uso. Además, en este inventario también se incluye a los responsables del aprovechamiento y resguardo del software, así como la instalación del software no autorizado (pirata), las razones para utilizarlo y el control que hay de los programas de la empresa.

El auditor de sistemas realiza este inventario con el propósito de contar con un registro pormenorizado del total de software institucional que tiene la empresa, ya sea en cada una de sus computadoras, en sistemas mayores, en redes de cómputo, sistemas multiusuarios o en todo el sistema; también puede realizar el inventario del soft-

ware que no esté instalado o del utilizado en cualquier equipo de otras áreas de la empresa. Asimismo, puede inventariar tanto el software adquirido de terceros, el llamado software comercial, como el desarrollado en la propia institución, llamado software desarrollado, o el que haya sido adquirido de cualquier otra forma.

El inventario del software se tiene que realizar invariablemente en dos partes, por un lado el recuento físico del software de los sistemas de la empresa, y por otro la comparación de ese recuento físico con lo que hay en los registros oficiales de la empresa. Supuestamente, estos registros deben ser iguales al recuento físico; en caso contrario, se deben establecer las diferencias entre ambos. A continuación analizaremos ambas partes por separado.

9.5.1.1 Inventario físico del software

Es el recuento físico, diríamos lógico, de todos los programas de aplicación, sistemas operativos, paqueterías, lenguajes y demás software instalado en los sistemas computacionales de la empresa; este recuento se hace con el propósito de identificar el software con el que cuenta el área de sistemas o los demás equipos de la empresa, ya sea del que tenga licencia o del instalado sin el permiso correspondiente (*conocido como software pirata*).

El auditor realiza este inventario introduciéndose al área de sistemas, identificando el software instalado en el equipo de cómputo, listando su existencia en papel o en cualquier otro medio informático en el cual contemple con lujo de detalles todo el software que sea considerado como programas, paquetes de aplicación y explotación, lenguajes, sistemas operativos y demás programas institucionales o adquiridos de terceros. También debe incluir en dicho listado todos los programas considerados como ejecutables o los considerados como aplicaciones, inclusive los juegos y utilerías.

FECHA DD MM AA 28 03 96 — **HOJA** 12 de 29

EMPRESA: Bonzai Audi Area Auditada *Centro de Cómputo*
PERÍODO: 04 marzo 96 al 08 marzo 96
RESPONSABLE: Claudia de León Ramírez

Inventario de Software

REF	Software	Versión	Núm. Inventario	Licencias	Presentación	Asignado a	Localización
W01	Windows NT	311	09 234-1	20	CD-ROM	C. Cómputo	Servidor 1
W02	Office	95	09 334-1	1	CD-ROM	C. Cómputo	Servidor 1
W03	Office	95	09 334-2	1	CD-ROM	Contabilidad	Finanzas
W04	Office	97	09 334-2	1	CD-ROM	Diseño	Producción
W05	Office	97	09 334-2	1	CD-ROM	R. Humanos	Admos.
BD 1	Easy Case	12	15 234-1	3	8 Disk	C. Cómputo	Desarrollo
BD 2	Informix	14	15 345-3	1	10 Disk	C. Cómputo	Desarrollo
SO 1	MS-DOS	60	01 565-2	1	3 Disk	C. Cómputo	Desarrollo
SO 2	Unix	30	01 456-3	1	CD-ROM	C. Cómputo	Desarrollo

En algunos casos, el auditor debe tratar de identificar el software que está instalado a simple vista y el que está escondido, así como el que estuvo instalado en el sistema de cómputo, sin importar que éste haya sido escondido o borrado al momento de hacer el levantamiento del inventario. Esto se logra mediante el uso de las utilerías modernas que permiten al auditor identificar y recuperar los archivos y programas borrados del sistema permanente de almacenamiento del sistema computacional. Lo anterior se hace con el propósito de evaluar la forma en que se usa este software.

En el cuadro anterior presentamos un prototipo del documento que se debe utilizar para hacer el inventario físico del software; éste incluye los detalles mínimos que se deben considerar en dicho inventario.

9.5.1.2 Registros existentes del inventario del software

Una vez realizado el inventario físico del software, el siguiente paso es realizar la revisión documentada del mismo; el software debe estar registrado en los documentos formales de la empresa, ya sea en los registros contables, facturas o en cualquier otro registro que avale que es propiedad de la empresa, así como el derecho de uso y explotación de los sistemas adquiridos de terceros o de los desarrollados en la empresa, incluyendo los lenguajes, programas de explotación y aplicación, paqueterías, sistemas operativos y demás software encontrado en la misma.

Cabe destacar que esta revisión documental del software se hace para comprobar que el software detectado en el inventario físico realmente corresponda a lo que se encuentra registrado en la empresa. Casi siempre se compara con las facturas y notas de adquisición, los registros contables y cualquier otro documento oficial que avale la posesión del software. Incluso debe haber documentación comprobatoria que avale el desarrollo de los propios sistemas en la empresa.*

Con esta comparación se pueden obtener los siguientes resultados:

Que no existan diferencias y que la empresa tenga las licencias y registros correspondientes para el software instalado.

En estos casos, el auditor debe comprobar que coincida el inventario físico del software con los registros del mismo. Éstos pueden ser localizados en contabilidad, en registros documentales del área de sistemas, en las propias licencias o en cualquier documento que a criterio del auditor avale la existencia del software.

Que haya software instalado en algún sistema sin que la empresa tenga el registro y la licencia correspondientes.

* En la práctica, las facturas que amparen la adquisición del software deben permanecer en el área contable, pero las licencias de uso, en el área de sistemas; el auditor debe verificar la ubicación de estas licencias y las razones para que permanezcan en ese lugar, así como el resguardo de las mismas.

Cuando ocurre esta situación, se debe investigar por qué la empresa carece de los registros oficiales para la instalación y explotación del software detectado en los sistemas computacionales, lo cual puede ocurrir por los siguientes factores:

Que haya sido adquirido e instalado en forma ilegal con el conocimiento de los responsables del área de sistemas.

Que la persona responsable del sistema haya instalado el software en forma ilegal, sin el conocimiento de los responsables del área de sistemas.

Que se desconozca dónde está su documentación oficial.

Que esté instalado doblemente sin el permiso correspondiente (con una sola licencia).

Que la empresa tenga el registro y la licencia del software y éste no esté instalado.

Es cuando por alguna causa imputable al área de sistemas (o al responsable del sistema), el software que aparece en los documentos oficiales no está instalado en los sistemas computacionales; en este caso, el auditor debe averiguar las razones de esto último; entre algunas de estas consideraciones podemos encontrar lo siguiente:

Que sea obsoleto y que ya no se requiera su instalación en el área de sistemas, pero que aún no se haya dado de baja del área.

Que haya sido extraviado o sustraído del área de sistemas, y que dicha desaparición no haya sido reportada.

Que haya sido extraviado o sustraído del área de sistemas, y que dicha desaparición sí haya sido reportada, pero que aún siga vigente en documentos.

Que esté registrado en documentos, pero que por cualquier razón no haya sido entregado en el área de sistemas.

Que haya software instalado sin que la empresa tenga el registro y la licencia correspondientes, y que la empresa tenga el registro y la licencia del software y éste no esté instalado.

Este caso es la combinación de las dos situaciones que analizamos anteriormente, y se dan los casos planteados en ambas.

9.5.2 Inventario del hardware

Otro de los aspectos fundamentales que debe ser considerado en una auditoría de sistemas es el inventario de los sistemas computacionales y de sus componentes y periféricos físicos utilizados en la institución para la captura de datos, el procesamiento de la información y la emisión de sus resultados. El propósito es evaluar su uso adecuado, su resguardo, su aprovechamiento y el estado en que éstos se encuentran; incluyendo las instalaciones internas y los componentes físicos de los sistemas computacionales.

Igual que en el punto anterior, este inventario se realiza mediante un documento formal, en el que se deben detallar todas las características del hardware que la empresa tiene a su disposición: *la marca, modelo, características propias del sistema, modalidades de procesamiento, velocidad, número y tipos de memorias, sistemas adicionales de almacenamiento, componentes asociados al propio sistema, e incluso periféricos que complementen su uso adecuado*. Además, en este inventario también se anota a los responsables del aprovechamiento del hardware, así como la existencia de sus resguardos correspondientes.

El auditor realiza este inventario con el propósito de tener un registro pormenorizado del total de hardware que tiene la empresa, ya sea en cada una de sus áreas, en todo el sistema, en sistemas mayores, redes de cómputo, sistemas multiusuarios o en forma individual; también puede realizar el inventario del hardware que no está en el área de sistemas de la institución.

Es importante que en este inventario también se realice la evaluación de los resguardos que existen para la asignación de este hardware, así como la identificación del responsable de su uso, ya que estos sistemas pueden estar asignados al responsable de un área o cada uno a una persona en específico.

El inventario del hardware también se tiene que realizar invariablemente en dos partes, por un lado el recuento físico del hardware, y por otro la comparación de ese recuento físico con lo que hay en los registros oficiales de la empresa, a fin de encontrar las posibles diferencias entre ambos. A continuación analizaremos por separado ambos tipos de inventarios.

9.5.2.1 Inventario físico del hardware

Es el recuento físico de todos los sistemas computacionales instalados en el área de sistemas, o de todos los equipos para el procesamiento de información disponibles en las demás áreas de la institución que cuentan con sistemas computacionales; dicho recuento se hace con el propósito de identificar el total del hardware que tiene la empresa, ya sea del que tenga una administración de sistemas de tipo centralizado, desconcentrado, compartido o independiente, así como de su conservación, custodia y formas de resguardo. El auditor realiza este inventario de muy distintas maneras, entre las cuales tenemos las siguientes:

Inventario individual de los equipos, contándolos uno por uno, así como sus componentes, tanto internos como externos, e incluyendo los periféricos y demás elementos que integran dichos equipos como una sola unidad.

Inventario global del hardware, contando en forma global los sistemas de cómputo, después sus componentes, posteriormente sus periféricos y también por separado todos los elementos adicionales a los sistemas.

Cuando el auditor realiza el inventario físico, en ambos casos tiene que identificar plenamente el hardware instalado como equipo de cómputo, detectando totalmente su

presencia en el área de sistemas que esté auditando, o en cualquier área que cuente con estos sistemas; además tiene que anotar en papel o en cualquier otro documento informático dichos datos. En este listado se tienen que contemplar, con lujo de detalles, todos los aspectos que integran el hardware considerado como sistema computacional, incluyendo en dicho listado los elementos tangibles que de alguna manera sean considerados como componentes directos o asociados a los propios sistemas computacionales.

A continuación presentamos un ejemplo de este inventario, considerando los detalles mínimos que debe contener.

AUDITORÍA EN SISTEMAS COMPUTACIONALES

DEL	28	3	98
AL	31	4	98

EMPRESA: Universidad
AUDITOR: Ma. Araceli Arceo Gálvez

PERÍODO: 01 al 16 de marzo de 1998

ÁREA AUDITADA: Dirección de Informática y Estadística

Inventario individual de hardware

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
1	Conexión en RED				
2	Computador	ACER	AS-1002-1		
3	Procesador	Pentium II		IntelII	
4	Coprocesador	n/a			
5	Moderboad	PCI			
6	Velocidad procesador	233 Mhz			
7	RAM Instalado	48 MB			Inicia 6 adquisición 32
8	RAM Instalable	DIP (100-rs)			
10	Memoria Caché	256 KE			
11	Monitor	GOLDSART	AS-1002-2	1024 x 768	
12	Tarjeta de multimedia	Sond Elaster		32 bit	
13	Tarjeta de Sonido	n/a			
14	Tarjeta de vídeo	CIRRUS LOGIC		4 MB	
15	Tarjeta de RED	NOVELL	Ra-20006	LM 4.0	
16	Tarjeta de TV	Pixel View	AS-1002-3		
17	Bocinas	GOLDSART	AS-1002-4	20 W	
18	Disco Duro	SEAGATE	AS-1002-5	1.2 GE	
19	CD-ROM	MITSUMI	AS-1002-6	4x-8x	
20	DVD				
21	CR-W				
22	Fax Módem	36.9 KEFS	AS-1002-7	Full duplex	
23	Impresora	HP 620	AS-1002-8	Color	
24	Teclado	Microsoft	AS-1002-9	AT-101	
25	Mouse	Microsoft	AS-1002-C		

9.5.2.2 Registros existentes del inventario del hardware

Una vez realizado el inventario físico del hardware, el siguiente paso es realizar la revisión documentada del mismo; el hardware debe estar registrado en los documentos

formales de la empresa, ya sea en los registros contables, facturas o en cualquier otro registro que avale que es propiedad de la institución.

Esta revisión documental del hardware se hace para comprobar que el equipo, periféricos y componentes detectados en el inventario físico, realmente corresponda a lo que se encuentra registrado en la empresa. Casi siempre se compara con las facturas y notas de adquisición, los registros contables y cualquier otro documento oficial que avale la posesión del hardware.

Con esta comparación se pueden obtener los siguientes resultados:

Que no existan diferencias y que la empresa tenga los registros correspondientes para el hardware instalado.

En estos casos coincide el inventario físico del hardware con los registros de ese mismo hardware.

Que haya hardware, equipos y componentes sin que la empresa tenga el registro y los documentos correspondientes.

Cuando ocurre esta situación, el auditor debe investigar por qué la empresa carece de los registros oficiales para la instalación y explotación del hardware detectado en los sistemas computacionales, lo cual puede ocurrir por los siguientes factores:

Que haya sido adquirido en forma provisional con el conocimiento de los responsables del área de sistemas.

Que la persona responsable de los sistemas haya instalado el hardware en forma provisional, sin el conocimiento de los responsables del área de sistemas.

Que se desconozca dónde está la documentación oficial del equipo, aunque éste se tenga físicamente.

Que haya sido prestado a algún usuario o proveedor, y que no se haya realizado la notificación correspondiente.

Que la empresa tenga el registro y los documentos del hardware, pero que no lo tenga físicamente.

Es cuando, por alguna causa imputable al área de sistemas, el hardware que aparece en los documentos oficiales no se encuentra físicamente en el área de sistemas o en el área que debería estar; entre algunas razones podemos encontrar las siguientes:

Que sea obsoleto y que ya no se requiera su uso en el área de sistemas, pero que aún no se haya dado de baja del área.

Que sea obsoleto y que ya no se requiera su uso en el área de sistemas, y que sí haya sido dado de baja del área, pero que aún siga vigente en documentos de la empresa.

Que esté descompuesto y fuera del área de sistemas, pero que no haya sido dado de baja del área y que no sea necesario notificar la situación.

Que haya sido extraviado o sustraído del área de sistemas, y que dicha desaparición no haya sido reportada.

Que haya sido extraviado o sustraído del área de sistemas, y que dicha desaparición sí haya sido reportada, pero que aún siga vigente en documentos.

Que esté registrado en documentos, pero que por cualquier razón éstos no hayan sido dados de baja ni entregados del área de sistemas al área contable.

Que esté prestado en forma externa y esto no haya sido notificado en documentos.

Que haya hardware instalado sin que la empresa tenga el registro y los documentos correspondientes, y que la empresa tenga el registro y los documentos del hardware, pero que no lo tenga físicamente.

Este caso es la combinación de las dos situaciones que analizamos anteriormente, y se dan los casos planteados en ambas situaciones.

Es importante que el auditor, al realizar las comparaciones entre el recuento físico del hardware y su registro en los documentos correspondientes, también evalúe que existan los resguardos correspondientes, debidamente actualizados y que estén asignados al personal que los utiliza, a fin de verificar el adecuado control de su asignación, protección y uso.

9.5.3 Inventario de consumibles

Otro de los inventarios que se debe realizar en una auditoría de sistemas computacionales es el inventario físico de todos los materiales que se consumen en el área de sistemas, a fin de conocer, valorar y resguardar todos los materiales que contribuyen al desarrollo de las actividades necesarias para el procesamiento de información de la empresa.

Este inventario es de carácter administrativo o financiero, debido a que se hace un conteo físico de los consumos normales de insumos de sistemas de la empresa, valorando contablemente las existencias, consumos promedios, periodicidad de abastecimientos, justificaciones de los faltantes y costos financieros de estos materiales, sin embargo, a pesar de que este inventario es de carácter contable, le ayuda al auditor de sistemas a valorar los activos del área de sistemas y a evaluar la forma en que se lleva acabo el control administrativo y los gastos de la empresa en este rubro, así como a determinar la razonabilidad de los gastos en materiales consumibles para dicha área.

9.5.3.1 Materiales que deben ser inventariados

Respecto a la forma de realizar este inventario, existen muchas técnicas y métodos utilizados en la auditoría contable; por esta razón, sólo señalaremos los principales rubros que deben ser inventariados como consumibles para el área de sistemas, los cuales serán clasificados de acuerdo con los siguientes materiales:

Inventario de medios de almacenamiento electromagnético

Disquetes
Cintas electromagnéticas
Casetes
CD-ROMs y CD-Rs
Otros medios

Inventario de material para impresión

Material para impresoras de matriz de puntos
Material para impresoras láser
Material para impresoras de inyección de tinta
Hojas stock y de consumo para impresión
Otros materiales especiales de impresión

Inventario de papelería y útiles de oficina

Materiales consumibles para oficina
Formas continuas y de consumo administrativo
Otros implementos para oficina
Materiales para mantenimiento y limpieza de oficinas

Inventario de refacciones y elementos para el mantenimiento de los sistemas

Tarjetas, procesadores, chips de memoria, etc.
Partes y refacciones para vídeo
Partes y refacciones para los periféricos externos del sistema
Partes y refacciones para los componentes y las conexiones internas del sistema
Diversas refacciones relacionadas con los sistemas

Inventario de otros consumibles para sistemas

Accesorios adicionales para los sistemas
Partes y refacciones eléctricas para mantenimiento de las instalaciones
Otros implementos auxiliares para los sistemas

9.5.3.2 Procedimiento para inventario de consumibles

El procedimiento para realizar este inventario es similar a los señalados para los inventarios anteriores, pero en el inventario de consumibles se deben seguir los siguientes pasos:

El primer paso es hacer el recuento físico de los diversos materiales que deben ser inventariados, aplicando cualquiera de las técnicas y métodos contables para levantar inventarios; generalmente se hacen conteos por cada grupo de consumibles.

A continuación se hace el análisis de los registros contables de los consumos de estos materiales.

Después se comparan los resultados del inventario físico y los datos obtenidos de la revisión documental, a fin de evaluar los registros de consumos y verificar diferencias y faltantes.

Después se elabora un estudio estadístico sobre el volumen de consumos, periodicidad y frecuencia de las reposiciones, estudios de consumos máximos y mínimos y otros aspectos estadísticos que permitan evaluar el aprovechamiento adecuado de estos materiales.

Finalmente se elabora una evaluación global sobre los costos financieros de los consumos, su aprovechamiento en el procesamiento de información, y en caso de haber faltantes de consumibles, la aclaración de esos faltantes.

Es evidente que cada auditor puede realizar el tipo de inventario de consumibles que más le convenga, incluso aprovechar el mismo que hace en la auditoría financiera.

9.5.4 Inventario de documentos

Este inventario se realiza para buscar los elementos de apoyo bibliográfico que contribuyan al buen desempeño de las actividades y tareas que se realizan en el área de cómputo; su propósito es verificar la existencia de documentos que apoyen y avalen la gestión administrativa de funcionarios, directivos, empleados y usuarios del centro de sistemas, así como la operación y el funcionamiento de los diversos sistemas instalados en el área de sistemas o en las demás áreas de la empresa.

Además de verificar si existen estos documentos, también se pretende evaluar si están a disposición de funcionarios, empleados y usuarios de los sistemas de la empresa para su consulta y si aplican en el desarrollo de sus tareas las técnicas y procedimientos establecidos en dichos documentos, así como la forma en que los utilizan.

La recopilación de información que aportan estos inventarios va más allá de verificar la existencia de documentación relacionada con los sistemas de la institución y su registro adecuado, ya que también se verifica, cómo ayudan a determinar si ese soporte documental sirve como respaldo y consulta para el funcionamiento correcto de los sistemas y el cumplimiento de las tareas y actividades de los funcionarios, empleados y usuarios del sistema de cómputo. Estos inventarios también sirven para verificar si el personal que está relacionado con los sistemas sabe de la existencia de dicha documentación, cada cuándo los consultan y cómo los aplican, así también para evaluar su elaboración, actualización y aplicación en los diversos trabajos que se desarrollan en el área de sistemas.

Para el mejor desarrollo de estos inventarios, a continuación mencionaremos los principales tipos de inventarios de documentos que se pueden realizar en una auditoría de sistemas computacionales, agrupándolos bajo el criterio de funcionalidad y uso de la información contenida en estos documentos.

9.5.4.1 Inventario de documentos administrativos

Con este inventario se busca evaluar toda la documentación relacionada con la gestión administrativa del área de sistemas, con lo cual el auditor podrá dictaminar si esa documentación sirve de soporte para el desarrollo y cumplimiento adecuados de las funciones y actividades administrativas encomendadas a los funcionarios, empleados y usuarios del sistema.

Estos documentos se pueden agrupar según el tipo de información que contienen.

Manuales de organización

El inventario de estos documentos se hace para verificar que existan y que esté plenamente difundida la estructura de organización del área de sistemas, las funciones de sus encargados, empleados y usuarios, así como los canales de autoridad y responsabilidad que regulan el trabajo en esta área.

Manuales de procedimientos administrativos

Este inventario también se hace para verificar la existencia de manuales e instructivos que regulen las acciones administrativas y los procedimientos normales de la operación que contribuyan a la obtención de información y emisión de resultados derivados del sistema; la información que contienen estos manuales se utiliza para identificar los procesos que se siguen en el área de sistemas, así como la forma en que se difunde el contenido de dichos manuales, su aplicación y cumplimiento, y para verificar que el personal que labora en el área desarrolle correctamente las actividades que indican estos manuales.

Manuales de perfil de puestos

Este inventario se realiza para verificar que existan los documentos formales que avalen los requerimientos establecidos para cada uno de los puestos del área de sistemas, así como para valorar las características, modalidades y demás aspectos inherentes a cada puesto, y para revisar si en el proceso de selección, capacitación y promoción de los empleados se cumple con lo normado en estos documentos. En algunos casos, estas auditorías también se hacen para revisar la existencia y aplicación de estos documentos en el área de sistemas y con el personal informático del área, así como para verificar su actualización permanente.

Otros manuales administrativos

Este inventario se realiza para verificar la existencia de todos los manuales e instructivos distintos a los antes señalados que regulan la actividad administrativa del área de sistemas, así como para verificar que dichos documentos se difundan y estén a disposición del personal, que éste los utilice en sus actividades y que sean actualizados constantemente.

9.5.4.2 Inventario de documentos técnicos para el sistema

Este inventario se realiza para verificar la existencia, difusión, uso y actualización de los manuales e instructivos técnicos que regulan la actividad específica de un sistema, así como la operación de los equipos, sistemas y procesamiento de datos del área. En algunos casos, este inventario se realiza para verificar si los usuarios de sistemas cumplen con lo especificado en estos documentos.

Podemos agrupar dichos inventarios bajo los siguientes aspectos relacionados con los principales manuales de sistemas de operación.

Manuales e instructivos técnicos del software del sistema

Es el inventario de los documentos con los que se regula la aplicación técnica de los programas, lenguajes, sistemas operativos, paqueterías y demás software instalado en el sistema, ya sea que dichos programas hayan sido desarrollados en la empresa o adquiridos a terceros.

Manuales e instructivos técnicos del hardware, periféricos y componentes del sistema

Este inventario se realiza con el propósito de verificar la existencia y uso de la documentación que auxilia en la operación de los equipos de cómputo, sus partes, conexiones, componentes internos, componentes asociados externos, periféricos y demás elementos de apoyo para el buen funcionamiento de dichos equipos.

Manuales e instructivos de operación del sistema de cómputo

Es el inventario de la documentación *técnico-especializada* que está a disposición de los operadores y responsables del sistema, tanto en lo relativo al software como al hardware, lo cual permite verificar el uso adecuado de estos documentos en lo relativo a la operación de los sistemas computacionales de la empresa.

Manuales e instructivos de los usuarios del sistema

Es el inventario de todos los documentos que sirven para conocer el funcionamiento y aplicación de los sistemas implantados en el centro de cómputo; este inventario se realiza con el propósito de evaluar la difusión y disponibilidad de estos documentos para los usuarios, qué tan habitualmente los utilizan, con qué facilidad, e inclusive su actualización permanente.

Manuales, instructivos y procedimientos para el procesamiento de información

Es el inventario de todos los procedimientos y normas documentados que regulan la captura de datos, el procesamiento de información y la emisión de resultados de un sistema de cómputo, tanto desde el punto de vista técnico y operativo del sistema, como desde el punto de vista administrativo de la información.

Manuales e instructivos de mantenimiento lógico del sistema (software)

Es el inventario de los documentos que regulan y determinan la actualización y mantenimiento del software de los sistemas, tales como reportes de fallas y mantenimiento correctivo, programas de mantenimiento preventivo y estadísticas de incidencias.

Manuales e instructivos de mantenimiento físico de sistemas (hardware)

Es el inventario de los documentos que regulan y determinan la actualización y mantenimiento del hardware de los sistemas, de los periféricos y de los componentes asociados, tales como reportes de fallas y mantenimiento correctivo, programas de mantenimiento preventivo, estadísticas de incidencias, compras de refacciones, piezas y otros componentes.

En algunos casos, este inventario se puede realizar para evaluar los servicios de mantenimiento y apoyo para los usuarios de los sistemas, por medio del llamado *Help-desk interno* de sistemas.

Manuales e instructivos didácticos de apoyo

Es el inventario de todos los documentos que sirven de apoyo didáctico para el aprendizaje, optimización de la operación y uso de los sistemas, capacitación de empleados y usuarios del sistema y de otros aspectos formativos que ayudan al buen funcionamiento de los sistemas.

Otros manuales e instructivos para el desarrollo del sistema

Es el inventario de los demás documentos normativos que contribuyen al desarrollo de las actividades y operación de los sistemas, de sus funcionarios y usuarios, dicho inventario también se hace para evaluar la disponibilidad y el uso de estos documentos.

9.5.4.3 Inventario de documentos para el desarrollo de sistemas

Este inventario le sirve al auditor de sistemas para evaluar las metodologías y los estándares de desarrollo de los sistemas que se crean en la empresa, tanto desde el punto de vista del análisis, diseño, bases de datos y programación del sistema, como desde el punto de vista de su implantación, aplicación, capacitación de los usuarios y su documentación.

También le sirve para evaluar las metodologías, normas y procedimientos que se utilizan en la empresa para la optimización, mantenimiento y modificación de los sistemas instalados, así como para evaluar la adquisición de sistemas, lenguajes, paqueterías y programas de aplicación y explotación en el área de sistemas y en los demás equipos computarizados de la empresa.

Existe una inmensa gama de aplicaciones y formas de desarrollar estándares de sistemas; por esta razón, a continuación proponemos la siguiente clasificación.

Inventario de metodologías para el desarrollo de sistemas

Es la recopilación de la documentación que regula los métodos para realizar el análisis, desarrollo, diseño e implantación de sistemas en la empresa; ya sea que estos métodos sean adaptados de los autores sobre el tema, o que sean los estándares de la propia institución; siempre y cuando estas metodologías estén debidamente documentadas.

Inventario de estándares, normas y procedimientos para el desarrollo de sistemas

Es el registro documental de las regulaciones del área, mediante las cuales se determinan los procedimientos y métodos de trabajo de carácter administrativo y técnico para el diseño de bases de datos, desarrollo y programación de nuevos sistemas, o para su compra, estos documentos regulan las fases, etapas, estándares y metodologías establecidas para el desarrollo de sistemas o para su adquisición.

Inventario de estándares para el diseño de bases de datos

Es el registro documental de los estándares, lineamientos y normas que regulan el diseño y elaboración de las bases de datos y de la información que se maneja en el área de sistemas y en la empresa en general, así como lo relacionado con su difusión y cumplimiento por quienes desarrollan los sistemas en la empresa.

Inventario de estándares y normas de documentación de sistemas

Es el inventario de los documentos relacionados con la aplicación de las normas y lineamientos que regulan la forma en que se van a documentar los sistemas de la empresa; ya sean los desarrollados en la empresa o los adquiridos a terceros, así como las paqueterías y programas de aplicación.

Inventario de otros estándares, normas y lineamientos que regulan el desarrollo de sistemas

Es el inventario de todos lo demás documentos que regulan el desarrollo de sistemas en la empresa, desde el análisis y diseño, hasta la programación, documentación, capacitación e implantación del sistema.

Inventario de documentos de apoyo para el funcionamiento de los sistemas

Es el inventario de los documentos que indican las actividades administrativas, técnicas y operativas para estandarizar el funcionamiento de los sistemas de la empresa; en este inventario se pueden incluir todas las funciones, actividades y tareas de los funcionarios, empleados, usuarios y demás personal que está en contacto con el área de sistemas, la información que se procesa en la misma o cualquier otra correlación con los sistemas.

En relación con este tipo de inventarios, debemos aclarar que el auditor debe decidir, según su criterio, cuáles serán los inventarios de documentos que le ayudarán a evaluar el apoyo para el funcionamiento de los sistemas de la empresa, ya que la infor-

mación que obtenga y su modo de adquirirla dependerá directamente de las actividades del centro de cómputo, de su forma de administración y del personal que trabaja en dicho centro.

Al realizar estos inventarios, el auditor también deberá evaluar el uso que se les da a estos documentos del sistema, ya que no sólo deben existir en el área de sistemas sino que deben ser utilizados por los responsables de la operación, los empleados y los usuarios del sistema. Para ello deben tomarse en cuenta los siguientes aspectos:

Que en el área de informática existan los manuales, instructivos y documentos del sistema.

Que estén vigentes y actualizados de acuerdo con las características de los sistemas en la empresa.

Que se difunda, mediante algún medio interno, la existencia, adquisición y actualización de estos documentos del sistema.

Que estén disponibles para la consulta de los directivos, empleados y usuarios del sistema.

Que el personal del área de sistemas los utilice para la operación de los mismos.

En caso de no cumplirse algunos de los casos anteriores, el auditor deberá evaluar las razones por las cuales no se cumplen, ya que esto implicaría deficiencias en el manejo de los sistemas de la empresa.

9.5.5 Inventario de inmuebles, instalaciones, mobiliario y equipos de sistemas

Éste es un inventario de carácter muy general, y bien podría pertenecer a otro tipo de auditoría, principalmente contable; debido a que es el recuento de los activos de la empresa y de sus instalaciones, es decir, de sus bienes muebles, inmuebles, conexiones eléctricas, de comunicación, de acceso al personal, del medio ambiente, de la seguridad de los empleados y demás aspectos relacionados con los edificios, oficinas, equipos y mobiliarios de la empresa.

Sin embargo, para el auditor de sistemas es muy importante realizar este inventario, debido a las propias características de los sistemas, ya que debe verificar si se cuenta con los activos inmuebles, muebles, equipos e instalaciones adecuados para el funcionamiento de los sistemas que satisfacen las necesidades de comunicación de la empresa; en su caso, para la instalación de redes de cómputo, transmisión de información, instalación y protección de sistemas de electricidad, mantenimiento de temperatura, diseño de sistemas de protección contra desastres y sabotajes, protección de los usuarios y equipos de cómputo, mobiliario y de los demás activos y tipos de instalaciones que contribuyen al desarrollo de los sistemas computacionales de la empresa.

A continuación presentamos una propuesta para realizar este tipo de inventarios bajo el siguiente criterio de clasificación.

9.5.5.1 Inventario de activos inmuebles del área de sistemas

Es el inventario físico de terrenos, edificios, instalaciones donde se encuentran los sistemas y en general de todos los activos inmuebles del área de sistemas de una empresa.

Debido a lo especializado de este tipo de inventarios, es recomendable que el auditor de sistemas utilice los inventarios que se realizan para las auditorías financieras o contables.

9.5.5.2 Inventario de mobiliario y equipos de sistemas

Este inventario es muy importante, ya que incluye los componentes de soporte para los sistemas computacionales, sus periféricos y usuarios, además de la forma de distribución y conexión de dichos sistemas.

Este inventario se realiza en dos partes: primero se hace el recuento físico del mobiliario y equipo asignado al área de sistemas, y después se comparan los resultados de ese recuento con los registros contables de la empresa para determinar la correcta asignación, distribución y resguardo de los bienes, así como las posibles deficiencias y faltantes de los mismos.

9.5.5.3 Inventario de las instalaciones eléctricas del área de sistemas

Es el inventario de todo lo relacionado con las instalaciones eléctricas, es decir, cableados, conexiones, tipos y ubicación de las tomas eléctricas a las que están conectados los sistemas computacionales, tomas especiales, instalaciones monofásicas, trifásicas, instalaciones de tierra, *no-breaks*, supresores de picos de corriente y todos los demás elementos eléctricos que hay en el área de sistemas.

El propósito de este inventario es comprobar que existan físicamente las instalaciones y compararlas con los planos de construcción e instalación, así como comprobar la existencia de las bitácoras de mantenimiento preventivo y correctivo de estas instalaciones para comprobar que sean adecuadas y seguras para el funcionamiento de los sistemas computacionales de la empresa.

9.5.5.4 Inventario de instalaciones de datos

Se refiere a la manera como están distribuidos y conectados los sistemas computacionales en la empresa, ya sean de manera individual, por medio de sistemas de redes, equipos de minicomputadoras o en los llamados sistemas mayores; el propósito es levantar el inventario de las instalaciones de estos sistemas y, contando con ello, evaluar su funcionamiento de acuerdo con los sistemas instalados en la organización. También se pueden comparar con los planos y diseños de instalación establecidos en la empresa. Incluso su estado de uso, mantenimiento y posible deterioro.

Este levantamiento de información está íntimamente relacionado con las formas de procesamiento establecidas en las áreas de la empresa, con las necesidades de información de las mismas, así como con el tipo de sistemas computacionales que se hayan adoptado.

En el caso de redes y sistemas multiusuarios, también se evaluarán las topologías de conexión, los protocolos de comunicación, el tipo de hardware y software de estos sistemas y los demás aspectos que se requieren para valorar el funcionamiento de las comunicaciones de datos en la empresa. Además, se pueden valorar la existencia de diseños arquitectónicos, planos y proyectos de instalación de estos sistemas.

9.5.5.5 Inventario de comunicaciones

El inventario de telecomunicaciones le ayuda al auditor de sistemas a evaluar adecuadamente la forma en que se encuentran interconectados los sistemas para la comunicación interna, externa y entre empleados y usuarios, tanto desde el punto de vista administrativo como del técnico.

En este inventario se recopila información relacionada con las comunicaciones telefónicas, las comunicaciones a través de los sistemas, los tipos de cableado utilizados en los sistemas de redes e Internet, los equipos de intercomunicación (redes, faxes, módems), así como las medidas de control y accesos a la información de la empresa. Debemos recordar que en el ambiente de sistemas las comunicaciones pueden ser vía telefónica, inalámbricas, satelitales o a través de los propios sistemas.

Con dicha información, el auditor de sistemas puede emitir un juicio respecto a la utilidad, aprovechamiento y explotación de la comunicación, tanto interna como externa, que existe en el área de sistemas.

9.5.6 Inventario del personal informático

Para el auditor de sistemas, este levantamiento de información relacionada con los directivos, empleados y usuarios del área de sistemas es de suma importancia, ya que le permitirá valorar la importancia y utilidad del factor humano que contribuye al desarrollo de los trabajos de sistemas de la empresa.

Con estos inventarios, además de otras técnicas de evaluación de sistemas y recopilación de información, se pueden evaluar la gestión administrativa del área de sistemas, el cumplimiento de las funciones y actividades administrativas y operativas del personal que labora en dicha área, así como su participación en el desarrollo de sistemas y el procesamiento y manejo de información de la empresa.

El inventario del personal informático está muy relacionado con los manuales de organización y los manuales de perfiles de puestos, entre otros documentos.

Es de suma importancia destacar que estos inventarios de personal, así como la evaluación de éste, estarán definitivamente influidos por el tipo de sistemas estableci-

dos en el centro de cómputo, su forma de administración y los puestos existentes en el mismo, de acuerdo con las necesidades concretas de procesamiento de información de la empresa. Para el mejor entendimiento de este punto, le recomendamos que vea lo señalado en el capítulo 4, "Control interno".

Conviene hacer un paréntesis para señalar la importancia del factor humano que participa en la operación del área de sistemas, así como las principales posiciones que ocupa en el desarrollo de las actividades de dicha área; así encontramos que existen cuatro tipos de personal que participan en las actividades de un centro de cómputo, y con base en ellos se deberá hacer el inventario del factor humano de los sistemas; dichos tipos de personal son los siguientes.

9.5.6.1 Personal adscrito al área de sistemas

Sobre este personal se tiene una autoridad directa y son los responsables de la operación de los sistemas de la empresa. Este personal está subordinado exclusivamente al jefe del área de sistemas, ya que es a quien rinden cuentas de sus acciones. Aquí se da un tipo de autoridad lineal y posiblemente la profesional y la carismática.

9.5.6.2 Usuarios del sistema

Sobre este personal no se tiene ningún tipo de autoridad formal, ya que sólo se presta el servicio de los sistemas a estos usuarios, pero la autoridad lineal de este personal pertenece a su área de origen. Se podrían dar la autoridad profesional y la carismática, pero su dependencia directa y subordinación estará en su área de origen.

Aunque este personal no pertenece al área de sistemas, es necesario considerarlo dentro del inventario del factor humano del área, ya que participa en la operación del sistema.

9.5.6.3 Asesores y consultores

Sobre este personal, que generalmente es ajeno a la empresa, se puede tener un cierto tipo de autoridad, la derivada de la contratación de los servicios; pero eso no es propiamente dependencia del área, mejor dicho es un convenio de prestación de servicios que difiere bastante de la relación laboral *jefe-subordinado*. Sin embargo, se presentan los servicios de este personal y, de alguna manera, son parte del inventario de los recursos humanos del área.

En esta clasificación se puede incluir al personal de *outsourcing* y, en algunos casos, al de los llamados escritorios de ayuda (*helpdesks*) o a quienes prestan servicios similares.

9.5.6.4 Proveedores, distribuidores y desarrolladores externos

Sobre este personal no se tiene ninguna autoridad en absoluto, y en casi todos los casos se depende de ellos profesionalmente, ya que de ellos se adquieren los sistemas (hardware, software, instalaciones, equipos adicionales, etcétera) con los cuales funciona la empresa. Por lo general, este personal no participa directamente en las actividades del área de sistemas, sino que imparte capacitación, adiestramiento y asesoría sobre nuevos productos. Sin embargo, también forma parte del inventario del factor humano de los sistemas de la empresa.

9.5.7 Inventario de bases de datos e información institucional

Este inventario se realiza de acuerdo con las características específicas de cada empresa, y no tiene alguna clasificación especial, es decir, se realiza de acuerdo con el tipo de información que se maneja en la empresa, con las características de los sistemas y con el aspecto normativo para el diseño de las bases de datos.

Sin embargo, el inventario de bases de datos e información institucional debe incluir algunos aspectos similares entre todas las áreas de sistemas; entre estos aspectos destacan los siguientes.

9.5.7.1 Inventario de la información importante de la empresa

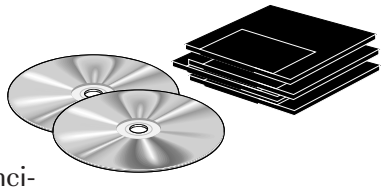
Es el inventario de la información considerada importante para el funcionamiento de la empresa; este inventario se realiza con el fin de evaluar la forma en que dicha información es almacenada, custodiada y protegida contra cualquier incidencia voluntaria o fortuita, así como su importancia, actualización periódica y utilidad para el área de sistemas, entre muchos otros aspectos.

9.5.7.2 Inventario de los respaldos de información (backups)

Es el inventario de los respaldos de información de la empresa, con el fin de evaluar su forma de almacenamiento, protección y custodia, periodicidad de las actualizaciones, y la utilidad de los respaldos, entre muchos otros aspectos.

9.5.7.3 Inventario de los sistemas de operación y programas de aplicación

Es el inventario global de todos *los sistemas computacionales y de los programas originales* que sean desarrollados en la empresa o adquiridos a terceros, y de los respaldos o copias de dichos programas.



Con la información obtenida en este inventario se pueden evaluar las formas de resguardo, la asignación de los programas y la forma de protección para el funcionamiento de los sistemas. Este inventario es similar al inventario de software que analizamos al principio de esta sección, y se aplican los mismos aspectos señalados en ese punto; la razón para mencionar aquí el inventario de software es que también puede formar parte de los inventarios de las bases de datos y del manejo de la información de la empresa.

No mostramos ejemplos de los últimos tipos de inventarios, ya que éstos serían muy especializados, de acuerdo con la empresa que se trate.

9.6 Muestreo

Es obvio que sería imposible y a la vez inoperante que un auditor se pusiera a revisar todas las actividades, transacciones y procesamientos de datos que se realizan cotidianamente en el centro de información de una empresa, sin embargo, para emitir una opinión fundamentada sobre el funcionamiento de esas operaciones, es necesario evaluarlas.

Esto se puede lograr si se recurre al auxilio de una muestra representativa del comportamiento de cada una de las actividades, transacciones y procesamientos que deben ser revisados; siempre y cuando esa muestra cumpla con las características y requerimientos necesarios para hacer válido su uso. Así, al revisar sólo las operaciones seleccionadas en la muestra, el auditor ahorra mucho trabajo y tiempo, y con la información que obtiene puede emitir un dictamen correcto y confiable.

Una de las técnicas que más aportaciones hacen a la auditoría de sistemas computacionales es el muestreo, ya que una aplicación correcta de los métodos y procedimientos estadísticos ayuda bastante a seleccionar una parte representativa del universo que se tiene que revisar; el propósito es obtener la misma información o parecida a la que se obtendría al revisar todo ese universo. De esta manera, el auditor

puede determinar el comportamiento global de todo el universo y con ello puede contar con los elementos de juicio necesarios para emitir un dictamen apegado a la veracidad de los hechos auditados.

No es necesario explicar que esta herramienta es de gran utilidad para cualquier tipo de auditoría. Sin embargo, en la práctica es poco empleada o se aplica en forma muy limitada, ya que para utilizarla es necesario tener amplios conocimientos en los aspectos estadísticos, matemáticos y de probabilística; además, se requiere una gran habilidad y experiencia para elegir el universo y determinar las muestras que serán utilizadas, así también de un buen manejo en la recopilación de información y la determinación de los procedimientos necesarios para la tabulación e interpretación de los resultados obtenidos.

Esta herramienta es fundamental en la auditoría de sistemas, debido a que el auditor se apoya en los propios sistemas computacionales para diseñar la muestra, seleccionar la probabilidad de la captura de datos y después procesar esa información para elaborar los cuadros y gráficas representativos de los resultados. Además, a través del uso de las hojas de cálculo y programas estadísticos se pueden manejar los aspectos estadísticos y matemáticos con mayor exactitud, e incluso en el propio sistema se pueden hacer pruebas con las muestras elegidas, utilizando los mismos datos del sistema, a fin de compararlos con los resultados elegidos.

Otro aspecto fundamental del muestreo es que mediante programas especiales de cómputo también se pueden hacer simulaciones y proyecciones que son de gran utilidad en una auditoría de sistemas, aunque el muestreo sea matemático, estadístico o por computadora.

Continuando con el mismo método de estudio seguido en este libro para cada una de las herramientas aquí señaladas, a continuación presentamos algunas definiciones y conceptos de esta herramienta.

Muestreo.

"Selección de muestras representativas de la calidad o características medias de un todo. Técnica empleada para la selección."[8]

"El muestreo en auditoría consiste en la aplicación de un procedimiento de cumplimiento o sustantivo a menos de la totalidad en las partidas que forman el saldo de una cuenta o una clase de transacciones (muestra), que permitan al auditor obtener y evaluar la evidencia de alguna característica del saldo o transacción y que le permita llegar a una conclusión en relación a tal característica."[9]

"Muestreo es seguir un método, un procedimiento tal que al escoger un grupo pequeño de la población podamos tener un grado de probabilidad de que ese pequeño grupo efectivamente posee las características del universo y la población que estamos estudiando... Los tres puntos importantes respecto a una muestra son los procedimientos para determinar la representatividad de la muestra, los procedimientos para determinar el error de la muestra y los procedimientos para determinar el tamaño de la muestra... Hay dos tipos principales de muestreo probabilístico que hace posible de-

terminar el error posible de la muestra y el muestreo probabilístico que carece de esa probabilidad [...]"[10]

Muestra

"Porción de un producto o mercancía que sirve para conocer su calidad. Porción de una sustancia que sirve para examinarla. Modelo que se ha de copiar o imitar [...]"[11]

"Muestra es un conjunto de **n** *observaciones (unidades elementales) extraídas de una población. Esta* **n** *es el tamaño de la muestra [...] El tipo de muestra que se obtiene depende de la forma en que se ha extraído la muestra de la población. Así se habla de muestreo simple, muestreo sistemático y muestreo o conglomerado [...]"*[12]

Muestra representativa

"[...] es aquella en la cual las características de la muestra de interés para la auditoría son aproximadamente las mismas de la población. Esto significa que las partidas muestreadas son similares a las no muestreadas."[13]

Universo

"Universo o población [...] Todo grupo de objetos que poseen una característica común [...] está formado por entidades que tienen una misma característica [...]"[14]

"Una población (o universo) se define como la suma (totalidad) de las unidades elementales. Si el número de unidades elementales es igual al número de observaciones, se dice que la población es la suma de las observaciones [...]"[15]

Población

"Es la totalidad de fenómenos a estudiar en donde las unidades de población poseen una característica común, la cual se estudia y da origen a los datos de la investigación [...] Shellhz nos indica que una población es el conjunto de todas las cosas que concuerdan con una serie determinada de especificaciones."[16]

El uso de esta herramienta exige ciertos conocimientos de estadística, probabilística y matemáticas, a fin de manejar correctamente las técnicas y procedimientos necesarios para determinar la muestra, la probabilidad de errores de la misma, la tabulación de datos y la obtención de resultados confiables, debido a que en su aplicación intervienen elementos estadísticos, aleatorios y de incertidumbre que hacen necesario el manejo de las estadísticas y probabilidades en la selección del universo, muestras y resultados.

Actualmente existen muchas formas de utilizar el muestreo estadístico para recopilar datos; el muestreo se utiliza de acuerdo con las características específicas de la exploración a realizar, sin embargo, en este libro no pretendemos realizar un tratado estadístico de la forma de seleccionar una muestra para una investigación, sino señalar la importancia que tiene la elección de una muestra en la recopilación de datos útiles para la auditoría de sistemas computacionales.

9.6.1 Procedimiento general para definir la recopilación de información mediante el uso de una muestra

Para obtener estadísticamente la información en una auditoría de sistemas computacionales, se debe emplear un método específico para determinar el universo donde se realizará la recopilación de información y elegir la muestra que será utilizada; por esta razón, a continuación presentamos un procedimiento general que se utiliza en la elección de una muestra para cualquier tipo de investigación:

- *Definir el tipo de investigación que se va realizar*
  - Planteamiento concreto del problema
  - Definir el método de investigación que se va a utilizar
- *Determinar el universo, la población y la muestra*
  - Determinar el universo y la población que serán utilizados para cubrir las necesidades de información para la investigación
  - Determinar el método y tipo de muestreo que serán utilizados en la recopilación de datos
  - Calcular el tamaño y la forma de seleccionar la muestra de datos para que sea válida para la investigación
  - Establecer las características, modalidades y cualidades que deberán reunir los elementos de la muestra
- *Definir las herramientas de recopilación de datos*
  - Diseñar los instrumentos de recopilación de datos
  - Elaborar pruebas piloto y correcciones
  - Elaborar los instrumentos de recopilación
- *Recopilar la información*
  - Preparar y capacitar a los recopiladores de información
  - Recopilar la información en campo, de acuerdo con la muestra
  - Verificar el cumplimiento de la recopilación de acuerdo con la muestra
- *Tabular los datos*
  - Concentrar y validar la información
  - Elaborar cuadros estadísticos y gráficas representativas
- *Interpretar los datos obtenidos*
  - Analizar cuadros y gráficas
  - Comparar con datos similares
- *Difundir los resultados*

Debido a que esta sección se refiere únicamente al muestreo, a continuación haremos un análisis de cómo obtener una muestra, citando en cada caso algunos ejemplos de la aplicación de esa muestra.

9.6.2 Elección de una muestra en una auditoría de sistemas

El primer paso para aplicar la técnica del muestreo es saber seleccionar el tipo de muestra que servirá para hacer el estudio, la cual dependerá del tipo de muestreo que será aplicado. En el caso de la auditoría de sistemas, se debe tomar en cuenta que tanto el universo como la muestra son elegidos de acuerdo con lo que se quiere evaluar. En relación con esto, se tienen que considerar los siguientes aspectos:

"...a partir de una muestra, es necesario primero escogerla y recopilar la información apropiada respecto a ella. Si la muestra no se selecciona adecuadamente, o si la recopilación de información es incorrecta, o no se ajusta a una secuencia apropiada... Se debe tener siempre mucho cuidado al evaluar los datos (así como al recopilarlos) con objeto de evitar posibles errores en la selección de las muestras y en las desviaciones de los datos."[17]

A continuación presentamos algunos ejemplos de los tipos de muestra que se pueden presentar en una auditoría de sistemas computacionales.

9.6.2.1 Muestreo aleatorio simple

"[...] Cuando todos los miembros de una población tienen la misma probabilidad de ser seleccionados."[18]

En estos casos, el auditor selecciona cualquier elemento de la población, mediante algún tipo de muestreo aleatorio, de entre los cuales tenemos los siguientes.

Por medio de algún sistema computacional

Es la elección de una muestra no probabilística por medio de un sistema computacional, con programas especiales de estadística, hojas de cálculo o programas realizados explícitamente para ello.

En la tabla se presenta un muestreo por computadora en el cual podemos identificar algunas operaciones elegidas mediante la función aleatoria y redondeo:

Día elegido	Núm. de operación
Del lunes 3	1 986
Del martes 4	106
Del miércoles 5	4 886
Del jueves 6	822
Del viernes 7	6 622

En este ejemplo seleccionamos cinco operaciones realizadas en el sistema computacional, del 3 al 7 de agosto de 2000, elegidas en forma aleatoria

en una hoja de cálculo como Excel®; estas operaciones fueron rastreadas desde la captura de datos, el cálculo manual y los resultados arrojados después del proceso.

Por una simple y sencilla operación aritmética

Para este caso se elige la muestra mediante una operación aritmética simple, que se hace arbitrariamente y sin mayores complicaciones, como en el siguiente ejemplo:

Supongamos que un auditor desea revisar la instalación, el tipo de cableado, aprovechamiento del procesamiento, las actividades de los usuarios durante la semana anterior, el monitoreo de las operaciones de los dos días siguientes y otros aspectos de 10 de las 100 estaciones de una red de cómputo de la empresa.

Nuestra fórmula, elegida arbitrariamente, será la siguiente:

N = N + 7

Inicio en la máquina N = 25 (porque así se eligió)

De ahí sumamos 7 a la N y nos queda una nueva N, a la cual se le vuelven a sumar otra vez 7, y así sucesivamente. Entonces los números de estación seleccionados serán:

25, 32, 39, 46, 53, 60, 67, 74, 81, 88, 95

Método aleatorio determinado por fórmulas matemáticas

Aquí el auditor realiza un proceso de cálculo utilizando una función algebraica o de cualquier tipo de arreglo matemático, mediante la cual obtiene números aleatorios que le servirán para seleccionar los elementos de la población.

Como ejemplo podemos citar lo siguiente:

Supongamos que un auditor va a revisar un universo de 3 000 empleados y que en el programa de auditoría se determinó que va a evaluar el cálculo correcto de las 24 quincenas del último año, así como el cálculo del aguinaldo de cada empleado.

Si el auditor decidiera revisar todas las operaciones de la nómina, estaríamos hablando de 72 000 resultados por calcular, en los cuales tendría que hacer operaciones por los ingresos, egresos, impuestos y retenciones de cada trabajador; además tendría que verificar la oportunidad, confiabilidad y veracidad en la captura de datos, emisión de resultados y almacenamiento de esa información, así como del procesamiento del sistema, la inclusión correcta de los datos del empleado, su capacitación, sus últimos movimientos salariales y otros aspectos inherentes al desempeño de su actividad en el área de sistemas.

Hacer uno a uno estos cálculos sería muy tedioso además de inoperante, con riesgos de errores y con un consumo de tiempo muy abundante.

Por esta razón, aprovechando una muestra determinada mediante una fórmula, en este caso un proceso aleatorio matemático, seleccionaremos a los empleados que cumplan con las condiciones de la fórmula, y en cada resultado revisaremos sus cálculos de nómina y demás condiciones.

Elegiremos el número de los empleados del entero que resulte de la siguiente expresión:

$$X = (4Y^2 + 5Z)$$

Donde tomamos como valores de Y = desde 24 hasta 5

Donde tomamos como valores de Z = desde 0 hasta 19

(valores elegidos en forma arbitraria)

La quincena se calcula de la siguiente manera:

$Q = Y - 3$ o $Q = Y + 3$

Donde se aplican estas restricciones:

Si $Y > Z$, entonces anotamos ($Q = Y - 3$)

Pero si $Y < Z$, entonces anotamos $Q = Y + 3$

Aplicando la primera fórmula para calcular el número de empleado, tenemos que:

Para el primer renglón del cuadro: donde $Y = 24$; $Z = 0$

$X = 4(24)^2 + 5(0) = 4(576) + 5(0) = 2304$,

Para el segundo renglón del cuadro: donde $Y = 23$; $Z = 1$

$X = 4(23)^2 + 5(1) = 4(529) + 5(1) = 2121$

Para el décimo renglón del cuadro: donde $Y = 15$; $Z = 9$

$X = 4(15)^2 + 5(9) = 4(225) + 5(9) = 945$

Aplicando la segunda fórmula para la quincena, tenemos que:

Para el primer renglón del cuadro: donde $Y = 24$; $Z = 0$

Como $Y > Z$ entonces $Q = (24 - 3) = 21$

Para el segundo renglón del cuadro: donde $Y = 23$; $Z = 1$

Como $Y > Z$ entonces $Q = (23 - 3) = 20$

Para el décimo renglón del cuadro: donde $Y = 15$; $Z = 9$

Como $Y < Z$ entonces $Q = (9 + 3) = 12$

Núm. de empleado	y	z	Quincena
2304	24	0	21
2121	23	1	20
1946	22	2	19
1779	21	3	18
1620	20	4	17
1469	19	5	16
1326	18	6	15
1191	17	7	14
1064	16	8	13
945	15	9	12
834	14	10	11
731	13	11	10
636	12	12	15
549	11	13	14
470	10	14	13
399	9	15	12
336	8	16	11
281	7	17	10
234	6	18	9
195	5	19	8

Concretando, para estos ejemplos tenemos que se revisarán los cálculos de las operaciones de los empleados: Número 2 304, y quincena 24
Número 2 121 y quincena 20
Número 947 y quincena 9

Como ejemplo tenemos la tabla anterior, en donde elegimos a 20 empleados.

El auditor puede elaborar estas tablas bajo cualquier criterio o fórmula, siempre y cuando las elabore para elegir aleatoriamente una muestra y dentro de los rangos del universo que va a utilizar.

9.6.2.2 Muestreo no probabilístico

Es frecuente que en una auditoría se tengan que seleccionar elementos de una población que tienen exactamente el mismo comportamiento que los elementos que se van a revisar; en estos casos se dice que la elección de la muestra es de carácter no probabilístico, ya que no existe ninguna posible variación en el comportamiento de los sujetos que van a ser utilizados en la revisión; todos guardan el mismo comportamiento.

El muestreo no probabilístico se define de la siguiente manera:

Es la muestra cuya elección no varía respecto a la población total y cuya designación no representa ningún riesgo de desviación ni alteración del comportamiento de cada miembro elegido. Estas muestras no estadísticas se obtienen cuando se toman todos los elementos de la población o cuando cualquiera de los integrantes elegidos es representante idéntico de cualquier otro miembro de ese universo, y en todos los casos su comportamiento es similar al de otro y no existe ninguna variación en la conducta observada entre ellos.

Al no ser probabilísticos, todos los elementos de la población tienen la misma oportunidad de ser elegidos, y no se seleccionan por ningún método matemático ni estadístico, sino por cualquiera de los siguientes métodos.

Muestreo intencional

En estos casos, el auditor aplica ciertos juicios y tendencias en la selección de las muestras, basándose en su experiencia, conocimientos y en las necesidades de evaluación, a fin de obtener muestras representativas de las características visibles del comportamiento específico de los elementos de la población; el propósito es que dichos elementos sean útiles para la auditoría.

Aunque este tipo de muestreo no es muy ortodoxo ni tiene nada de estadístico ni matemático, es muy útil para el auditor con experiencia y conocimientos en auditorías de sistemas, ya que con su correcta aplicación puede obtener lo siguiente:

Elementos de la población con tendencias a errores significativos en sistemas.

Desviaciones comunes que se dan en todas las actividades, procesos y operaciones del área de sistemas.

Desviaciones de la operación normal que se presentan en muchos centros de cómputo.

Tendencias de desviación características de las actividades de un sistema computacional.

Uno de los principales criterios que avala el uso de este método, es que le permite al auditor dirigir una muestra hacia una intención específica de revisión, aunque ésta no sea estadística, pero sí representativa de las desviaciones típicas que se presentan en una auditoría de sistemas computacionales.

Ejemplo para comprobar cálculos

Un auditor con experiencia en el cálculo y procesamiento de nóminas puede establecer las siguientes consideraciones:

Supongamos que el sueldo mínimo actual es de $30.00.

Si al trabajador con este sueldo se le han pagado incapacidades por accidente de trabajo o por enfermedad general, por cualquier número de días, los últimos dígitos de estas incapacidades invariablemente tendrían que terminar en ***.00****. En caso de accidente de trabajo, de 10 días a ese sueldo le corresponden $300****.00****. En caso de enfermedad general, le corresponden $180****.00*** *(10 × 30.00) × .60%.**

Si fuera cualquier otro sueldo sin decimales, los dos últimos decimales deben terminar forzosamente en .00; en caso contrario existen errores de cálculo. Si se dan estos caso, entonces los podemos seleccionar para investigar el porqué de esas desviaciones.

Bajo estas consideraciones, el auditor puede elegir los elementos de una muestra intencional por medio de una rutina de cómputo para seleccionar trabajadores que han tenido incapacidades y elegir aquellos cuyas últimas cifras terminen en decimales diferentes a .00, según sus salarios. Con esto, el auditor comprobará la elaboración correcta de estas operaciones. Es obvio que sólo las operaciones con error darán alguna cifra en los dos últimos decimales; las operaciones correctas deben dar .00; es fácil hacer la comprobación con cualquier cálculo.

Ejemplo para verificar la existencia y uso de manuales de operación

Cuando en la visita preliminar el auditor se da cuenta de que los manuales e instructivos de operación están impecablemente acomodados, bajo llave, sin ningún desgaste aparente y, en algunos casos, todavía en su envoltura original, y bajo la custodia de la secretaria del departamento o de la persona encargada

* En México, la ley del IMSS establece el pago de las incapacidades de carácter profesional al 100% del salario diario del trabajador; mientras que las incapacidades por enfermedad general se pagan al 60% del salario diario del trabajador.

del manejo de la documentación de paquetes y programas del centro de cómputo, y no los prestan a los empleados y usuarios, lo más probable es que estos manuales e instructivos jamás sean utilizados; entonces elegirá una muestra de operadores y usuarios para preguntarles sobre los siguientes aspectos:

La existencia de manuales e instructivos de los paquetes y programas que manejan en los sistemas computacionales

La difusión de dichos documentos

La posibilidad de asesoramiento y préstamo para estudiarlos y consultarlos

El uso de estos manuales e instructivos en su operación cotidiana de los sistemas

Lo más probable es que el auditor encuentre desviaciones del uso y utilidad de estos documentos de sistemas. Entonces todos los empleados que entreviste, sean quienes sean, arrojarán esta información.*

Recordemos que los instructivos y manuales de sistemas deben tener estas características: *que estén* en el centro de cómputo, *que se difunda* su existencia, *que estén a disposición* de los usuarios y *que sean utilizados* en las actividades del sistema.

En el ambiente de sistemas podemos agrupar esta muestra intencional de muchas maneras; a continuación mencionaremos algunos ejemplos de posibles muestreos:

Operaciones similares que tengan mayor o menor probabilidad de errores en su procesamiento. Esta muestra sería similar para todos los casos, ya que todos los elementos tienen la probabilidad.

Actividades normales susceptibles de deficiencias. La muestra de cualquiera de los elementos tiene la misma probabilidad de mostrar esos errores.

Actividades que normalmente tienen deficiencias aceptables en su operación, y que se pueden presentar en cualquiera de los casos seleccionados como muestra.

Análisis de las funciones administrativas que atienden normalmente *los empleados y usuarios de sistemas, o que las evitan o las atienden deficientemente. Es otro ejemplo de tomar cualquier elemento de la muestra para evaluar su comportamiento similar.*

Suposiciones de piratería de paquetes y programas. Cuando se dan estas suposiciones, cualquier equipo seleccionado como muestra tiene las mismas posibilidades de tener software no autorizado.

* Una práctica muy común y nefasta de las instituciones públicas o privadas es que no difunden la existencia de los instructivos y manuales de los sistemas entre los usuarios; lo mismo ocurre en institutos y universidades que imparten materias relacionadas con sistemas computacionales; además, muchas veces no permiten que los alumnos consulten los manuales e instructivos de las paqueterías y programas que tienen instalados en sus centros de cómputo (¿a servicio de los estudiantes?), salvo honrosas excepciones.

Suposición de deficiencias en las operaciones, uso de los sistemas y en el desarrollo de las actividades de usuarios inexpertos. Al tomar una muestra de estos usuarios, por su inexperiencia, existe la probabilidad de encontrar deficiencias en el desarrollo de sus operaciones.

Muestreo por volúmenes (bloques) homogéneos

En este tipo de muestreo no probabilístico, el auditor selecciona, bajo algún criterio no matemático ni estadístico, grandes bloques o sectores de información, operaciones, actividades o cualquier otro aspecto global que debe analizar, de acuerdo con las necesidades concretas de la evaluación; de esta manera puede elegir elementos de la población que cumplan con determinadas características específicas y que, en este caso, sean similares a los demás elementos de la población.

Para utilizar este tipo de muestras es necesario que cada uno de los bloques en que se divide la población cumpla con ciertos parámetros de homogeneidad, igual o más o menos igual, a fin de que todos los elementos que integran el universo tengan la misma representatividad y condiciones de selección. Es decir, los elementos de la población se agrupan en grandes bloques con los mismos tipos de información, características y condiciones de comportamiento que los hacen similares entre sí.

Ejemplo de selección de bloque de terminales de una red

La selección de un grupo de cinco terminales de servicios de la red de cómputo, las cuales podemos agrupar por número de terminales (por pares, cada número 3 o múltiplo de 3), por agrupación de terminales en una sola área (las de contabilidad, las del área de personal), por la cercanía entre las propias terminales, por los tipos de usuarios que las manejan o por cualquier criterio que permita agruparlas en bloques homogéneos, siempre y cuando éstos tengan características y condiciones más o menos iguales.

En este tipo de bloques, el auditor aprovecha la muestra de cada elemento (en este caso de cada terminal) para hacer una revisión global; a continuación presentamos algunos aspectos que pueden ser evaluados con este criterio:

La configuración de la terminal, las instalaciones y cableados que se utilizan por cada elemento del bloque seleccionado. Se puede aprovechar para revisar la instalación y configuración total de la red.

Los protocolos de comunicación, programas y paqueterías de que dispone la terminal para su funcionamiento como parte de la red y como equipo individual.

Inventarios del software, hardware, consumibles, respaldos, información, etcétera.

La oportunidad, confiabilidad y veracidad del procesamiento de información.

Monitoreo de las actividades de cada terminal para evaluar su aprovechamiento.

La capacidad de operación de sus usuarios, asesoría y asistencia para el desarrollo de su trabajo, etcétera.

Niveles de acceso y seguridad de cada terminal, contraseñas, privilegios y acceso a la información.

Desarrollo de proyectos especiales para servicio de los usuarios de esa terminal, etcétera.

Con el ejemplo anterior podemos establecer que el auditor, de acuerdo con las necesidades de la evaluación y con su programa de trabajo, puede elegir una muestra no probabilística de una manera casi arbitraria, pero que puede aprovechar para hacer una evaluación integral de muchos aspectos relacionados con los sistemas computacionales; quizás en esto radica la importancia de este tipo de muestreo.

Muestreo al azar

En este tipo de muestras, el auditor selecciona a cada uno de los elementos que tendrá que evaluar durante su auditoría de sistemas bajo cualquier tipo de criterio al azar (por sorteo, rifa, lotería, tómbola, juego, etcétera). En este caso, cada elemento puede o no cumplir con las características homogéneas de la población, pero es elegido totalmente al azar.

Para efectos del muestreo, aquí se deben olvidar el tamaño de la muestra, sus características, su origen y aportación a la operación o cualquier otro aspecto que pueda interferir en su elección al azar. Lo único válido es que entre en el sorteo que se hará de todos los elementos de la población.

Ejemplo de muestreo al azar para evaluar niveles de seguridad

El auditor realizará una selección al azar de los usuarios que están laborando en el centro de cómputo de la institución; para ello revisa los niveles de acceso, contraseñas, privilegios, accesos permitidos a los programas, paqueterías e información y todos los aspectos de seguridad que evaluará de los usuarios que fueron seleccionados.

Está claro que en el ejemplo citado el auditor realiza la evaluación de la seguridad de estos usuarios de acuerdo con el azar con que fueron seleccionados, sin importar ni las características, tiempo de uso del sistema, veces que lo frecuentan, capacidad para el manejo de los sistemas ni algunos otros elementos inherentes a estos usuarios.

9.6.2.3 Muestreo probabilístico

"[...] se entiende como un plan de muestreo en que cada miembro de la población tiene una probabilidad conocida de ser incluido en la muestra."[19]

Para seleccionar una muestra de carácter probabilístico, cada uno de los elementos de la población debe cumplir con ciertos requisitos de carácter estadístico, matemático e inclusive probabilístico, de tal manera que cada uno tenga la misma probabilidad de salir seleccionado en la muestra mediante algún proceso estadístico.

Para entender este tipo de muestreo vamos a estudiar los siguientes conceptos:

Muestreo con reemplazo y sin reemplazo

"Si el muestreo se realiza de tal manera que la unidad elemental se pueda reemplazar (devolver) a la población, de forma que pueda ser extraída de nuevo, tendremos ***un muestreo con reemplazo****. Si la unidad elemental se retira de la población de manera que no pueda volver a aparecer, el* ***muestreo es sin reemplazo."***[20]

En la selección de la muestra probabilística con reemplazo (o sin reemplazo), lo primero que hace el auditor es establecer matemáticamente las probabilidades estadísticas de cada uno de los elementos de una población, previamente determinada, para que pueda ser seleccionado; el propósito es que el auditor consiga establecer las posibilidades de que cualquiera de esos elementos pueda ser elegido y utilizado con éxito en la evaluación.

Por lo general, la probabilidad en el muestreo está asociada al grado de incertidumbre y límites de confianza que se tienen que establecer en la selección de los elementos de una muestra; estos dos aspectos darán la confiabilidad a la auditoría de sistemas computacionales; por esta razón, lo primero que debe hacer el auditor es establecer los niveles de error que va a tolerar, tanto en la elección de las muestras que utilizará, como en las desviaciones de los elementos que va a auditar.

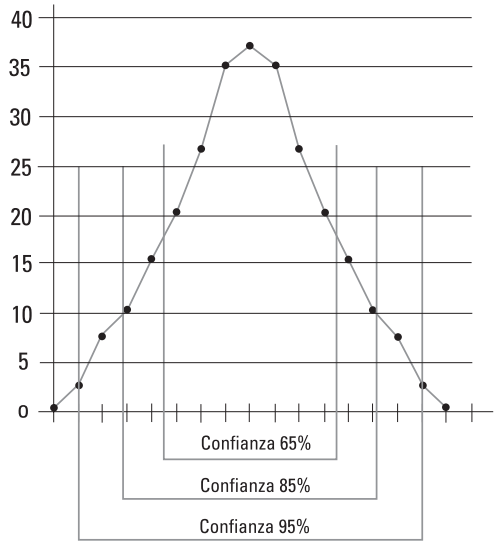
Es decir, el auditor debe definir los límites, mínimos y máximos, que tolerará del comportamiento de cada uno de los elementos que analice. A esto le podemos llamar *grado de error tolerable* (GET).

Para el mejor entendimiento de este punto debemos establecer los siguientes conceptos.

Grado de confianza

Es un número menor que 1, medido en unidades porcentuales, al cual se le da un valor que representa la creencia de que las encuestas realizadas cumplirán con ciertos límites razonablemente confiables (grados de confianza), lo cual dará cierto grado de certeza de que las encuestas van satisfacer las necesidades del auditor.

Esto es la representación de la campana de Gauss, aplicada a la recopilación de información por medio de encuestas.



En esta gráfica se representan los siguientes valores:

El 65% de confianza indica lo siguiente: de todas las encuestas que se realizan, sólo el 65% pueden tener cierto grado de certeza de que las respuestas serán razonablemente confiables. También se puede interpretar como el límite de error que puede tolerar el auditor en la información que obtenga por este medio. La explicación es similar para el 85 y 95% de confianza, sólo que los niveles de confiabilidad varían.

En otras palabras, si el auditor toma el grado de confianza de 65%, puede tolerar el 35% de errores de captura y obtención de información al realizar sus encuestas. En caso de que tome el 85%, sólo puede tolerar 15% de errores o sólo el 5% de errores en el grado de confianza de 95%.

Con el siguiente ejemplo entenderemos la importancia del GET:

El auditor pretende evaluar la utilidad del sistema contable utilizado en la empresa; para ello pretende realizar una encuesta de contabilidad y de finanzas en el área de sistemas, con el propósito de conocer las opiniones de los empleados respecto a la utilidad de ese programa y en general del sistema computacional, sin embargo, estas áreas representan más de 500 empleados, lo cual sería, además de inoperable y tedioso, demasiado trabajo para el auditor. Por esta razón, debe establecer una muestra representativa de esos trabajadores y el grado de confianza que aceptará de las opiniones de esos encuestados.

En este caso, lo primero que debe hacer el auditor es determinar el grado de confianza que aceptará para las encuestas, es decir, qué opiniones no va a tomar en cuenta debido a que son demasiado cargadas a la utilidad de los sistemas y qué encuestas va a eliminar debido a que son demasiado negativas sobre el funcionamiento de éstos. En ambos casos debe establecer el nivel de tolerancia superior e inferior que aceptará de las opiniones que recabe.

9.6.2.4 Muestreo simple al azar

*"Una **muestra simple al azar** de tamaño **n** es una muestra elegida de una población en la que todas las muestras posibles de tamaño **n** tienen la misma posibilidad de ser elegidas."*[21]

En este tipo de muestreo se hace la selección mediante un método estadístico aleatorio, en el cual se tiene que establecer la posibilidad de que cualquiera de los elementos de la población tenga la misma posibilidad de ser elegido mediante algún muestreo al azar. La importancia de este tipo de muestreos y su utilidad para una auditoría de sistemas está en la forma de determinar las probabilidades de cada elemento elegido al azar.

Ejemplo de selección de los procesamientos de información

Supongamos que el sistema computacional de la institución realiza un procesamiento de 1 000 operaciones por jornada, y que el programa de auditoría establece que se tienen que seleccionar *100 procesamientos de datos* (*elementos*) *ocurridos durante las jornadas diurna y nocturna* en el sistema computacional de la empresa *durante todo el mes de junio de 1998* (*población de donde extraeremos la muestra*), para verificar la oportunidad, confiabilidad y veracidad en la captura de datos, procesamiento en el sistema y emisión de los resultados, con el fin de evaluar la operación adecuada del sistema.

En este caso, si el auditor trabajara ininterrumpidamente los 31 días del mes de julio, tendría un total de 62 000 operaciones procesadas en el sistema computacional de la empresa. La probabilidad de elegir al azar 100 operaciones de cualquiera de esos días es igual para todos los casos, ya que en este caso no hay ninguna condición para los elementos de la muestra. Por lo tanto, la probabilidad de que un elemento sea elegido en forma aleatoria al azar es igual a 0.0016129 (100/62 000), entonces cada elemento tiene la misma posibilidad de ser elegido.

En el ejemplo, el auditor puede hacer un procesamiento aleatorio de cómputo, por sorteo o por cualquier otro método de azar para elegir los 100 elementos de muestra que le servirán para evaluar el funcionamiento del proceso de cómputo de la empresa.

9.6.3 Otros muestreos aplicables en una auditoría de sistemas

En el ambiente de auditoría de sistemas hay muchos tipos de muestreo para recopilar información útil para evaluar los sistemas computacionales; el auditor puede determinar estos tipos de muestreo a través de múltiples medios y métodos estadísticos y matemáticos, e incluso sin ningún método en especial, y de acuerdo con su experiencia, conocimientos y necesidades de recopilación de información.

Por esta razón, a continuación presentamos algunos muestreos distintos a los señalados anteriormente, analizándolos con menor profundidad, ya que se trata de mostrar que existen más formas de elegir el muestreo para auditoría, pero éstas pueden ser elegidas de acuerdo con las necesidades del auditor de sistemas y en función de la propia evaluación.

9.6.3.1 Muestreo estratificado

Es cuando la población elegida para obtener información se estratifica en varias partes (segmentos), con el propósito de obtener muestras representativas de cada uno de los segmentos elegidos; con esto se busca homogeneizar la representatividad de cada elemento elegido. En estos casos, la elección de muestras es proporcional a la representación de cada segmento.

Una manera de utilizar este muestreo estratificado es tomar un universo de encuestados, los cuales son agrupados en ciertos rangos más o menos homogéneos, de acuerdo con características específicas, ya sea por actividad, por funciones, por tipo de procesamiento o por cualquier otro aspecto. Tomando como base dichos grupos (estratos), se conforman clasificaciones similares y se eligen muestras representativas de los segmentos de cada grupo, en el supuesto de que los elementos elegidos serán representativos de todo el segmento. Así, tomando una muestra de cada segmento, se formará una muestra representativa de todo el universo, haciendo confiable la elección de esas muestras.

No presentaremos ejemplos del muestreo estratificado, debido a que este tipo de muestreo se realiza específicamente de acuerdo con las características de la empresa o del área de sistemas.

9.6.3.2 Muestreo de juicio

Éste no es un método matemático ni estadístico, ni elaborado con métodos científicos; por esta razón, es difícil aceptarlo como un método científico de investigación aplicable a comprobaciones requeridas en una auditoría, ya que al implantarlo no se cumplen los requisitos de confianza que exigen los formalismos estadísticos y matemáticos para validar la muestra seleccionada. Sin embargo, su empleo empírico sí puede ser de mucha utilidad para obtener datos significativos en una auditoría de sistemas computacionales, pero el auditor debe utilizarlo de acuerdo con su experiencia, conocimientos y necesidades, con el universo del cual vaya a elegir la muestra y con lo relevante de los elementos que esté evaluando.

Este método de carácter empírico permite elegir una muestra de manera muy sencilla y, hasta cierto punto, razonablemente confiable, debido a que consiste en determinar algún criterio de selección que, a juicio del auditor, tiene que cumplir cada uno de los elementos seleccionados, siempre y cuando este criterio sea útil para el aspecto de sistemas que será evaluado.

En este muestreo, todos los elementos que cumplen con el criterio señalado pueden ser elegidos del universo total mediante alguno de los métodos anteriores o pueden ser seleccionados mediante algún otro método.

Lo importante de este tipo de muestreo es que el auditor establece, de acuerdo con la evaluación, el criterio de juicio que le será útil para satisfacer las exigencias de la auditoría de sistemas computacionales, permitiéndole hacer la selección de una muestra de elementos que satisfagan esos requerimientos. Dicho criterio es el factor determinado para asegurarse de que esta selección cumplirá con las necesidades específicas de revisión de los sistemas.

Al lector y al auditor principiante podría parecerles que el uso de este tipo de muestreo carece de fundamentos metodológicos, aún más si lo comparan con lo formal de los tipos de muestreo anteriores, sin embargo, este criterio puede ser muy útil

en una auditoría de sistemas computacionales, debido a que ayuda a obtener información privilegiada (de los elementos seleccionados) que contribuye a identificar posibles problemas relacionados con algún tópico o problemática específica que se presente en el ámbito de sistemas bajo evaluación. Incluso, en algunos casos también ayuda a ratificar o rectificar alguna desviación.

Algunos auditores llaman también a este muestreo, *muestreo inducido*, y es muy frecuente que los auditores con una amplia experiencia y conocimientos en su especialidad lo utilicen, debido a que en su práctica diaria obtienen cierto tipo de *tips* sobre la problemática concreta del ámbito de sistemas donde se realiza la evaluación y, con base en su experiencia, se dan a la tarea de elegir aquellos elementos que pueden proporcionar información valiosa sobre ese tópico, a fin de reforzar, con datos más concretos y de fuentes más fidedignas, su conocimiento sobre esa problemática. Contando con ello, entonces pueden confirmar o rechazar una posible desviación de esos tips.

El auditor experimentado aplica este método, aun sin bases estadísticas ni matemáticas, ya que lo primordial es obtener elementos que proporcionen información útil para una auditoría, y éste es un elemento muy valioso para ello.

Una manera práctica de entender el funcionamiento del muestreo de juicio es mediante ejemplos; por esta razón, a continuación presentamos algunos.

Ejemplo 1

En la evaluación del procesamiento del sistema computacional de la empresa, el auditor obtiene información confusa, tips, guías de acción o datos aislados sobre algún comportamiento anómalo en el procesamiento de información del sistema de nómina; en especial por cierto retraso o errores en el cálculo quincenal de las horas extras, lo cual obliga a reprocesar frecuentemente los cálculos de esos pagos.

Aplicando el criterio de muestreo de juicio, *se tiene que elegir una muestra de todos los procesos relacionados (directa o indirectamente) con los cálculos del tiempo extra, a fin de obtener información más concreta, más valiosa e íntimamente relacionada con las posibles incidencias donde se presentan esos errores de cálculo o retrasos.*

Independientemente del volumen de las operaciones que se realicen para la nómina de la empresa, si el auditor eligiera realizar un muestreo de todo el procesamiento de datos para calcular el total de la nómina, tanto cálculo normal como cálculo de tiempo extra, tendría que aplicar cualquiera de los métodos de muestreo anteriores y con ello tendría la probabilidad de elegir algunos casos donde se presente este problema de retraso o errores de cálculo.

Si el auditor aplica correctamente el muestreo, obtendrá una muestra que sí será representativa de esos problemas. Pero si puede omitir el muestreo del cálculo normal de la nómina, y elegir sólo aquellos casos donde se realiza el cálculo del tiempo extra, entonces tendría información muy valiosa y relacionada directamente con los retrasos o errores en ese procesamiento.

La ventaja de este muestreo de juicio o inducido, es que el auditor induce el muestreo hacia los casos en los que se pueden presentar las incidencias con mayor frecuencia, a fin de analizar más profundamente las posibles desviaciones, sus verdaderas causas y todos los aspectos que hacen que se presenten estas desviaciones.

Ejemplo 2

Mediante algún cuestionario, entrevista, observación, etcétera, el auditor obtiene información informal y sin confirmar sobre el uso de equipos piratas en la empresa; supongamos que el auditor sospecha que esto se presenta en las PCs que no dependen directamente de los equipos que controla el área de sistemas, ni de las redes de la empresa.

Entonces el auditor tiene dos opciones:

Hacer un muestreo formal, cualquiera de los señalados anteriormente, y conforme a la formalidad del método elegido, esperar la probabilidad de encontrar algunas incidencias de piratería en alguno de los equipos elegidos como muestra. El auditor encontrará estas incidencias si aplica bien la muestra, pero habría muchos casos en los que no encontraría ninguna problemática, y aunque es válido aplicar una muestra así, podría retrasar mucho su trabajo y frecuentemente podría desviar su atención de este problema.

Su otra opción es elegir una muestra de todos los usuarios que cumplen con la condición de tener una PC manejada en forma independiente y que no depende del área de sistemas (éste es el criterio del muestreo de juicio). *En la elección de esta muestra determina que sólo revisará a los usuarios de estos equipos, lo cual seguramente le ayudará a identificar la problemática de una manera más sencilla y directa.*

Cuando un auditor experimentado obtiene tips similares, puede orientar su revisión hacia la comprobación de esa incidencia. Aunque este procedimiento no es totalmente válido ni científico, sí satisface las expectativas del auditor respecto a la evaluación del uso de equipos piratas de este ejemplo.

Como un agregado a este ejemplo de detección de piratería, diremos que el auditor puede utilizar paqueterías en la revisión de cada PC, con las que puede detectar los programas borrados y, si es necesario, reactivarlos. Esto se puede hacer con paqueterías tales como Norton Utilities, programas especiales de Windows para reactivar programas y con el comando Unerase de MS-DOS, por citar sólo algunos programas que identifican los archivos borrados y localizan los programas que son instalados sin contar con las licencias correspondientes, conocidos como piratas, los cuales nunca debieron ser instalados.

Para aplicar este tipo de muestreo sugerimos utilizar los siguientes criterios:

Que el criterio de elección de la muestra esté relacionado con el aspecto específico que el auditor desea investigar.

Procurar elegir los elementos que cumplan (o que se sospeche que cumplirán) con ese criterio, aunque la elección de la muestra no satisfaga los criterios estadísticos y matemáticos formales.

Que el juicio elegido como criterio no tenga vicios o tendencias que lejos de ayudar perjudiquen la elección de la muestra.

Que el criterio para elegir los elementos de la muestra no se utilice para validar casos aislados con los cuales se quiera generalizar a los demás, nada más para suponer la presencia de desviaciones.

Cuando se pueda, extender este muestreo a 100% de la muestra; siempre y cuando el criterio lo permita y los resultados ameriten este incremento significativo para la opinión del auditor.

Que no se desvirtúe el uso de los resultados de este tipo de muestreo, ni para minimizar ni maximizar problemas.

Utilizar este tipo de muestreo sólo para casos concretos y específicos, pero nunca para sustituir comprobaciones formales de los otros métodos de muestreo. Mucho menos para darle validez estadística y matemática para comprobaciones formales.

9.6.3.3 Muestreo por computadora

Este tipo de muestreo se hace utilizando la computadora como elemento de apoyo, ya que por medio de hojas de cálculo, programas estadísticos o programas especiales de cómputo se puede elegir una muestra representativa de la población, tomando los datos por cierta característica especial que deben cumplir para ser útiles en la auditoría, o tomando los datos que cumplan con alguna condición especial en el procesamiento de información, o simple y sencillamente eligiendo los sistemas computacionales al azar.

Existen muchos procedimientos de elección de mues-

AUDITORÍA EN SISTEMAS COMPUTACIONALES

Proceso de selección aleatoria de operaciones realizadas

Operación seleccionada

Día	Núm. aleatorio	Operación	Observaciones	Marca
Sábado	1	0,18314232	164	
Domingo	2	0,42077695	842	
Lunes	3	0,66172642	1986	
Martes	4	0,02645002	106	
Miércoles	5	0,97698049	4886	
Jueves	6	0,13672134	822	
Viernes	7	0,95160259	6662	
Sábado	8	0,9003148	7204	
Domingo	9	0,20294288	1828	
Lunes	10	0,31336561	3134	
Martes	11	0,77496015	8526	
Miércoles	12	0,0949986	1140	
Jueves	13	0,19257464	2504	
Viernes	14	0,48686793	8818	
Sábado	15	0,74124672	11120	

tras de los propios sistemas, desde procesos aleatorios y estadísticos, los que cumplen con una condición especial, hasta la elección al azar de los propios datos que se procesan en el sistema y que son seleccionados para su evaluación. Para el caso de la auditoría de sistemas computacionales cualquiera es válido, lo importante es que con dicho método se satisfagan los objetivos de recopilación de información.

9.6.3.4 Muestreo por censos

La principal característica de este tipo de muestreo es que se parte de un censo previo que se toma como el universo del cual saldrán todos los elementos que conformarán la muestra, pero, en este caso especial, el censo también incluye cada una de las estratificaciones, divisiones y rangos naturales de la población que conforma el universo, y de cada rango se toma una muestra representativa.

Ejemplo para estratificar muestras

Para un buen entendimiento de este punto, supongamos que una empresa tiene 2 500 empleados y que 1 000 de ellos no tienen ninguna relación con los sistemas computacionales de la empresa, mientras que los otros 1 500 utilizan los sistemas para realizar sus actividades. Entonces, si la evaluación fuera sólo sobre el uso de los sistemas computacionales, el universo útil para el auditor serían únicamente los 1 500 empleados. Si fuera otro tipo de evaluación, entonces el universo serían los 2 500 empleados.

En el muestreo por censos es muy importante estratificar el 100% de todos los elementos que pueden ser elegidos como muestra (universo) y seguir estratificando cada uno de los rangos por características o peculiaridades naturales en que se puede dividir ese universo, para obtener el porcentaje que corresponda a cada estrato del universo.

Ejemplo para definir un universo

Supongamos que del total de 1 500 empleados del ejemplo anterior, el 54% son hombres y el 46% son mujeres; entonces se tomará como otra parte del censo el total de empleados del sexo masculino ($1\,500 \times .54 = 810$) y el total del sexo femenino ($1\,500 \times .46 =$ *690*).

Si dentro de ese universo existieran más estratificaciones, cualesquiera que sean, estos rangos serían respetados, considerando el porcentaje que representan para cada estrato, en relación con el 100% de los elementos con los que se puede hacer un muestreo (universo). En todos los casos se indican estos porcentajes.

El siguiente ejemplo aclarará más la concepción de este tipo de muestreo:

Supongamos que la empresa Grandota, S.A. tiene un total de 3 000 empleados y que el auditor desea conocer la opinión de los empleados sobre el comportamiento, apoyo y utilidad de los sistemas computacionales; pero de los 3 000 empleados, 1 000 son los que realmente utilizan los sistemas computacio-

nales para realizar sus funciones. La opinión de estos trabajadores es la que desea conocer el auditor, por lo tanto, su universo censado serán 1 000 empleados y de ellos obtendrá la muestra representativa.

En el censo se encontró que de estos 1 000 empleados (100%), 200 están asignados al área de sistemas (20%) y los 800 restantes son usuarios de los sistemas computacionales en alguna de sus modalidades (80%).

El primer grupo de empleados adscritos al área de sistemas, que representa *el 20% del universo*, está constituido de la siguiente manera, según el censo realizado previamente:

- **50** empleados (5%) asignados al desarrollo de sistemas, en cualquier modalidad
- **80** empleados (8%) asignados a la operación de los sistemas de la empresa
- **40** empleados (4%) asignados al mantenimiento de los sistemas
- **20** empleados (2%) asignados al apoyo administrativo del área de sistemas
- **10** empleados (1%) son ejecutivos del área de sistemas

El segundo grupo, representado por usuarios, está compuesto por el 80% del universo; según el censo realizado previamente, se determinó que está estratificado de la siguiente manera:

- 400 usuarios (40%) utilizan los sistemas sólo como medio de consulta
- 200 usuarios (20%) utilizan los sistemas para la captura de información
- 100 usuarios (10%) utilizan los sistemas para corrección de bases de datos
- 100 usuarios (10%) utilizan los sistemas para hacer modificaciones al programa

Mediante algún criterio, cualquiera que sea, se determina que la muestra será el 10% del total de los elementos que integran ese universo. El auditor puede obtener opiniones de los 1 000 empleados que utilizan los sistemas, respecto a la utilidad, comportamiento y apoyo que brindan los sistemas, porque ellos sí trabajan en los sistemas y los conocen.

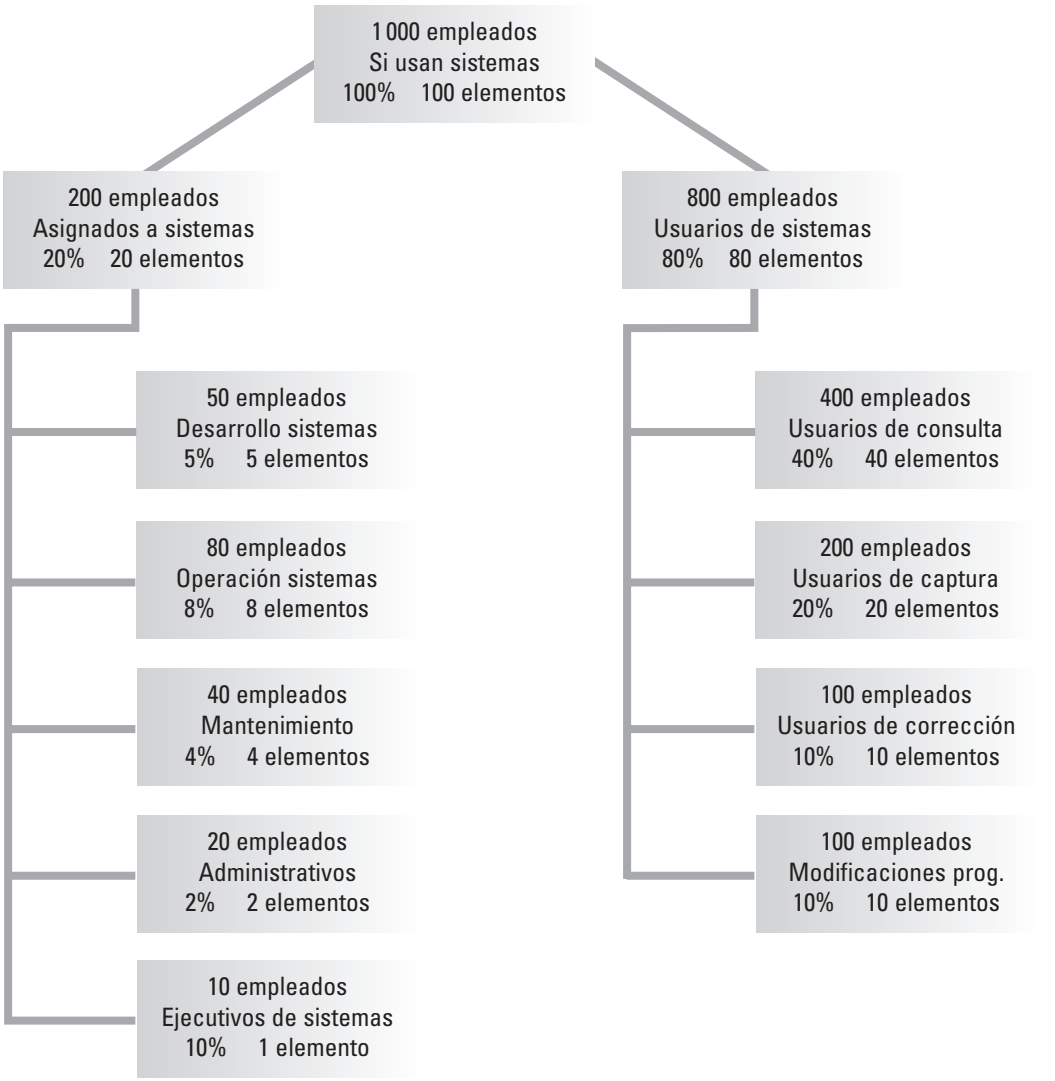
En este caso, la opinión de los 2 000 empleados restantes no será tomada en cuenta, debido a que no aportarían ningún dato significativo para el auditor y, al no estar en contacto con los sistemas computacionales, su opinión sería demasiado vaga y subjetiva.

Entonces la selección de la muestra quedaría conforme a los porcentajes obtenidos del número de empleados de cada estrato censado. Los 1 000 empleados representan el 100% del universo y el porcentaje de cada rango será calculado conforme a esta sencilla fórmula: el número de empleados del rango entre el total de empleados del universo nos da el porcentaje.

Empleados del rango

Total de empleados del universo

Este ejemplo se describe mejor en los siguientes cuadros:



El número de empleados elegidos para cada estrato será determinado por el porcentaje que representa del total del universo, por ejemplo, el estrato de *200* empleados del área de sistemas representa el **20**% del universo y los elementos elegidos serán *20*, mientras que los 800 usuarios representan el **80**% del universo y serán elegidos *80* elementos. El estrato de *40 empleados* de

mantenimiento de sistemas representa el **4%** del total del universo y los elementos elegidos serán 4, y así en cada estrato utilizado.

El formato que proponemos utilizar es un cuadro con los siguientes conceptos:

Total de elementos que pueden ser elegidos por cada estrato	
Nombre del rango o estrato	
% del universo total	Número de elementos elegidos

Total de elementos que pueden ser elegidos por cada estrato; aquí se anotará el total del universo o el número de los integrantes de cada uno de los estratos. En el ejemplo del universo total fueron 1 000 empleados, del estrato de usuarios fueron 800 empleados y del estrato de ejecutivos del área de sistemas fueron 10 empleados.

Nombre del rango o estrato; en esta parte media del cuadro se anota, lo más completo posible, el nombre que se le da al estrato.

Porcentaje del universo total; aquí se anota el porcentaje que representa el número de integrantes del estrato, respecto al 100% del universo total. En el ejemplo, los empleados asignados al área de sistemas representan el 20% del total del universo y los usuarios para corrección de datos representan el 10%.

Número de elementos elegidos; en este recuadro se anota el total de los elementos que serán elegidos de cada estrato; es propiamente el número de integrantes de ese estrato que serán seleccionados para integrar la muestra. En el ejemplo se eligen cuatro elementos de los empleados de mantenimiento y 20 de los usuarios de captura.

El uso de este muestreo por censo es de mucha ayuda para elegir muestras más o menos homogéneas y representativas del total de elementos que pueden integrar una muestra; siempre y cuando se parta de un censo previo que abarque el total de los elementos que pueden integrar la muestra.

Si es necesario, se pueden aplicar fórmulas estadísticas y matemáticas para establecer los rangos de seguridad en la elección de las muestras, así como los rangos de confiabilidad necesarios para darle la validez matemática a este tipo de muestreos.

9.7 Experimentación

Ésta es una de las herramientas más utilizadas en cualquier tipo de auditoría y una de las que más ayudan al auditor a recopilar la información que requiere para realizar una auditoría de sistemas; el auditor puede aplicar esta herramienta por sí mismo o ayudándose de algún instrumento de registro, en el que recopilará los datos que le servirán para su evaluación.

La experimentación se puede definir de la siguiente manera:

Es la observación de un fenómeno en estudio, al cual se le van adaptando o modificando sus variables conforme a un plan predeterminado, con el propósito de analizar sus posibles cambios de conducta como respuesta a las modificaciones que sufre dentro de su propio ambiente o en un ambiente ajeno. Todo ello con el fin de estudiar su comportamiento bajo diversas circunstancias y sacar conclusiones.

En la experimentación, quien lleva a cabo la auditoría puede o no participar activamente en la observación del fenómeno en estudio y, conforme a un plan preconcebido (*el programa de auditoría*),* puede hacer deliberadamente los cambios necesarios con los cuales modifica sistemáticamente el comportamiento del fenómeno en estudio; posteriormente, el auditor observa las alteraciones que se presentan con esas modificaciones, las valora cuantitativa y cualitativamente, y analiza las repercusiones de esos cambios en el sistema observado; después toma nota de todas las repercusiones que se van presentando durante la experimentación, a fin de ampliar su conocimiento sobre el fenómeno en estudio para poder emitir un juicio adecuado respecto a su comportamiento.

A continuación presentamos algunos de los principales métodos de experimentación que se pueden aplicar en una auditoría de sistemas computacionales.

9.7.1 Experimentos exploratorios

Son los experimentos cuyo objetivo fundamental no es demostrar una suposición del comportamiento del fenómeno o sistema en evaluación (hipótesis), sino investigar si las técnicas, métodos y procedimientos que serán usados serán útiles para llevar a cabo una evaluación correcta y para contemplar el comportamiento de los fenómenos en estudio; los resultados de estas experimentaciones permiten al auditor identificar el comportamiento de los sistemas que está evaluando, y le ayudan a determinar los instrumentos, técnicas y herramientas con los que realizará la evaluación de dichos sistemas.

Este tipo de experimentos se realiza con el fin de analizar y examinar los sistemas que serán evaluados, antes de iniciar el estudio formal de la problemática que repercute en dichos sistemas; el propósito de esta experimentación es descubrir los aspectos que pueden intervenir en la evaluación, así como determinar los requerimientos de investigación para la auditoría, la factibilidad de llevar a cabo dicha auditoría y todos los factores que de alguna manera intervendrán en su desarrollo.

* En el capítulo 6 explicamos todo lo relacionado con la planeación de una auditoría, así como el plan y el programa de auditoría.

Un claro ejemplo de los experimentos exploratorios es la visita preliminar que se realiza antes de iniciar una auditoría.*

En las investigaciones relacionadas con auditorías de sistemas computacionales, los experimentos exploratorios son el estudio inicial de lo que se quiere evaluar; dichos experimentos son muy útiles para el auditor, debido a que con ellos puede establecer las posibles desviaciones que encontrará durante la revisión y puede plantear los requerimientos específicos para llevar a cabo la auditoría de sistemas, así como decidir el camino que seguirá para realizar la evaluación.

Una aplicación concreta para estos experimentos es el diseño de un sistema de información, debido a que durante el diseño se experimenta el comportamiento del sistema, mediante algún modelo donde se va comprobando su comportamiento antes de ser implantado.

9.7.2 Experimentos confirmatorios

Mediante los experimentos confirmatorios se pueden corroborar o desmentir las sospechas de desviaciones que dieron origen a la realización de la auditoría,** así como confirmar la presencia de desviaciones cuando se hacen cambios en el comportamiento normal del ámbito de sistemas evaluado.

Es importante establecer que con este tipo de experimentación se busca confirmar los resultados de la suposición inicial de una desviación, ya sea para probar que ésta existe o para refutar su presencia en el ambiente de sistemas auditado; no obstante, su aplicación debe apegarse siempre a los mismos parámetros que se manejan en la operación normal, dentro del mismo marco establecido para el procesamiento del sistema y con las mismas aplicaciones, plataforma, bases de datos, programas de cómputo o cualquier otro elemento que se presente en la operación cotidiana del ambiente de sistemas. Además, para confirmar su comportamiento, también se debe contemplar que los instrumentos, técnicas y métodos utilizados en la experimentación sean siempre los mismos, a fin de garantizar los mismos resultados durante la realización de los experimentos y que éstos sean satisfactorios para el auditor.

> Un ejemplo concreto del uso de la experimentación confirmatoria es cuando se quiere confirmar la sospecha de ciertas deficiencias en la seguridad de los sistemas; para hacer esto, el auditor, u otra persona designada por él, trata de ingresar al sistema y a las bases de datos de la empresa sin tener autorización para ello, con el único fin de verificar la seguridad para el acceso a la red y la protección de la información y programas. En teoría, el auditor no

* En el punto 6.3.2. del capítulo 6 presentamos los aspectos fundamentales de esta visita preliminar, la cual se puede llevar a cabo con estos experimentos exploratorios.

** En el capítulo 6 también presentamos un apartado referente a los orígenes de una auditoría de sistemas, que en muchos casos es la parte de la fijación de objetos específicos que interesa auditar.

puede entrar al área de sistemas; mucho menos accesar al sistema ni consultar, modificar o alterar datos de las bases de datos, de los programas o del sistema.

Aunque el auditor tiene que hacer cambios a fin de analizar el comportamiento del sistema, en este caso se supone que el auditor no debería haber tenido ningún acceso al sistema. Si el auditor ingresó al sistema, entonces deberá tomar nota de todas las deficiencias que existen, ya que estaríamos hablando de desviaciones respecto a la seguridad. Con esta experimentación también se obtienen las causas de estas desviaciones.

Este método puede ser aplicado en varios aspectos de sistemas en los que sea necesario confirmar la sospecha de alguna desviación; también se aplica con bastante éxito para hacer el análisis de los resultados obtenidos con cualquier herramienta utilizada para recopilar información para la auditoría, o con las observaciones reportadas en el dictamen de auditoría de sistemas.

9.7.3 Experimentaciones cruciales

Este tipo de experimentación pone a prueba algunas de las suposiciones planteadas en el programa de auditoría, las cuales se supone que son los aspectos relevantes del ambiente de sistemas que será evaluado, por lo tanto, se tienen que comprobar dichas suposiciones por medio de experimentaciones que son cruciales para el desarrollo del propio sistema, examinando con sumo cuidado los cambios que se hacen mediante los conocimientos, teorías y métodos de investigación necesarios para evaluar el sistema, hasta comprobar su verdadero funcionamiento.

En el diseño de esta experimentación se tienen que establecer perfectamente detallados todos los procedimientos, técnicas, métodos e instrumentos que serán útiles para comprobar, al mayor grado posible, la conjetura establecida de antemano; más aún si es una presunción de una desviación del funcionamiento normal del sistema que será evaluado.

Es importante recalcar que con las experimentaciones bajo estas circunstancias se busca obtener un verdadero conocimiento del sistema en evaluación, a fin de comprobar o desmentir cualquier situación mediante la experimentación; de ahí la importancia de la experimentación y de las técnicas, instrumentos y procedimientos que serán utilizados para obener los conocimientos que se espera encontrar.

El más claro ejemplo que existe de este tipo de experimentación, es la que se debió realizar para verificar el funcionamiento de los sistemas para el año 2000, ya que fue necesario analizar todos los aspectos cruciales que hubieran podido repercutir en el funcionamiento de los sistemas. A continuación presentamos algunos casos para ejemplificar esta situación trascendental del cambio de fechas:

El funcionamiento del BIOS de los sistemas

Los cambios de fechas que pudieron afectar el funcionamiento de los sistemas que no reconocen cuatro dígitos para la fecha (DDMMAAAA), sino únicamente dos (DDMMAA):

9 de septiembre de 1999. Anotada como 090999.

El cambio de las 11:59 del 31 de diciembre de 1999, al primer segundo del 1º de enero de 2000 (de 23:59/311299 a 00:01/01012000).

El cambio del 28 al 29 de febrero del 2000, para verificar si el sistema acepta el año bisiesto.

El desarrollo, instalación y pruebas de migración de plataformas, los cuales se tienen que probar exhaustivamente hasta comprobar su perfecto funcionamiento antes de liberar el sistema.

En los puntos anteriores destacamos la importancia de hacer experimentos en los ambientes de sistemas que se están evaluando, a través de cambios programados y controlados por el auditor, de acuerdo con un plan previamente diseñado y con la importancia de la evaluación.

9.7.4 Aspectos que intervienen en la experimentación

Al hablar de experimentación, inmediatamente se le asocia con las llamadas variables, dependientes o independientes, y con las constantes, ya que ambas están íntimamente relacionadas con la investigación, no sólo para auditoría de sistemas, sino para cualquier otra área; por esta razón es fundamental conocer los aspectos que intervienen en la experimentación, mismos que presentamos a continuación.

Constante

Es un fenómeno con atributos y propiedades, cualesquiera que éstos sean, cuya característica principal es que no se alteran ni llegan a variar en magnitud, categoría ni condiciones, en relación con el fenómeno de sistemas al que pertenecen.

Variable

Es un fenómeno con una propiedad o atributo cualquiera, el cual puede llegar a tomar diferentes magnitudes o categorías, en relación con el conjunto de fenómenos del ambiente de sistemas al que pertenece.

Variables independientes

Es una variable manipulada por el auditor, bajo los criterios de objetividad, confiabilidad y veracidad, de tal manera que su modificación sea real y tangible. Esta variable generalmente es considerada como la "causa" que modifica el fenómeno estudiado.

Variable dependiente

Son los resultados derivados de la manipulación de la variable independiente, ya que forman el "efecto" que modifica su conducta, y su comportamiento estará determinado por la primera variable.

Variables recurrentes

Son las variables que por algunas circunstancias de la observación siempre están presentes en los resultados y sobre las cuales no se tiene un control absoluto; en muchos casos estas variables son desconocidas y sólo se localizan como resultado de la acción de las variables anteriores; también se dice que son recurrentes porque están relacionadas directamente con el fenómeno.

Variables ajenas

Son las variables que se derivan de resultados no esperados, ya sea porque se dieron variaciones y aspectos no contemplados, o por cualquier otra causa que no había sido considerada, pero que están presentes y el auditor tiene que descubrirlas.

Variables discretas

Es frecuente que una variable independiente y una variable dependiente no guarden absoluta dependencia entre sí, dándose el caso de que se puedan presentar algunos fenómenos no contemplados en la causa y efecto de las mismas; en este caso estaremos hablando de una variables discreta.

Causalidad

Entendida como la relación que existe entre la causa y el efecto, para la experimentación en sistemas es el estudio de todas las posibles variaciones que se proyectan para afectar el fenómeno observado, a fin de conocer sus repercusión en la conducta y características de dicho fenómeno.

La causalidad siempre será determinada por los posibles criterios utilizados para normar la igualdad en su aplicación para todas las variaciones que se den en los fenómenos observados. Entre dichos criterios tenemos los siguientes.

Temporalidad

Es el ámbito especial sobre el cual se presenta el funcionamiento del fenómeno y sobre el cual se hacen las variaciones de dicho funcionamiento. Este ámbito siempre debe estar circunscrito a un mismo periodo.

Control de los factores de causalidad

Los cambios que se hacen a las variables siempre deben ser iguales o similares y estar libres de cualquier influencia, en relación con los resultados espe-

rados del fenómeno observado, a fin de que dichos resultados sean válidos en el ambiente de sistemas; dentro de este control se tiene que tomar en cuenta la validez, tanto de carácter interno como externo, y considerar los mismos factores de sistemas en las variables.

Variaciones concomitantes

Es el análisis de los resultados esperados por la variación producida que altera el sistema, es decir, es el estudio de los nuevos atributos y propiedades que son resultado de la variación inducida sobre el fenómeno del ambiente de sistemas estudiado.

Comparabilidad

Se refiere a que el efecto, resultado de la variación, sólo se da cuando está presente la supuesta causa, es decir, cuando se omite la causa no se presenta el efecto, y en caso de que se presente sin la causa, se tiene que analizar como resultado de otra causa.

Fuentes de invalidación

Es la contemplación correcta y oportuna de los posibles factores que pueden invalidar una observación, en este caso una experimentación, ya que al no considerar estos factores o al no acatarlos, los resultados de la experimentación son nulos o falsos; dichos factores son los siguientes.

Factores ambientales

Es el entorno donde se realiza la experimentación para que esté libre de influencias ajenas al fenómeno observado. En el caso de sistemas, es el ambiente de sistemas computacionales en donde se realizan las operaciones normales del sistema, contemplando todos los aspectos inherentes al mismo, a fin de que no existan factores externos que puedan influir en los resultados obtenidos del fenómeno observado.

Medición

Es la aplicación de instrumentos similares de medición para que no repercutan en los resultados de la experimentación. En el caso de sistemas computacionales, es el uso de los mismos instrumentos de medición para los experimentos realizados, así como de los mismos aspectos para experimentar el comportamiento de los sistemas.

Instrumentación

Son las herramientas de medición y comprobación que se diseñan para hacer la experimentación de los sistemas computacionales, también se incluye el di-

seño de los estándares que garanticen siempre las mismas mediciones y los mismos resultados.

Maduración

Es la ubicación exacta en tiempo y proceso del fenómeno observado en la experimentación, de tal forma que ésta sea igual para fenómenos similares.

Regresión

Es la identificación plena de la tendencia natural de los fenómenos observados, estableciendo claramente los posibles casos extremos, a fin de estandarizar las observaciones para que el auditor pueda realizar un buen análisis de las variaciones de dichos fenómenos.

Selección

Es la similitud en los criterios de elección de los fenómenos observados, tanto de elementos computacionales, herramientas, hardware, software, como de los demás elementos del sistema, a fin de que los fenómenos con los que se experimenta sean siempre los mismos y que no cambien sus conductas.

Deserción

Es la discriminación de elementos del fenómeno en experimentación; esta discriminación no impide que dicho fenómeno sea válido, si se garantiza que tal situación se contempló de antemano.

Diseño

Es la construcción correcta de los fenómenos que serán observados, de tal forma que sean adecuados para hacer la experimentación.

Las definiciones anteriores también pueden ser aplicables para las otras herramientas tratadas en este capítulo y para las herramientas, métodos, procedimientos y técnicas de auditoría de sistemas computacionales que tratemos en los siguientes capítulos.

10

Técnicas de evaluación aplicables en una auditoría de sistemas computacionales

Estructura del capítulo:

Objetivos del capítulo

Mostrar las principales técnicas de evaluación aplicables en una auditoría tradicional, con el propósito de que el auditor conozca los elementos fundamentales que le ayudarán a realizar su auditoría de sistemas, así como todos los procedimientos, herramientas, técnicas y métodos que se pueden aplicar en la evaluación de los sistemas computacionales, de las áreas de sistemas, de las actividades, funciones y demás operaciones relacionadas con dichos sistemas.

Introducción del capítulo

Debido a su probada eficiencia en otros tipos de auditorías, en la auditoría de sistemas computacionales se utilizan las herramientas tradicionales de auditoría, así como otras técnicas de valoración que permiten hacer una evaluación más eficiente de dichos sistemas o de su gestión informática.

El auditor, al utilizar estas herramientas, adopta y adapta las técnicas, métodos y procedimientos tradicionales de auditoría a las necesidades específicas de evaluación del ambiente de sistemas computacionales, aplicando lo mejor de estas herramientas.

Como profesional especializado en el ramo, el auditor de sistemas computacionales utiliza una serie de técnicas específicas que le ayudan a examinar y evaluar correctamente los diferentes aspectos del ambiente de sistemas en el que realizará su trabajo. A continuación presentamos las técnicas, métodos, procedimientos o herramientas que analizaremos:

El examen
La inspección
La confirmación
La comparación
La revisión documental
El acta testimonial
La matriz de evaluación
La matriz DOFA

10.1 Examen

En una auditoría, el examen consiste en analizar y poner a prueba la calidad y el cumplimiento de las funciones, actividades y operaciones que se realizan cotidianamente

en una empresa, y se aplica en un área o actividad específica o en una unidad administrativa completa. El examen también se utiliza para evaluar los registros, planes, presupuestos, programas, controles y todos los demás aspectos que afectan la administración y control de una empresa o de las áreas que la integran.

El auditor aplica esta herramienta con el propósito de investigar algún hecho, comprobar alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de las técnicas, métodos y procedimientos de trabajo, verificar el resultado de una transacción, comprobar la operación correcta de un sistema computacional y para evaluar muchos otros aspectos.

Dentro del ambiente de la auditoría de sistemas computacionales, esta herramienta se utiliza, entre muchas cosas, para inspeccionar la operación correcta del sistema, analizar el desarrollo adecuado de los proyectos informáticos, examinar la forma en que se realiza la captura y el procesamiento de datos, así como la emisión de resultados; también se emplea para inspeccionar las medidas de seguridad del sistema y del área de informática, examinar el acceso a dicha área, al sistema, a sus programas y a la información de las bases de datos, para examinar la forma en que se archivan y protegen los datos de los sistemas, sus programas y la propia información; además pone a prueba el cumplimiento de las funciones y actividades de los funcionarios, personal y usuarios del centro de cómputo.

Para entender mejor la aplicación de esta técnica, a continuación haremos un análisis de sus principales definiciones y posteriormente presentaremos algunos ejemplos de las aplicaciones de esta herramienta.

Examinar

"Investigar con diligencia algún hecho o situación. Comprobar la calidad de una cosa. Poner a prueba la aptitud y conocimientos de alguien [...]"[1]

"Del latín ***examinare****: Hacer el examen de una persona o una cosa [...] Inspeccionar, escrutar, sondear, analizar, estudiar [...] Interrogar a un candidato [...] Mirar atentamente [...]"*[2]

Examen

"Estudio y análisis que se hace de personas, hechos o cosas. Prueba de idoneidad en alguna ciencia o arte."[3]

"Del latín **examen***:* Investigación, indagación *[...] Reflexión [...] Prueba a que se somete un candidato a un grado o examen [...] Prueba, comparación [...]"*[4]

Prueba

"Acción y efecto de probar. Razón con la que se demuestra una cosa. Demostración y testimonio. Examen y tentativa. Operación que sirve para comprobar si estaba bien otra operación anterior."[5]

"Acción o efecto de probar. Razón o argumento, hecho que muestra la verdad o falsedad de algo. Ensayo o experiencia que se hace de algo. Acto, indicio, documento, etcétera, que se aportan [...] para demostrar algo."[6]

En la auditoría de sistemas computacionales podemos entender el examen o prueba como:

> *El análisis, prueba o demostración al que se somete algún fenómeno o hecho relacionado con la gestión administrativa de un centro de cómputo, de sus componentes o de la operación del sistema procesador de información, con el propósito de evaluar el cumplimiento de sus funciones, actividades y operaciones, así como el cumplimiento del procesamiento de datos y la emisión de información que se requiere en la empresa o en las áreas que la integran.*

El término *examen* es una aplicación enunciativa de carácter genérico, debido a que la palabra examen casi siempre se vincula con la escuela o con un aspirante a algún empleo. Sin embargo, en una auditoría de sistemas computacionales este vocablo siempre se debe acompañar de algún calificativo *(examen y su calificativo)*; ambos determinarán el direccionamiento y su aplicación concreta en este tipo de auditoría. Conviene agregar que esto puede ser aplicable en cualquier otro tipo de auditoría.

A continuación presentamos las principales aplicaciones de los exámenes en una auditoría de sistemas computacionales.

10.1.1 Examen del comportamiento del sistema

Esta aplicación se refiere a las pruebas que hace el auditor, e incluso el propio desarrollador de un sistema, con el propósito de saber cómo se comporta el sistema en los distintos ambientes en donde se realiza su operación normal; esto permite comprobar las características del comportamiento y actuación del propio sistema y en muchos casos ayuda a examinar el ambiente donde será implantado; asimismo, el auditor puede evaluar el funcionamiento del sistema computacional, el rendimiento de su procesador, componentes y periféricos, además del uso y aprovechamiento de los lenguajes y programas utilizados en el procesamiento y emisión de informes. Claro que dicho examen se hará de acuerdo con las características y necesidades específicas de la evaluación, así como del propio sistema computacional y del centro de cómputo que será examinado.

10.1.1.1 Examen de los resultados del sistema

Es la aplicación de las pruebas necesarias al ciclo normal de captura, procesamiento y emisión de la información procesada en el sistema computacional de la empresa, por medio de exámenes específicos del comportamiento, velocidad, exactitud y demás características del procesamiento de los datos. Además, es recomendable reali-

zar también la comprobación manual, mecánica o electrónica del procesamiento de esos datos, con el propósito de comparar el comportamiento de ambos resultados, el del sistema computacional y el manual o mecánico; esto ayuda a evaluar la confiabilidad y veracidad del procesamiento de la información. A este tipo de exámenes se le conoce como prueba de los resultados y tiene muchas modalidades y formas de aplicación.

10.1.1.2 Pruebas de implantación

Son las comprobaciones previas a la implantación de un sistema computacional, con el fin de verificar si el diseño del nuevo sistema corresponde al comportamiento real de dicho sistema; estas comprobaciones se realizan a través del procesamiento de datos (supuestos o verdaderos), comparando los resultados que arrojan las pruebas del nuevo sistema con los resultados reales que se obtuvieron por cualquier otro medio (con otro sistema similar, en forma manual, mecánica, etcétera).

Básicamente se conocen tres formas de realizar estas pruebas de implantación:*

Las pruebas piloto

Son las pruebas que se realizan a los prototipos del sistema computacional, al diseño y programación de los propios sistemas e incluso a los diseños en papel; el propósito es evaluar el comportamiento del sistema antes de empezar su diseño detallado (formal) o final, con el fin de identificar toda la problemática que se puede presentar en el funcionamiento del sistema; con este tipo de pruebas se pueden elaborar todas las correcciones que sean necesarias para el mejor diseño del sistema.

El auditor debe verificar la existencia de estas pruebas y la manera en que se aplicaron; además puede analizar los resultados obtenidos y las correcciones derivadas de esas pruebas. También puede utilizar los resultados de esas pruebas para evaluar el desarrollo de los proyectos informáticos, e incluso puede evaluar si la forma en que se realizaron estas pruebas, sus resultados y aplicaciones, son los adecuados para el trabajo de los sistemas.

Las pruebas en paralelo

Son las pruebas del funcionamiento del nuevo sistema y, al mismo tiempo, del sistema anterior; para ello se utilizan las mismas operaciones y procesos de in-

* Recordemos que los métodos de implantación de sistemas son: **instantáneo** (mediante esta práctica se sustituye el sistema anterior por el nuevo), **por etapas sucesivas** (aquí se implanta por partes el sistema nuevo, primero una sección, luego otra y así sucesivamente, hasta que se implanta en su totalidad)**, en paralelo** (es cuando se implanta el sistema nuevo, pero al mismo tiempo sigue funcionando el anterior, a fin de evaluar el resultado del sistema nuevo en comparación con el anterior) y **pruebas piloto** (en este método se hacen todas las pruebas necesarias al sistema hasta que los resultados son satisfactorios; después se adopta alguno de los métodos anteriores).

formación, con datos y secuencias iguales, y en sí con los mismos procedimientos, a fin de comparar los resultados de ambos sistemas; con esto se garantiza que el funcionamiento del nuevo sistema sea igual o mejor que el del sistema anterior.

Estas pruebas tienen muchas aplicaciones en una auditoría de sistemas computacionales, por ejemplo, se pueden aplicar pruebas en paralelo, con los mismos datos, en un sistema nuevo y en uno anterior. También se pueden hacer las pruebas del sistema con datos falsos o datos simulados, ya sea en el sistema a probar o en otro sistema ajeno a éste.

Es importante que también se evalúe el registro de las pruebas realizadas al sistema, así como la implantación del mismo, bajo el método de pruebas en paralelo.

Las pruebas de aproximaciones sucesivas

Este tipo de pruebas se realiza por partes; primero se hacen las pruebas elementales y después se van realizando más pruebas, cada vez más complicadas, de tal manera que en cada nueva prueba se van obteniendo los resultados esperados del funcionamiento del sistema.

Para aplicarlas en la auditoría de sistemas computacionales, el auditor comprueba la manera en que se realizaron y registraron estas pruebas, así como los resultados alcanzados con ellas; en caso de ser necesario, también se pueden realizar las pruebas con el método descrito anteriormente.

10.1.1.3 Pruebas del sistema

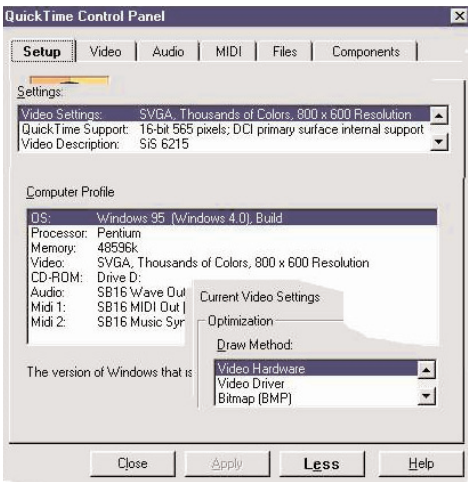
También identificadas como auditoría del sistema computacional, es la sucesión de pruebas, exámenes y comprobaciones de la actividad del sistema computacional, en cuanto a la confiabilidad de su operación, el procesamiento de información, el funcionamiento de sus periféricos y equipos asociados, su arquitectura, el funcionamiento de sus procesadores, la velocidad de éstos, el trabajo de las memorias, la lectura y grabación correctas de información en los dispositivos externos y todas las demás pruebas que se realizan al sistema, con el propósito de conocer y evaluar su funcionamiento.

Estas pruebas se pueden realizar por medio del sistema operativo, aprovechando las rutinas integradas en el procesador, o se pueden hacer utilizando paqueterías y programas de cómputo diseñados para ello.

En estos casos el auditor verifica y comprueba, por medio de pruebas, procedimientos y rutinas especiales de auditoría, que los procesos y programas del sistema, así como la actividad de todos sus componentes, periféricos y equipos asociados, funcionen correctamente.

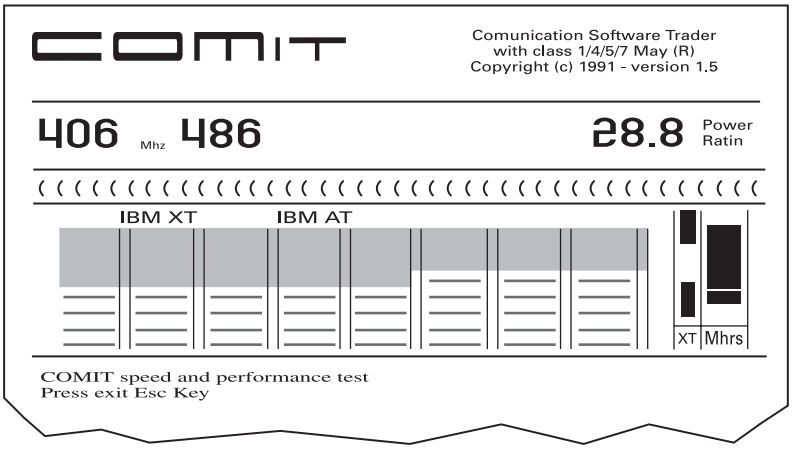
Los siguientes son algunos ejemplos de las pruebas al sistema:

En este ejemplo se maneja un programa especializado de Apple Computer Inc., Quick Time for Windows*, el cual se utiliza para verificar el contenido, los componentes y el funcionamiento del sistema. Como ya se dijo anteriormente, estas utilerías se emplean para verificar el funcionamiento del sistema, así como cada uno de sus componentes internos, su velocidad de procesamiento, la forma de lectura y captura de información y muchas otras rutinas de revisiones especializadas.



Presentamos esta utilería únicamente para ejemplificar alguno de los muchos productos que pueden ayudar a realizar las pruebas requeridas para una auditoría de sistemas.

COMIT** es una marca registrada por *Communications Software by Tradenw Inc*., la cual se utiliza para ejemplificar otra manera de comprobar el funcionamiento del procesador de estos sistemas, como apoyo al trabajo del auditor de sistemas.



* **Quick** Time for Windows es propiedad de *Apple Computer, Inc.* 1988-1996. Derechos reservados.
** **COMIT** es propiedad de *Communications Software by Tradenw, Inc*. 1993. Derechos reservados.

10.1.1.4 Pruebas de los programas de aplicación

Comúnmente conocidas como pruebas de escritorio, son las experimentaciones del diseño de un nuevo proyecto de sistemas, a través de pruebas que se realizan de manera manual, mecánica o electromecánica (o también por medio de algún modelo), comparando, uno por uno, todos los pasos que supuestamente seguirían las rutinas de procesamiento de información del nuevo sistema, con el propósito de localizar las posibles deficiencias del nuevo proyecto. En la práctica, estos experimentos se realizan antes de implantar un sistema computacional. En estas pruebas, el diseñador del proyecto simula el comportamiento del nuevo sistema, con el fin de encontrar las posibles fallas del diseño del sistema para hacerlo más eficiente.

La diagramación de sistemas* es uno de los ejemplos más ilustrativos de estas pruebas; mediante este método, tanto el diseñador del sistema como el programador, el líder de proyecto e incluso el auditor de sistemas pueden simular el comportamiento de un sistema, con el fin de evaluar su posible funcionamiento, a través del seguimiento de las operaciones que éste realiza por medio de la simbología con significados específicos. También se utilizan los modelos y la programación para comprobar el funcionamiento de los proyectos de sistemas.

10.1.1.5 Pruebas del sistema operativo

Son las rutinas de verificación y comprobación instaladas dentro del propio sistema computacional, las cuales se activan cuando inicia el sistema operativo; el propósito de estas pruebas es verificar el funcionamiento del procesador, de sus componentes, las memorias, los sistemas de operación y procesamiento, los buses de conexión (conexiones del sistema) y funcionamiento de los periféricos, comunicaciones y demás partes que hacen funcionar el sistema. Éste es un procedimiento de comprobación interna diseñado por los fabricantes del sistema, el cual se aplica en forma secuencial y ordenada. Al encontrar diferencias o desviaciones en el funcionamiento del sistema, este programa las reporta de inmediato y en algunos casos las corrige por medio de sus mismas rutinas.

Además de las rutinas del sistema operativo, también existen varias utilerías y programas especiales de revisión que puede utilizar el auditor para evaluar el funcionamiento de los sistemas; en algunos casos, sobre todo en los sistemas de red y sistemas mayores, el propio sistema puede almacenar los resultados de su revisión en bitácoras y reportes, con el fin de tener registrado el proceso de verificación de su comportamiento.

En la actualidad es común que los propios sistemas computacionales realicen una revisión de sus sistemas operativos, mediante rutinas especiales, corrigiendo sus posibles deficiencias y reportándolas mediante mensajes en pantalla.

Cada sistema operativo reporta en pantalla sus propios mensajes de error al encontrar deficiencias en su funcionamiento. Cuando el auditor ve estos mensajes, debe

* En el capítulo 11, sección 11.6, se presentan las diferentes formas de diagramación de sistemas.

revisar su tipo y frecuencia y la manera en que los responsables del sistema solucionan los errores; algunas veces estos errores son reportados en las bitácoras del sistema, en los reportes internos de la auditoría del sistema o en algún otro registro del sistema operativo.

10.1.1.6 Pruebas de encendido del sistema

Similares a las anteriores, son las verificaciones y comprobaciones que el sistema, al encender, realiza de sus componentes, periféricos y programas de operación y procesamiento; estas revisiones también se realizan por medio de rutinas y procedimientos de verificación internos diseñados por los fabricantes del sistema.

10.1.1.7 Exámenes de las instalaciones del centro de cómputo

Es la verificación y evaluación del funcionamiento de las instalaciones de un centro de cómputo, de sus comunicaciones, sus sistemas eléctricos, sus conexiones entre componentes, sus sistemas de aire acondicionado, las medidas de prevención para evitar y combatir incendios, inundaciones y demás riesgos internos o externos, así como de los sistemas de seguridad y planes de contingencias, y en sí de todos los aspectos que repercuten en el funcionamiento del área de sistemas de la empresa.

No presentamos ejemplos de estas pruebas, ya que sería muy exhaustivo debido a que son muy especializadas y se tienen que realizar de acuerdo con las necesidades específicas de evaluación del auditor; por esta razón, sólo mencionamos este tipo de pruebas.

10.2 Inspección

En la auditoría de sistemas computacionales, la técnica de inspección está relacionada con la aplicación de los exámenes que se realizan para evaluar el funcionamiento de dichos sistemas; mediante la inspección se evalúa la eficiencia y eficacia del sistema, en cuanto a operación y procesamiento de datos. Lo mismo ocurre para la gestión administrativa de un centro de cómputo, en donde se hace una inspección detallada con el propósito de evaluar el cumplimiento de sus funciones, actividades, estructura organizacional y todos los demás aspectos administrativos.

La inspección se realiza a cualquiera de las actividades, operaciones y componentes que rodean los sistemas. Con esta técnica se puede evaluar, verificar y juzgar el funcionamiento de los sistemas computacionales de la empresa, así como la realización adecuada de todas sus actividades.

Los comentarios y análisis del punto anterior también sirven para la aplicación de esta técnica; la única diferencia es que en la inspección se deben aplicar los resultados de los exámenes con el propósito de emitir un veredicto sobre el aspecto verificado.

Siguiendo la costumbre de este libro, a continuación presentamos algunas definiciones de inspección:

Inspección

"Acción y efecto de inspeccionar [...] Cuidado de velar por una cosa [...]"[7]

"Acción y efecto de informar o examinar [...] Revista [...] Examen que hace un juez de un lugar o de una cosa."[8]

Inspeccionar

"Examinar atentamente una cosa; vigilar el funcionamiento de alguna empresa."[9]

"Examinar como inspector [...] Examinar."[10]

El término inspección, aplicado al ambiente de sistemas computacionales, también puede ser sinónimo de supervisión, ya que en ambos casos se trata de examinar la forma en que se desarrollan las actividades de un área de sistemas computacionales, a fin de evaluar y emitir un informe sobre el desarrollo normal de sus funciones y operaciones. La inspección también tiene como propósito monitorear el desarrollo cotidiano de las funciones, actividades y operaciones normales de la empresa, para evaluar y, si es necesario, corregir su desarrollo; claro está, con las diferencias específicas que existen en cuanto a la acepción del vocablo y su aplicación concreta en el ambiente de sistemas. Por ello, es importante tomar en cuenta que no es lo mismo hacer una inspección de auditoría que hacer la supervisión de las actividades de los sistemas.

Esta herramienta se aplica de acuerdo con las características específicas de cada centro de cómputo o de cada sistema computacional. Sin embargo, a continuación presentamos algunos ejemplos de los posibles aspectos del ambiente de sistemas computacionales en donde se puede aplicar la inspección:

- *La inspección de los sistemas de seguridad y protección de las instalaciones, equipos, personal y de los propios sistemas de procesamiento, con el propósito de dictaminar sobre su eficiencia y confiabilidad.*
- *La inspección de los formatos para la captura de datos y sus procedimientos en su introducción al sistema de procesamiento de información, a fin de evaluar su eficiencia, oportunidad, confiabilidad y veracidad.*
- *La inspección del uso, almacenamiento y protección de los sistemas, programas e información que se procesa en el centro de cómputo, con el propósito de emitir un dictamen sobre su seguridad y uso.*
- *La inspección del cumplimiento de las funciones, actividades y responsabilidades de cada uno de los funcionarios, personal, usuarios, asesores y proveedores del área de sistemas, a fin de opinar sobre su actuación.*
- *La inspección de la distribución geográfica del mobiliario, equipos, sistemas y conexiones del área de sistemas computacionales, así como de los aspectos relativos a su ambiente, ergonomía, funcionalidad, y seguridad.*

- *La inspección del uso, funcionalidad, configuración y aprovechamiento de las redes de cómputo, así como de sus sistemas operativos, de aplicaciones, desarrollo de sistemas, arquitectura, conexiones y de todos los demás aspectos relacionados con la operación de la red de cómputo.*

10.3 Confirmación

Uno de los aspectos fundamentales para la credibilidad de una auditoría es la confirmación de los hechos y la certificación de los datos obtenidos durante la revisión, ya que el resultado final de una auditoría es la emisión de un dictamen en el que el auditor vierte sus opiniones; pero, para que el dictamen sea plenamente aceptado, es necesario que los datos sean veraces y confiables, y que las técnicas y métodos utilizados para la auditoría sean los adecuados.

Un auditor jamás puede fundamentar sus opiniones en suposiciones y conjeturas falsas, ni emitir juicios basados en *datos que no sean verídicos* o que no estén certificados plenamente, o en datos obtenidos con técnicas y herramientas de auditoría que no garanticen la comprobación de la información recabada.

La absoluta confianza en las opiniones emitidas en el dictamen de la auditoría es uno de los aspectos fundamentales de esta disciplina, debido a que los resultados deben estar fundamentados en información que sea plenamente comprobada y confirmada a través del uso de las técnicas, herramientas, procedimientos e instrumentos adecuados para la auditoría.

La característica fundamental de una auditoría, cualquiera que sea su tipo, es la autenticidad con la que el auditor emite sus opiniones, sean a favor o en contra.

Debemos reiterar que en la auditoría de sistemas computacionales, al igual que en otras auditorías, la confirmación es uno de los elementos fundamentales que ayudan al auditor a certificar la validez de su dictamen de auditoría.

Como podemos ver, en una auditoría de sistemas computacionales es muy importante comprobar la veracidad y confiabilidad de los datos obtenidos durante la revisión, así como confirmar que los procedimientos utilizados para su captura y procesamiento estén apoyados en pruebas realizadas por el auditor.

De esta manera, el dictamen lleva implícitas la autenticidad y confiabilidad de las pruebas con las que se obtuvo la información; esto por sí solo sería la confirmación de que la información obtenida es veraz, confiable y que está debidamente comprobada.

A continuación presentamos algunas definiciones de confirmación:

Confirmar

"Del latín **confirmare***: Hacer más cierto, más estable [...]"*[11]

Confirmación

"Del latín **confirmatio:** *Lo que hace una cosa más segura. Nueva prueba o seguridad de una cosa."*[12]

"Corroborar la verdad de una cosa. Dar validez a lo ya probado. Dar mayor seguridad a una persona o a una cosa [...]"[13]

A continuación presentamos algunos ejemplos sobre la confirmación en la auditoría de sistemas:

- *Confirmar la oportunidad, confiabilidad y veracidad de los pagos de nómina del personal de la empresa, comparando los resultados de una quincena con los cálculos manuales de esa misma quincena.*
- *Autentificar la captura de una base de datos de los registros de alumnos de licenciatura del plantel sur de una universidad privada, cotejando los registros individuales de esos estudiantes, contra la información emitida en el sistema computacional.*
- *Validar las desviaciones encontradas en el procesamiento de datos de un lote de captura para ingresar suscriptores de una revista cualquiera para el mes de marzo, a través del cotejo manual de los datos de los suscriptores contra los listados capturados.*
- *Revisar las licencias del software instalado en los sistemas computacionales de la empresa, a fin de confirmar que no haya software instalado sin licencia.*
- *Realizar los simulacros de las medidas preventivas y correctivas establecidas en los planes de contingencias del área de sistemas, a fin de confirmar la suficiencia y buen funcionamiento en la aplicación de dichos planes.*
- *Confirmar la confiabilidad de las protecciones, contraseñas y demás medidas de seguridad establecidas para el acceso a la información y a los sistemas de la empresa, verificando su invulnerabilidad y buen funcionamiento.*

10.4 Comparación

Otra de las técnicas utilizadas en el desarrollo de cualquier auditoría es la comparación de los datos obtenidos de una área o de toda la empresa, cotejando esa información contra datos similares o iguales de un área o empresa con características semejantes. Con la comparación de la información se pueden encontrar las similitudes y diferencias entre ambas áreas o empresas, con lo cual se pueden hacer conjeturas y deducciones sobre las desviaciones encontradas.

La utilidad de esta herramienta radica en que permite hacer la evaluación de datos similares o iguales entre dos entidades (*la analizada y una similar*); con esto se obtiene información relevante para la evaluación de la entidad evaluada, ya que se compara la forma en que debería funcionar y la forma en que está funcionando, en relación con la otra entidad.

En la auditoría de sistemas computacionales, la comparación de los datos procesados en el sistema computacional que va a ser evaluado con los datos de algún sistema similar o igual, sirve para avalar y comprobar que los procesamientos sean similares o

iguales y que los resultados obtenidos sean confiables, verídicos, oportunos y que satisfagan las necesidades de procesamiento del área de cómputo de la empresa.

En algunos casos, los resultados obtenidos del procesamiento de datos de un sistema computacional deben ser comparados con los resultados obtenidos de manera manual o mecánica de esos mismos cálculos; el objetivo de dicha comparación es comprobar la similitud y veracidad de ambos resultados, o determinar las posibles desviaciones, errores o deficiencias que hay entre ambos procesamientos.

Esta herramienta también se utiliza para evaluar el cumplimiento de las funciones, actividades y operaciones del personal de informática, la aplicación de metodologías para el desarrollo de sistemas, las técnicas de programación de lenguajes, el uso de paqueterías, programas integrales y aplicaciones de sistemas computacionales, así como el uso de técnicas similares y métodos de instalación de sistemas, e inclusive la adopción de los tipos de topologías, protocolos, configuraciones y demás herramientas utilizadas para la implantación de sistemas de redes.

A continuación analizamos sus principales conceptos:

Comparación

"Del latín **comparatio***:* Acción de comparar*. Paridad, similitud, paralelo, cotejo, confrontación."*[14]

Comparar

"Del latín ***comparare****: Establecer la relación que hay entre dos seres. Analizar. Cotejar. Confrontar."*[15]

"Determinar las semejanzas o diferencias que hay entre dos o más elementos."[16]

A continuación presentamos algunos ejemplos de comparación en una auditoría de sistemas; como ya hemos dicho en muchos puntos, la comparación también se debe aplicar de acuerdo con las necesidades y características específicas del área de sistemas o del propio sistema que va a ser auditado:

- *La corrida de datos del área de contabilidad en su programa de contabilidad (el sistema por evaluar) y la corrida de esos mismos datos en otro programa de contabilidad de otra área u otra empresa (el sistema que sirve de referencia), a fin de comparar los resultados obtenidos en ambos programas, para evaluar las similitudes y diferencias de ambos procesamientos y emitir un dictamen sobre el funcionamiento del sistema por evaluar.*
- *Determinar las actividades y operaciones desarrolladas en un centro de cómputo, a fin de compararlas con las de otro centro similar para evaluar su eficiencia y eficacia.*
- *Comparar las similitudes y diferencias en el uso de la metodología institucional para el análisis, diseño e implantación de sistemas computacionales de una empresa, a fin de verificar que en los diferentes proyectos que se realizan en el área de sistemas se utilicen la misma metodología, técnicas y herramientas.*

- *Desarrollar una aplicación en una paquetería específica (por ejemplo, una hoja de cálculo) en el equipo computacional de un área de la empresa y hacer la misma aplicación (también en hoja de cálculo) en el sistema central de la empresa, a fin de corroborar la similitud en los resultados de esa aplicación; en caso de ser necesario, se comparan los procedimientos y los cálculos obtenidos; en algunas ocasiones se analizan las diferencias y similitudes en el desarrollo de las actividades y operaciones para el mismo procesamiento.*

10.5 Revisión documental

Una de las herramientas tradicionales y quizá de las más utilizadas en cualquier auditoría es la revisión de los documentos que avalan los registros de operaciones y actividades de una empresa, principalmente en aquellos casos donde la evaluación está enfocada a los aspectos financieros, el registro de los activos de la empresa y a cualquier otro aspecto contable y administrativo. Esta técnica se aplica verificando el registro correcto de datos en documentos formales de la empresa y, con mucha frecuencia, en la emisión de sus resultados financieros.

Esta costumbre de revisar los registros es muy socorrida por los contadores en las auditorías de carácter contable, fiscal y financiero, debido a que es un requisito obligatorio evaluar el registro de las operaciones financieras de la empresa, ya que con esos registros se evalúa la elaboración de sus estados de resultados financieros. Esto se lleva a cabo mediante la revisión y evaluación de los registros realizados en las llamadas pólizas, libros diarios y otros documentos contables.

Sin embargo, además de revisar los documentos financieros de la empresa, también se puede revisar el registro de las actividades y operaciones que se plasman en documentos y expedientes formales, con el fin de que el auditor sepa cómo fueron registradas las operaciones, resultados y otros aspectos inherentes al desarrollo de las funciones y actividades normales de la empresa.

En esta evaluación se revisan los manuales, instructivos, procedimientos diseñados para las funciones, actividades y operaciones, el registro de resultados, estadísticas y otros instrumentos de registro formal de los alcances obtenidos, la interpretación de los acuerdos, memorandos, normas, políticas y todos los aspectos formales que se asientan por escrito para el cumplimiento de las funciones y actividades en la administración cotidiana de las empresas.

Como es fácil observar, esta técnica tiene muchos alcances, y para muchos profesionales de auditoría es la forma más importante de evaluar a las empresas; además, no sólo sirve para aplicaciones en una auditoría tradicional, sino también como un importante apoyo en los diferentes tipos de auditoría de sistemas computacionales; claro está, adaptándola a las características específicas de evaluación de los sistemas computacionales.

A continuación presentamos algunos ejemplos de la aplicación de esta técnica en la auditoría de sistemas computacionales:

- *Evaluar el desarrollo de las operaciones y funcionamiento del sistema, mediante la revisión y el seguimiento de las instrucciones plasmadas en los manuales e instructivos de operación, manuales de usuarios, manuales del sistema y, en sí, de los flujogramas de actividades, procedimientos y de otros documentos que especifican la manera de operar los sistemas computacionales.*
- *Evaluar la existencia y cumplimiento de las normas, políticas, lineamientos y reglamentos de uso del área de sistemas y otros documentos que regulan los derechos y obligaciones del personal y los usuarios del sistema, a fin de valorar el desarrollo correcto de sus funciones y actividades, así como el uso adecuado de los sistemas computacionales.*
- *Revisar el uso y registro adecuados de documentos (bitácoras) para el control del software, hardware, la información de las bases de datos, el acceso del personal, de los usuarios y de todas las personas que tienen acceso al centro de cómputo, así como las funciones y actividades plasmadas en los documentos del área utilizados para la administración y control de los sistemas computacionales.*
- *Verificar la existencia y actualización de registros formales para la administración y control de operación del sistema, así como de las bitácoras de mantenimiento, la asignación de sistemas a los usuarios, el acceso a las bases de datos, la asignación de equipos, la entrega y registro de consumibles y el registro formal de otros activos de uso cotidiano en el área de sistemas, a fin de valorar su aprovechamiento.*
- *Verificar la existencia y actualización de planes, programas y presupuestos formales en el área de sistemas, así como su seguimiento, ejercicio y control, a fin de revisar su aplicación.*
- *Verificar la existencia y el uso correcto de documentos formales de apoyo para la administración y el control de activos del área de sistemas, así como la existencia y actualización de los resguardos del hardware, equipos y sistemas computacionales, la asignación del software institucional, el uso y resguardos de información, bases de datos y archivos y de todos los demás documentos que sirven de apoyo para la gestión administrativa de dicha área.*
- *Revisar los documentos de las pruebas, reportes de datos, resultados de operación, seguimiento y monitoreo de las actividades, operaciones, estadísticas de aprovechamiento y otros reportes emitidos por medio del sistema, a fin de verificar el uso correcto de los sistemas computacionales, así como revisar la captura de datos, el procesamiento de información y emisión de reportes, con el fin de evaluar el funcionamiento y aprovechamiento de los recursos informativos del área de cómputo.*

Como podemos observar, la aplicación de la técnica de revisión documental en la auditoría de sistemas también es de gran utilidad para dictaminar el desarrollo correcto de las operaciones, así como para valorar la gestión administrativa del área de sistemas, la existencia, actualización y uso de los documentos formales de administración y control de los activos informáticos del centro de cómputo y del aprovechamiento del sistema, entre muchas otras aplicaciones. Sin embargo, el auditor de sistemas computacionales que utiliza la revisión documental, además de ajustarse a las características tradicionales de revisión de los documentos formales, también debe adaptarse a las técnicas específicas de registro utilizadas en el área de sistemas, así como utilizar las computadoras para la captura, almacenamiento y acceso de datos.

Actualmente ya se acepta el almacenamiento de datos en discos flexibles, discos duros, cintas, CD-ROMs y otros dispositivos exclusivos de los sistemas computacionales para hacer la revisión documental. Incluso, las autoridades fiscales ya aceptan los registros en dispositivos de almacenamiento magnético, siempre y cuando sean registros formales de las operaciones financieras de los sistemas computacionales en donde se lleva la contabilidad. Además, con el avance del comercio electrónico, se tienen que tomar en cuenta las actividades y operaciones financieras que se realizan a través de Internet.

Para un mejor entendimiento de este tema, a continuación presentamos un cuadro concentrado de los principales tipos de documentos con los que se puede realizar la revisión documental en una auditoría de sistemas computacionales: (figura 10.1)

Al llevar a cabo la revisión documental, el auditor de sistemas debe estar abierto para analizar los distintos documentos utilizados en el área de sistemas computacionales, considerando los siguientes aspectos.

10.5.1 Que en el área haya documentos relacionados con los sistemas

En la revisión documental, el auditor de sistemas computacionales debe verificar que la empresa cuente con todos los documentos relacionados con el manejo de los sistemas computacionales, ya sean documentos de la operación del sistema, manuales de usuario, manuales técnicos, diagramas de flujo, bitácoras o cualquier documento relacionado con los sistemas; también debe verificar que la empresa cuente con los demás documentos relacionados con el aspecto administrativo del área de sistemas.

Es muy importante que el auditor compruebe que existan todos los documentos que, conforme a las necesidades de los usuarios y de los empleados del área, se requieran para el buen manejo de los sistemas computacionales; esto lo puede realizar mediante un inventario de los documentos que, según sus apreciaciones, deberían ser utilizados en el área evaluada (vea la sección 9.5.4 del capítulo anterior).

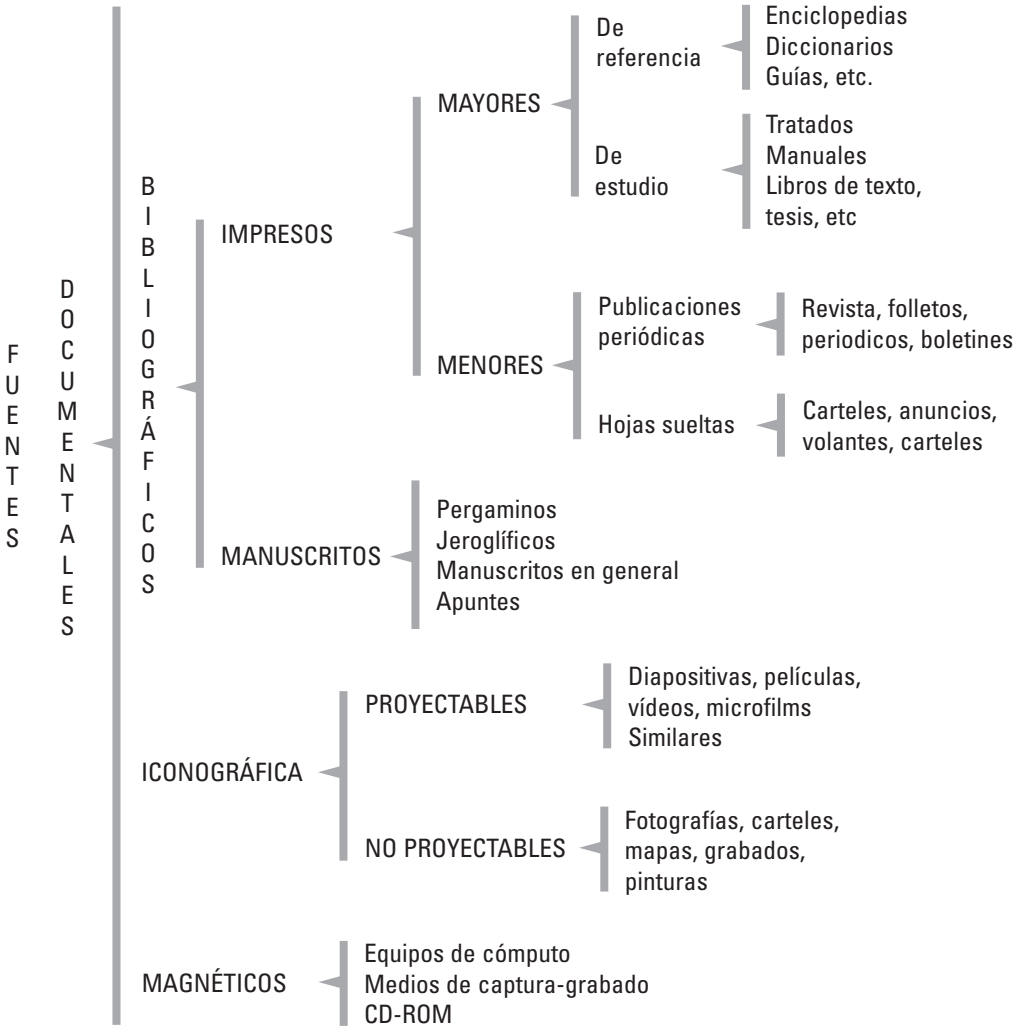


Figura 10.1 *Principales tipos de documentos para realizar la revisión documental.*

10.5.2 Que los documentos relacionados con el uso de los sistemas estén disponibles para los usuarios y empleados del área de sistemas

Es muy frecuente que las áreas de sistemas cuenten con todos los documentos relacionados con el uso de los sistemas computacionales; sin embargo, también es muy frecuente que estos documentos estén guardados y, por costumbre o política, los usua-

rios no puedan utilizarlos ni para consulta, ni para la operación de dichos sistemas. En algunos casos se impide el uso de manuales de operación de los sistemas, debido a vicios muy arraigados tales como querer conservar la exclusividad de conocimientos en el manejo de los sistemas, porque se desconoce la importancia de su difusión entre los usuarios, por una mal entendida no difusión en el manejo de estos documentos, por un supuesto mal uso de estos documentos y muchos otros vicios similares.

El auditor debe verificar que la información documental del área de sistemas esté a disposición de los empleados y usuarios; puede hacer esto a través de cuestionarios, entrevistas o cualquier otra técnica de recopilación de información. En caso de ser necesario, debe investigar los motivos para que dichos documentos no estén a disposición de los usuarios.

10.5.3 Que se difunda la existencia de los documentos relacionados con el uso de los sistemas entre los empleados y usuarios del área de sistemas

Así como se debe verificar que los documentos relacionados con el uso de los sistemas estén disponibles para el personal del área de sistemas, también se debe verificar que se difunda su existencia entre dichos empleados, ya sea cada vez que se implante un nuevo sistema computacional, cuando se actualicen los documentos de otros sistemas o como resultados de revisiones periódicas.

El auditor debe verificar que se realice la difusión de los documentos del área de sistemas computacionales; ya sea mediante avisos publicados para el personal que tiene acceso al área, listados que contengan la relación de todos los documentos del área, publicaciones en revistas y boletines internos o mediante cualquier otro método de difusión. Lo importante es que el auditor compruebe que exista esta divulgación, así como su frecuencia y resultados.

10.5.4 Que se trabaje con el apoyo de estos documentos

Además de verificar que se cumplan todos los aspectos anteriores, el auditor debe corroborar que el personal del área de sistemas, así como los usuarios de los sistemas, utilicen los manuales de operación para el desarrollo correcto de su trabajo; el auditor puede verificar esto mediante la aplicación de exámenes a los usuarios y empleados del área, mediante la observación de sus actividades o por medio de cualquier otro método que le permitan corroborar que dichos empleados están utilizando estos documentos.

Como complemento del análisis de la técnica de evaluación documental, a continuación presentamos algunos de los documentos que el auditor debe comprobar que existan y que estén disponibles para los empleados del área de sistemas computacionales:

Inventarios de documentos administrativos

- *Manuales de organización*
- *Manuales de procedimientos administrativos*
- *Manuales de perfil de puestos*
- *Otros manuales administrativos*

Inventario de documentos técnicos para el sistema

- *Manuales e instructivos técnicos del software del sistema*
- *Manuales e instructivos técnicos del hardware, periféricos y componente del sistema*
- *Manuales e instructivos de operación del sistema*
- *Manuales e instructivos para los usuarios del sistema*
- *Manuales, instructivos y procedimientos para el procesamiento de información*
- *Manuales e instructivos de mantenimiento lógico del sistema (software)*
- *Manuales e instructivos de mantenimiento físico del sistema (hardware)*
- *Manuales e instructivos didácticos de apoyo*
- *Manuales del sistema operativo utilizado por el sistema computacional*
- *Otros manuales e instructivos para el desarrollo de sistemas*

Inventarios de documentos para el desarrollo de sistemas

- *Inventario de metodologías para el desarrollo de sistemas*
- *Inventario de estándares, programación, normas y procedimientos para el desarrollo de sistemas en el área*
- *Inventario de estándares, normas y procedimientos para el diseño de las bases de datos*
- *Inventario de estándares y normas de documentación de sistemas*
- *Inventario de otros estándares, procedimientos, normas y lineamientos que regulan el desarrollo y adquisición de sistemas en el área*
- *Inventarios de documentos de apoyo para el funcionamiento de sistemas*

Es importante destacar que en el ambiente de sistemas computacionales, la revisión documental se puede hacer a través de documentos formales, en registros en sistemas computacionales o en cualquier otro medio de uso común en el área de sistemas, como discos duros, disquetes, CD-ROMs, cintas magnéticas, DVDs o cualquier otro dispositivo de captura y lectura de información.

10.6 Acta testimonial

El acta testimonial es un documento de carácter formal, que por su representatividad, importancia y posibles alcances de carácter legal y jurídico es uno de los docu-

mentos vitales para cualquier auditoría; este documento no sólo sirve de testimonio para comprobar, corroborar, ratificar o evidenciar cualquier evento que ocurra durante la revisión, sino que es tal su alcance que se puede convertir en un documento de carácter legal, probatorio de alguna anomalía de tipo jurídico, penal o de cualquier otro aspecto legal. Por esta razón es muy importante que el auditor sepa elaborarla correctamente.

La importancia de esta herramienta radica en que con su uso se pueden evidenciar pruebas fehacientes, circunstanciales, probatorias y, en algunos casos, jurídicas para comprobar desviaciones en el área auditada; incluso se pueden utilizar para comprobar manejos dolosos, desviaciones de recursos o cualquier otro tipo de indecencias que el auditor descubra durante su evaluación y que, al plasmarlas en actas testimoniales, fundamenten posibles acciones posteriores a la evaluación o durante la misma evaluación.

El acta testimonial puede, y debe, aplicarse en muchos casos de carácter jurídico y legal que inciden no sólo en una auditoría, sino en cualquier acto formal y protocolario de la administración cotidiana del área de sistemas y de cualquier otra actividad administrativa relevante de la empresa. Un acta de este tipo se utiliza en muchos de los siguientes aspectos:

- *Para la entrega de un puesto, ya que ampara la entrega-recepción de los bienes asignados tanto a quien los entrega como a quien los recibe, incluyendo las responsabilidades, funciones, compromisos, obligaciones y derechos de dicho puesto.*
- *Para testimoniar alguna falta (grave o leve) por parte del algún miembro del área de sistemas, la cual se tiene que registrar en algún documento donde consten las circunstancias del caso.*
- *Para testimoniar los robos, desapariciones, sustracciones o cualquier faltante de bienes de la empresa, de los cuales se tiene que aclarar su ausencia, las circunstancias en que ocurrió, los posibles responsables y todos los aspectos relacionados con la desaparición de algún bien en la empresa.*
- *Para deslindar o fincar responsabilidades en caso de siniestros o cualquier otra circunstancia catastrófica que repercuta en la marcha normal de la empresa o del área involucrada, ya sean accidentales, provocados, por negligencia o por cualquier otra causa.*
- *Para fincar responsabilidades por deficiencias en la actividad normal de la empresa, incumplimiento de trabajo o cualquier otro aspecto que repercuta en el desarrollo normal de las funciones encomendadas a un trabajador, un área de trabajo o toda una institución.*
- *Levantamientos de acciones jurídicas y legales que repercutan en las actividades o los bienes de la empresa, como pueden ser embargos, suspensiones de actividades, huelgas, paros laborales, quiebras o cualquier otra circunstancia que repercuta en la actividad normal del área o de la empresa.*

- *Para reportar desviaciones relevantes como resultado de la auditoría en el área de sistemas de la empresa, en los equipos o en otros aspectos reportados, las cuales, por ser relevantes, se tienen que asentar en un documento de carácter legal.*
- *Cuando se presume o se comprueba la existencia de software que no es el autorizado (software pirata), y que está siendo utilizado en los sistemas de la empresa, así como de las evidencias encontradas y las formas de obtener dicho software.*
- *Cualquier otra falta que a criterio del auditor o autoridades del área evaluada deba ser plasmada en un documento de carácter legal, sea de algún miembro del área o de los directivos e incluso del propio auditor.*

Las anteriores son sólo algunas de las muchas situaciones para poder levantar un acta testimonial en el desarrollo de una auditoría; aunque en la práctica esta acta puede ser levantada por cualquier otra incidencia de las actividades cotidianas de una empresa, de un área administrativa o de la propia área de sistemas, e incluso por incidencias de carácter laboral, despidos, renuncias y demás situaciones que están fuera de las actividades normales de una empresa.

10.6.1 Contenido del acta testimonial

En el caso de auditoría de sistemas computacionales, o de otros tipos de auditoría, no hay formatos específicos donde se indique el contenido total que debe tener un acta testimonial y la forma de elaborarla, salvo los casos en que sea una diligencia de carácter legal, en donde ya se tiene establecido un protocolo de procedimientos. Al auditor le conviene conocer el contenido mínimo que debe tener un documento de este tipo; por esta razón, a continuación analizaremos dicho contenido:

10.6.1.1 Fecha y hora de inicio del acta testimonial

Al elaborar un acta testimonial, se debe iniciar con la fecha y hora exactas en que se inicia el levantamiento de dicha acta. El formato debe ser de preferencia con número y letra conforme a los formulismos acostumbrados para estos actos. Por ejemplo:

> Siendo las 18:46 del día 9 de marzo del 2002 [...]
>
> A los 23 días del mes de julio del 2002, siendo las 19:00 horas [...]
>
> A los quince días del mes de enero del 2002, siendo las diez horas con doce minutos [...]

10.6.1.2 Lugar en donde se levanta el acta testimonial

Aquí se anota, lo más detalladamente posible, el lugar exacto en donde se lleva a cabo el levantamiento del acta testimonial; es decir, el domicilio completo (número inte-

rior, exterior, local), población, estado, país y las demás características relacionadas con la ubicación del lugar en donde se practica esta diligencia. Por ejemplo:

> [...] en el número 12,345 de la calle Insurgentes, colonia Nueva Esperanza, delegación Venustiano Carranza, México, D.F., código postal 32456 [...]
>
> [...] en el pueblo de San Jacinto, vecino de la ciudad de León, Guanajuato, en la casa marcada con el número 54,321 de la calle Rayón Mercado; entre las calles de corregidora y Mártires de la Revolución, con código postal 43212 [...]

Si es necesario, se debe anotar también el local físico donde se lleva a cabo el levantamiento del acta testimonial.

> [...] en el edificio principal, segundo piso, donde se encuentra el centro de cómputo [...]

10.6.1.3 Participantes en el levantamiento del acta testimonial

Después de anotar la fecha, hora, lugar y el local en donde se lleva a cabo el levantamiento del acta constitutiva, el siguiente paso es anotar el nombre completo, cargo o puesto, títulos y demás identificaciones de cada uno de los participantes en el evento señalado; si es necesario, también se consigna el documento con el que se identifica cada uno de los participantes.

No hay ningún orden específico para hacer la relación de participantes, ni por jerarquía, ni por representatividad, ni por orden alfabético, ni por algún otro criterio; lo único importante es que estén anotados todos y cada uno de los participantes en el levantamiento del acta. No debe haber observadores ni visitantes que participen en el levantamiento del acta sin que sean anotados. Por ejemplo:

> [...] se reunieron el M.C.E. Carlos Muñoz Razo, gerente auditor de sistemas de la empresa Auditores de Sistemas Computacionales, responsable de realizar la auditoría; el licenciado José Manuel Sáenz Pérez, director general de Practicantes, S.A., en representación de la institución auditada; el Sr. José Fidelio Sánchez Pedriza, representante sindical de la empresa, y el Sr. Juan Antonio Carranza Contreras, responsable de la operación del equipo de cómputo adscrito al área de sistemas de la empresa [...]

10.6.1.4 Descripción de los hechos

Ésta es la parte medular del acta testimonial, ya que aquí se hace la relatoría de cada uno de los eventos y acciones que dieron (o dan) motivo a la realización del acto; por esta razón, para que sea válido este documento, se debe hacer una descripción detallada, lo más descriptiva posible, de todos y cada uno de los acontecimientos que se suscitaron durante el levantamiento de este documento. Esta reseña se debe hacer con

todo lujo de detalles, anotando en orden cada participación, así como el nombre de quien habla y sus aportaciones. Asimismo, en la redacción del acta se deben anotar todos los incidentes del caso, las descripciones concretas de hechos y eventos, los acontecimientos relevantes e irrelevantes, y en sí todos los detalles que aporta cada uno de los participantes en el levantamiento del acta testimonial.

Para que esta acta sea totalmente válida, es indispensable registrar correctamente cada una de las participaciones tal y como fueron expuestas. También se deben anotar las palabras altisonantes, incongruentes, aclaraciones y demás aspectos que se presenten durante esta diligencia, sin limitar, modificar ni omitir nada de lo que se diga.

Esta parte del acta testimonial culmina cuando todos los participantes hayan hecho sus declaraciones sobre los acontecimientos que motivaron el acta; es indispensable que todos los anotados en el acta participen. Si algún integrante no participa o declina hacer declaraciones, entonces se anota su nombre y el motivo por el cual no quiso hacer declaraciones. Es indispensable anotar las declaraciones de todos los participantes en el acto. No se debe omitir uno solo, aunque no opine nada. Por ejemplo:

> [...] El M.C.E. Carlos Muñoz Razo, responsable de la auditoría de sistemas, manifiesta que encontró software de dudosa procedencia instalado en la máquina asignada al Sr. Juan Sánchez, ubicada en el área de contabilidad, de la cual la empresa tampoco tiene la licencia correspondiente ni autorización alguna para su uso. Después de realizar las aclaraciones pertinentes, y al no encontrar documentación legal ni la autorización de algún superior para instalar el software en esa máquina, se considera que dicho software es pirata. Por esta razón, se procedió a levantar la presente acta administrativa, a fin de deslindar responsabilidades sobre este acontecimiento. El Sr. Juan Sánchez declara [...]

10.6.1.5 Cierre de los testimonios

Una vez que todos los participantes en el levantamiento del acta hicieron sus declaraciones, se procede a hacer el cierre de los testimonios. Por ejemplo:

> [...] Al interrogar sobre más aportaciones y no haber más declaraciones sobre este caso, de común acuerdo con los participantes se procede al cierre de los testimonios [...]
>
> [...] Concluyendo con las declaraciones de quienes participan en el levantamiento de esta acta, y no habiendo objeción por parte de ninguno de los presentes, se procede al cierre de los testimonios.

10.6.1.6 Lectura del acta testimonial

Después de haber concluido los pasos anteriores, el encargado de levantar el acta, de viva voz, debe leer el contenido total de la misma, sin omitir nada; incluso debe leer los

errores ortográficos, deficiencias de redacción o cualquier otra incorrección. Una vez terminada la primera lectura, si es necesario se procede a una nueva lectura; tantas veces como sea necesario.

10.6.1.7 Aclaraciones y correcciones

Después de leer el acta, se procede el cierre de la misma, si es que no existe alguna aclaración sobre lo plasmado; si existen objeciones, aclaraciones y correcciones, se procede a realizar las aclaraciones y correcciones necesarias, siguiendo los mismos pasos de la descripción de hechos. Se anota el nombre de quien hace la aclaración, así como la aclaración completa y sin ninguna alteración. Si es necesario, se utilizan los mismos conceptos de los párrafos que serán modificados.

Esta parte del acta queda terminada hasta que ya no exista ninguna aclaración o corrección, y hasta que éstas hayan sido leídas. Por ejemplo:

> [...] *en la parte que dice*: "en la maquina asignada al sr. Juan Sánchez, ubicada en el área de contabilidad," *debe decir:* "en la máquina asignada al Sr. Juan Sánchez, responsable del área contable, ubicada en el área de contabilidad [...]

Para hacer las modificaciones del acta, el secretario puede tomar la opinión de cada uno de los participantes sobre los formatos y modelos que serán utilizados para anotar las aclaraciones o dudas; en el ejemplo se utilizan cursivas para indicar que se van a hacer cambios y se subraya el párrafo que se va a corregir.

10.6.1.8 Lugar, fecha y hora del cierre del acta

Después de hacer las aclaraciones pertinentes, se tiene que establecer el cierre definitivo del acta testimonial, por lo cual se procede a anotar el lugar del cierre,* así como la fecha y hora exactas en las cuales se da por terminada la diligencia.

10.6.1.9 Firma de los asistentes

Una vez concluidos los pasos señalados anteriormente, entonces se procede a obtener la firma autógrafa de todos los participantes en el levantamiento del acta; para ello se anotan, en cualquier orden, y al calce del documento,el nombre, título, puesto y cargo de cada uno de los asistentes a la diligencia.

* No es frecuente pero suele suceder que, por necesidades de los actos y debido a lo consignado en el acta testimonial, los participantes tengan que desplazarse del lugar en donde se inició el acta a otros sitios; por eso es indispensable registrar en el acta el cambio a nuevos lugares, los motivos de dicho cambio y el lugar donde culminó el levantamiento de la misma. Se puede cambiar el lugar donde se levanta el acta tantas veces como sea necesario, a condición de que cada uno de esos nuevos lugares, las causas de los cambios, los acuerdos y argumentos para tomar la decisión, así como las objeciones, sean anotados en el acta.

Después, cada uno de los participantes tiene que firmar no sólo al calce del documento sino en los costados de cada una de las hojas y copias utilizadas en el acta.

En caso de que, por cualquier motivo, alguno de los presentes se negara a firmar estos documentos, se anota el hecho al final del acta, estableciendo los motivos de la negativa. Es necesario que algunos de los presentes firmen como testigos de la negativa.

El contenido puede variar dependiendo de las partes en que se divida el acta testimonial, pero los puntos mencionados anteriormente son el contenido mínimo que debe tener este documento para que sea válido como acta testimonial. Es recomendable elaborar este documento con la asesoría de un abogado, con el fin de que su contenido y redacción sean los correctos.*

10.6.2 Requisitos para elaborar el acta testimonial

Así como fue necesario señalar el contenido mínimo que debe tener una acta testimonial, también es necesario indicar los requisitos que se deben cumplir para elaborarla, la mayoría de tipo legal, a fin de que lo que se asiente en dicho documento sea totalmente válido.

Para esto, sólo indicaremos los procedimientos mínimos que, de acuerdo con la experiencia de este autor, se tienen que utilizar para no invalidar este documento. Es recomendable que un abogado esté presente para determinar estos requerimientos con exactitud.

10.6.2.1 Procedimiento para convocar a la elaboración del acta testimonial

El primer requisito para elaborar este documento es hacer, de preferencia por escrito y a cada uno de los participantes, la convocatoria para este acto protocolario, ya sea mediante citatorios, memoranda o cualquier otro medio.

Este requisito es fundamental para evitar problemas posteriores que puedan invalidar la legitimidad de este documento, y el responsable de la auditoría debe elegir el método para convocar a los participantes, de acuerdo con su criterio. Lo único no válido es que sea de carácter coercitivo ni por cualquier otro medio ilegal.

En una auditoría de sistemas computacionales no es difícil hacer esta convocatoria, ya que es una práctica común para recabar información útil para la evaluación; a menos que se trate de supuestos delitos, en cuyo caso el levantamiento del acta tomará otro curso legal, para lo cual es recomendable asesorarse de abogados para proceder conforme al derecho vigente.

* El concepto actual de auditoría es de carácter interdisciplinario, por eso se puede contar con un abogado que realice este tipo de documentos, lo cual no sólo es válido sino lo más recomendable. Recordemos, estimado lector, que la auditoría debe ser realizada por un grupo interdisciplinario de profesionales.

10.6.2.2 Determinar a los responsables de elaborar el acta

También es requisito obligatorio elegir a los responsables de conducir el levantamiento del acta testimonial, ya sea por votación o por jerarquía; también se puede elegir a alguien que pueda asentar los datos en forma mecanografiada. Concretamente se requiere de los siguientes puestos:

Responsable de la conducción

Será el encargado de conducir el levantamiento del acta con la suficiente autoridad para vigilar que se realice en forma correcta; además, será el responsable de revisar la redacción del acta, dictar los acuerdos y establecer el orden de participación y limitar las intervenciones. Es preferible que algún miembro con jerarquía en la empresa presida este acto, a fin de imponer la autoridad requerida para mantener el orden en las intervenciones. Todo de común acuerdo con los integrantes del acto.

Secretario

Esta persona será la encargada de mecanografiar todas las partes de que conste el acta y las participaciones de cada uno de los miembros que participen en el acto. Es preferible que sea alguien familiarizado con la mecanografía, ya que es casi indispensable que el documento sea elaborado a máquina. También se puede elaborar en forma manuscrita, pero sería sólo como una excepción y bajo circunstancias muy especiales.

Vocal

Aunque no es indispensable, sí es recomendable que al menos dos personas de las que participen en el acto funjan como vocales, a fin de que asesoren sobre aspectos específicos que se presenten durante el desarrollo de este acto, o para dar fe de posibles acuerdos entre el grupo.

10.6.2.3 Determinar el formato del acta testimonial

Otro de los requisitos fundamentales es que los participantes del acto acuerden el formato que será utilizado para la elaboración del acta testimonial; esto se puede convenir previamente, sin ningún tipo de limitación, salvo el contenido mínimo del documento y la forma de regular las intervenciones, los acuerdos y todos los demás detalles del caso.

10.6.2.4 Completar todos los renglones

Para que el acta sea válida, es un requisito obligatorio, incluso muy conveniente, que todos los renglones que contengan información estén complementados con algún carácter similar después del punto. Esto se hace cuando el renglón no ha sido llenado completamente, y tiene el mero propósito de evitar que se agregue algún otro comen-

tario después del punto. Es recomendable que el renglón sea llenado con guiones (- - - -) o con equis minúsculas (xxxxx) o mayúsculas (XXXXX) o con cualquier otro carácter, siempre y cuando sea el mismo en toda el acta.

Además, es indispensable que todo el documento sea redactado a renglón seguido, así como agregar caracteres suficientes, los mismos que se utilizan para completar los renglones, para indicar que es el final del documento.

> [...] El M.C.E. Carlos Muñoz Razo, responsable de la auditoría de sistemas, manifiesta que encontró software de dudosa procedencia instalado en la máquina asignada al Sr. Juan Sánchez, ubicada en el área de contabilidad, de la cual la empresa tampoco tiene la licencia correspondiente. ——————————
>
> Después de realizar las aclaraciones pertinentes y al no encontrar documentación legal ni la autorización de algún superior para instalar el software en esa máquina, se considera que dicho software es pirata. Por esta razón, se procedió a levantar la presente acta administrativa, a fin de deslindar responsabilidades sobre este acontecimiento. XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

10.6.3 Tipos de actas testimoniales para una auditoría de sistemas computacionales

Existen muchos documentos que pueden ser clasificados como actas testimoniales; para ejemplificar esto, a continuación presentaremos algunos de estos documentos, con un breve comentario de su contenido, importancia y utilidad, a fin de que el lector pueda elegir la más adecuada para el trabajo que esté realizando:

10.6.3.1 Acta de entrega-recepción de puesto

Esta acta se elabora con la finalidad de hacer la entrega de un puesto por quien lo transfiere a un nuevo titular o a alguien temporal. Dicha entrega incluye todos los activos del puesto, así como las funciones y actividades que se estén realizado, los proyectos, responsabilidades y todos los aspectos inherentes al desempeño de la funciones de quien antes las tenía y del que ahora ocupa el puesto.

Por regla general, esta entrega-recepción se hace con la participación de quien lo entrega y de quien lo recibe y, preferiblemente, con la asistencia de un auditor o de algún funcionario de la empresa para avalar dicha entrega.

10.6.3.2 Acta de carácter disciplinario

Este documento se elabora para asentar por escrito alguna desviación, incidencia o medida disciplinaria que repercuta en el desarrollo normal de las funciones y actividades de un puesto. Por lo general se realiza en el ámbito operativo, contando con la participación del responsable del área donde se presenta la incidencia, el(los) empleado(s) in-

volucrado(s), su representante sindical, si es necesario, y de algún representante del área de personal. El auditor también puede participar para avalar el acto.

10.6.3.3 Acta por incumplimiento de actividades

Aunque es muy similar a la anterior, debido a que puede ser producto de alguna incidencia disciplinaria, es preferible levantar esta acta testimonial por incumplimiento, ya que puede llegar a consecuencias que repercutan en la operación normal de la empresa y en sus activos; por eso es recomendable asentar el hecho lo más claramente posible y con lujo de detalles.

Además, con el levantamiento de esta acta se pueden deslindar responsabilidades y, en su caso, fincarlas hacia alguien en especial.

10.6.3.4 Acta de liberación de sistemas

En la operación cotidiana de sistemas computacionales, la entrega y liberación de un sistema se realiza mediante algún documento de carácter oficial, mismo que se elabora con la participación del representante del área de sistemas que lo entrega y el representante del área que lo recibe; sin embargo, lo más aconsejable es que esta entrega y liberación del sistema se haga por medio de algún acta testimonial, con todos los requisitos indicados anteriormente, a fin de que sea más formal.

10.6.3.5 Acta por faltantes de activos

Cuando se sospecha o se sabe de algún faltante en los activos de la empresa, es indispensable levantar un acta testimonial, con el propósito de testificar la desaparición del bien, deslindar y fincar responsabilidades y dejar la constancia del hecho para que sea investigado posteriormente. En el levantamiento de esta acta participan el responsable del bien, quien tiene el resguardo del mismo, el responsable del área, los testigos, si es que los hay, y alguna persona que dé fe del faltante, que puede ser el auditor o algún funcionario de la empresa. Si existiera la sospecha sobre alguien en especial, esa persona también tiene que participar en el evento; aunque no es muy fácil lograr esto.

En el caso concreto de la auditoría de sistemas computacionales, cuando el auditor sospecha que falta algún activo, o sabe que éste es sustraído, debe proceder a levantar el acta testimonial del caso después de realizar las averiguaciones correspondientes. El propósito es protocolizar y asentar el hecho detectado e iniciar las diligencias correspondientes. Además, le servirán de sustento para su informe de auditoría.

10.6.3.6 Acta por existencia de software pirata en la empresa

Cuando el auditor encuentra o sospecha de la existencia de software no autorizado o del cual, aparentemente, hacen falta las licencias correspondientes, es su deber levan-

tar el acta testimonial correspondiente, a fin de establecer las causas de ese ilícito y, en su caso, proceder a deslindar responsabilidades.

En este acto deben participar el propio auditor, el responsable del sistema en donde se localizó dicho software y el responsable del área, con el propósito de efectuar, la testificación que el caso requiera.

El responsable del área puede realizar esta misma acción cuando detecte la existencia de software pirata.

10.6.3.7 Acta de alteración de programas e instrucciones del sistema

Si el auditor observa desviaciones, alteraciones o modificaciones no autorizadas en las instrucciones, lenguajes, códigos, bases de datos y/o rutinas de programación de algún software institucional, independientemente de la repercusión que tenga para el propio sistema, es indispensable que levante el acta testimonial correspondiente, con el propósito de establecer las causas, reales y aparentes, las repercusiones y posibles alteraciones que sufran los sistemas, o para asentar las justificaciones de quien hizo las modificaciones y la respectiva autorización.

En este acto deben participar el propio auditor, el responsable del sistema en donde se localizaron las modificaciones del software, el programador y el responsable del área, con el propósito de efectuar la testificación que el caso requiere.

Esta misma acta se puede levantar cuando se detecten desviaciones en el manejo de la información utilizada en el sistema computacional.

10.6.3.8 Acta por resultados de siniestros y catástrofes

Cuando ha ocurrido un siniestro que repercute en el funcionamiento de los sistemas, independientemente de su magnitud, por rutina se debe levantar el acta testimonial correspondiente, ya que se deben asentar las repercusiones que sufrieron los sistemas por este percance; más aún cuando se trata de las bases de datos que pudieron verse afectadas por el siniestro. También se debe incluir en el acta la reanudación de las actividades normales y las modificaciones y correcciones realizadas para subsanar las posibles repercusiones.

En este acto es indispensable la participación del auditor, ya que debe asentar, con lujo de detalles, todas las incidencias del caso y las repercusiones que hayan sufrido los sistemas, así como la reanudación de las operaciones normales del sistema.

10.6.3.9 Acta administrativa por deficiencias en el trabajo

Es poco frecuente, pero llegan a darse casos en los que se tienen que levantar actas testimoniales por deficiencias en el desarrollo del trabajo normal de un empleado o, incluso, de toda un área de trabajo; entonces, para asentar esto, el auditor debe levantar el acta correspondiente, describiendo detalladamente las situaciones que se pre-

sentan para fundamentar la deficiencia del trabajo, ya sean por negligencia, descuido, accidente, dolo, mala fe o por cualquier otra deficiencia de parte de quienes realizan el trabajo.

En este documento se debe señalar, si es posible, en qué consiste esa deficiencia, las pruebas, si es que las hay, y las repercusiones que esto trae consigo, con todos los detalles que sean necesarios para evidenciar los acontecimientos.

Evidentemente, el auditor tiene que participar en el acto, así como el responsable del área y el o los trabajadores involucrados y, si es necesario, los representantes del sindicato y de la empresa.

10.6.3.10 Acta administrativa por acumulación de faltas

Aunque esta acta testimonial es un documento elaborado casi exclusivamente en el área de recursos humanos de las empresas, también se puede dar el caso que se tenga que elaborar en el área de sistemas por el número de faltas injustificadas que acumula un trabajador durante 30 días hábiles.

El levantamiento de esta acta consiste en testimoniar la acumulación de faltas no justificadas de un trabajador, con objeto de establecer alguna sanción de acuerdo con la Ley Federal del Trabajo.[17] En estos casos deberán estar presentes el auditor, el representante sindical de la empresa, el responsable de recursos humanos y el propio trabajador.

Debido a lo serio de las sanciones a las que se puede hacer acreedor el trabajador, es necesario asentar las causas de las faltas conforme a lo señalado en la Ley Federal del Trabajo.

10.7 Matriz de evaluación

La matriz de evaluación es uno de los documentos de recopilación más versátiles y de mayor utilidad para el auditor de sistemas computacionales, debido a que por medio de este documento es posible recopilar una gran cantidad de información relacionada con la actividad, operación o función que se realiza en estas áreas informáticas, así como apreciar anticipadamente el cumplimiento de dichas actividades.

Esta herramienta consiste en una matriz de seis columnas, de las cuales la primera corresponde a la descripción del aspecto que será evaluado y las otras cinco a un criterio de calificación descendente (o ascendente), en las que se anotan los criterios de evaluación para accesar a esa calificación, conforme se indica en el inciso siguiente.

10.7.1 Sección de evaluación del servicio a los usuarios

Descripción de los conceptos que serán evaluados	***Calificación***				
	10 Excelente	**9 Bueno**	**8 Suficiente**	**7 Regular**	**6 Deficiente**
Calidad en el otorgamiento del servicio de cómputo al usuario solicitante.	Atiende de inmediato y soluciona satisfactoriamente las necesidades de cómputo del usuario.	Atiende satisfactoriamente las necesidades de cómputo del usuario, aunque con cierto retraso en la solución.	Atiende las necesidades de cómputo del usuario, aunque sus soluciones no siempre son satisfactorias.	Atiende parcialmente las necesidades de cómputo del usuario, aunque con deficiencias en sus soluciones.	Atiende deficientemente las necesidades de cómputo del usuario, con frecuentes deficiencias en sus soluciones.

Explicación de la matriz de evaluación

- En la primera columna se describe, lo más explícitamente posible, el concepto que será evaluado, detallándolo de tal manera que no haya ninguna duda sobre lo que se va a calificar.
- En la siguiente columna (**10 Excelente**) se describe el criterio por el cual el concepto es calificado con la más alta puntuación. *Aquí se anota la más alta calificación por el cumplimiento excepcional del concepto evaluado*.
- En la siguiente columna (**9 Bueno**) se describe el criterio por el cual el concepto es calificado como bueno. *Aquí el cumplimiento es bueno, pero en menor escala que en la columna anterior.*
- En la siguiente columna (**8 Suficiente**) se describe el criterio por el cual el concepto apenas alcanza la calificación mínima necesaria. *Aquí el cumplimiento del concepto apenas llega al mínimo necesario para satisfacer lo que se califica.*
- En la siguiente columna (**7 Regular**) se describe el criterio por el cual el concepto es calificado como mediano o regular. *Aquí el cumplimiento del punto evaluado es francamente regular o mediocre.*

- En la última columna (**6 Deficiente**) se describe el criterio por el cual el concepto es calificado como insuficiente o pésimo. *Aquí el cumplimiento del punto evaluado es francamente pésimo, más que mediocre o simplemente no se cumple.*

Esta matriz de evaluación es un documento muy útil para el auditor de sistemas, debido a que le permite realizar cualquier tipo de valoración acerca del cumplimiento de una función específica de la administración del centro de cómputo, ya sea en la verificación de una serie de actividades de cualquier función del área de sistemas, del sistema computacional, del desarrollo de proyectos informáticos, del servicio a los usuarios del sistema o de muchas otras actividades exclusivas del área de sistemas de la empresa; además tiene la gran ventaja de poder valorar dicho cumplimiento con varios criterios que van desde lo excelente hasta lo pésimo.

A continuación presentamos los siguientes criterios para la elaboración de parámetros de evaluación en este tipo de matriz:

- **Excelente.** *Es cuando se califica con un 10, el 100% o la cifra considerada como el máximo posible que se pueda alcanzar.* Esta calificación se utiliza cuando el desarrollo del trabajo, el cumplimiento de las funciones, el servicio o cualquier otro aspecto se cumplen con la mayor calidad y excelencia posibles.
- **Bueno.** *En este punto se califica con un 9, el 90% o la cifra considerada como la siguiente en la escala.* Esta calificación se utiliza cuando el desarrollo del trabajo es altamente satisfactorio, pero existen algunos aspectos menores que impiden su total cumplimiento, ya sea de funciones, al otorgar el servicio o en cualquier otro aspecto.
- **Suficiente.** *En este punto se califica con un 8, el 80% o la cifra considerada como la escala normal o la equivalente a ésta.* Esta calificación se utiliza cuando el cumplimiento en el desarrollo del trabajo es satisfactorio, pero se considera como el mínimo necesario para ejecutar lo encomendado. Aquí se admiten algunos aspectos menores que impiden el cumplimiento total, ya sea de funciones, al otorgar el servicio o en cualquier otro aspecto de la actividad normal.
- **Regular.** *En este punto se califica con un 7, el 70% o la cifra considerada como la mínima aceptable.* Esta calificación se utiliza cuando el desarrollo del trabajo es francamente deficiente. Es decir, cuando el desarrollo del trabajo no es nada satisfactorio, pero se evalúa como el mínimo necesario para realizar la tarea encomendada. Aquí se cumple parcialmente con el trabajo, pero dentro de un rango

muy por debajo de lo normal; apenas lo suficiente para efectuar lo encomendado, ya sean funciones, otorgamiento del servicio o cualquier otro aspecto.

- **Deficiente.** *En este punto se califica con un 6, el 60% o la cifra considerada como la escala menor de lo aceptable.* Esta calificación se utiliza cuando el desarrollo del trabajo es francamente deficiente y queda dentro de un rango muy por debajo de lo mínimo aceptable para realizar la tarea encomendada. Aquí se califican todos aquellos aspectos de incumplimiento que no satisfacen en lo más mínimo lo evaluado.

Esta matriz tiene rangos en escala descendente, de **10** (*excelente*) hacia **6** (*deficiente*), pero la escala se puede cambiar a otro tipo de valores, desde **10** hasta **5** o desde **5** hasta **0**, con la condición de que estos valores sean considerados de mayor a menor y dentro de los parámetros establecidos para calificar. También se puede utilizar escala alfabética (A, B, C, D, E) y alfanumérica (A5, A4, A3, A2, A1), o cualquier otro tipo de escala que sea descendente, según las preferencias del auditor.

Es conveniente señalar que para diseñar correctamente este tipo de matriz se debe determinar, lo más detallada y claramente posible, el contenido de cada uno de los aspectos que serán evaluados, así como su calificación, a fin de que no exista ninguna posibilidad de desviación; estas calificaciones se establecen en una escala que va desde el máximo rango posible (*excelente*) hasta el mínimo rango (*deficiente o insuficiente*).

10.7.2 Ejemplo de matriz de evaluación para calificar el desarrollo de proyectos informáticos

Tomando en cuenta las fases de la metodología general para el desarrollo de proyectos informáticos, esta matriz de ejemplo constará de las siguientes etapas:

- *Análisis del sistema actual*
- *Diseño del sistema*
- *Programación*
- *Pruebas*
- *Implantación*
- *Liberación y mantenimiento*

A continuación presentamos esta matriz de evaluación, considerando los conceptos que serán evaluados, así como los criterios para calificarlos en un rango de 10 a 6.

Descripción de los conceptos que serán evaluados	***Calificación***				
	10 Excelente	**9 Bueno**	**8 Suficiente**	**7 Regular**	**6 Deficiente**
Calidad en el análisis del sistema actual, para saber las necesidades, opiniones y sugerencias de los usuarios, a fin de satisfacer lo que necesitan del sistema.	El analista investigó a fondo, diligentemente y con excelente disposición las necesidades de los usuarios, a fin de captar todo lo que necesitan del sistema.	El analista investigó a fondo, diligentemente y con buena disposición las necesidades de los usuarios, a fin de captar todo lo que necesitan del sistema.	El analista investigó con la suficiente profundidad, diligencia y disposición las necesidades de los usuarios, a fin de captar lo que necesitan del sistema.	El analista investigó con regular profundidad, diligencia y disposición las necesidades de los usuarios, a fin de captar lo que necesitan del sistema.	El analista investigó sin la más mínima profundidad, diligencia ni disposición las necesidades de los usuarios, por lo cual desconoce lo que necesitan del sistema.
Grado de excelencia en el uso de las herramientas para la recopilación de información, conforme a los estándares de análisis de la empresa, para conocer las necesidades de los usuarios.	Excelente planeación, diseño y aplicación de los instrumentos de recopilación de información, con lo cual obtuvo magnífica información acerca de las necesidades de los usuarios.	Buena planeación, diseño y aplicación de los instrumentos de recopilación de información, con lo cual obtuvo buena información acerca de las necesidades de los usuarios.	Suficiente planeación, diseño y aplicación de los instrumentos de recopilación de información, con lo cual obtuvo información aceptable acerca de las necesidades de los usuarios.	Regular planeación, diseño y aplicación de los instrumentos de recopilación de información, con lo cual obtuvo información mínima aceptable acerca de las necesidades de los usuarios.	Deficiente planeación, diseño y aplicación de los instrumentos de recopilación de información, con lo cual obtuvo pésima información acerca de las necesidades de los usuarios.

Grado de aceptación en el análisis y diseño de nuevos sistemas que satisfagan las necesidades de cómputo de los usuarios.	Gran profundidad en el análisis, y total comprensión de los requerimientos de cómputo de los usuarios.	Buena captación en el análisis, y adecuada comprensión de los requerimientos de cómputo de los usuarios.	Suficiente identificación en el análisis, y comprensión de los requerimientos de cómputo de los usuarios.	Mínima identificación en el análisis, y poca comprensión de los requerimientos de cómputo de los usuarios.	Absoluta ausencia de identificación en el análisis, y nula comprensión de los requerimientos de cómputo de los usuarios.
Grado de excelencia en el diseño de nuevos sistemas para satisfacer las necesidades del usuario.	El diseño de los nuevos sistemas computacionales es de gran calidad, y satisface plenamente las necesidades del usuario.	El diseño de los nuevos sistemas computacionales es bueno, y satisface en buena medida las necesidades del usuario.	El diseño de los nuevos sistemas computacionales es suficientemente bueno para satisfacer las necesidades del usuario.	El diseño de los nuevos sistemas computacionales es de una calidad mínima aceptable, y apenas satisface las necesidades del usuario.	El analista no diseñó ningún sistema nuevo, o hizo propuestas deficientes, por lo cual no satisface las necesidades del usuario.
Evaluación del grado de uso de los códigos y estándares de programación establecidos en la empresa.	Utiliza con gran eficiencia los códigos, estándares y utilerías de Visual Basic, para diseñar los programas que satisfacen plena-	Utiliza los códigos, estándares y utilerías de Visual , Basic para diseñar los programas de acuerdo con los requerimientos del usuario.	Se apega a los códigos, estándares y utilerías de Visual Basic, para diseñar los programas del usuario.	Se apega a los códigos, estándares y utilerías de Visual Basic en forma mínima; con ello sólo diseña un programa que sa-	Nunca se apega a los códigos, estándares y utilerías de Visual Basic, o lo hace muy poco; con ello diseña programas que no sa-

	mente los requerimientos del usuario.			tisface mínimamente los requerimientos del usuario.	tisfacen las necesidades del usuario.
Grado de eficiencia en la aplicación, comportamiento y evaluación de las pruebas de los nuevos sistemas computacionales, y evaluación de los resultados y la eficiencia en la corrección de los programas con datos reales.	Aplica con gran eficiencia y exactitud las pruebas necesarias para medir el comportamiento del nuevo sistema, y con los resultados corrige eficientemente sus programas.	Aplica con eficiencia y exactitud las pruebas necesarias para medir el comportamiento del nuevo sistema, y con los resultados corrige los programas.	Sólo aplica las pruebas necesarias para medir el comportamiento del nuevo sistema, y con los resultados corrige los programas.	Sólo utiliza algunas pruebas mínimas para medir el comportamiento del nuevo sistema, y con los resultados corrige parcialmente los programas.	Jamás realiza pruebas para medir el comportamiento del nuevo sistema, y no obtiene resultados para corregir los programas.
Grado de documentación de los programas establecidos en la empresa	Siempre elabora todos los manuales e instructivos del nuevo sistema, sean del usuario, técnicos, de mantenimiento o todos los demás documentos requeridos.	Elabora la mayoría de los manuales e instructivos del nuevo sistema, los más utilizados por los usuarios y técnicos, los de mantenimiento y algunos otros documentos requeridos.	Elabora algunos de los manuales e instructivos que necesitan los usuarios y técnicos del nuevo sistema.	Sólo elabora la cantidad mínima de manuales e instructivos que necesita el usuario del nuevo sistema.	Jamás elabora los manuales e instructivos que necesita el usuario del nuevo sistema

Grado en que la elección del método de implantación satisface las expectativas de funcionamiento del sistema.	Siempre analiza la conveniencia del mejor método de implantación del sistema, de acuerdo con las características y necesidades de la empresa.	Analiza la conveniencia del método de implantación del sistema, de acuerdo con las características y necesidades de la empresa.	Utiliza un método de implantación del sistema, suponiendo las características y necesidades de la empresa.	Elige un método de implantación del sistema que apenas satisface las necesidades de la empresa.	Elige un método de implantación del sistema que no es acorde a las características y necesidades de la empresa.
Evaluación del grado de aceptación del nuevo sistema por parte de los usuarios.	Obtiene la plena y absoluta aceptación del usuario del nuevo sistema.	Obtiene buena aceptación del usuario del nuevo sistema.	Apenas obtiene aceptación del usuario del nuevo sistema.	Aceptación mínima del usuario del nuevo sistema.	No tiene ninguna aceptación del usuario del nuevo sistema.
Evaluación de la periodicidad de mantenimiento del sistema.	Da un excelente mantenimiento al nuevo, sistema con apego irrestricto al programa preventivo y correctivo.	Da buen mantenimiento al nuevo sistema, conforme al programa preventivo y correctivo requerido.	Da mantenimiento al nuevo sistema siguiendo el programa preventivo y correctivo requerido.	Da poco mantenimiento al nuevo sistema y sigue muy poco el programa preventivo, por lo cual utiliza de más el correctivo.	Da poco mantenimiento al nuevo sistema y no utiliza ningún programa preventivo, y sólo utiliza ocasionalmente el correctivo.

En el ejemplo anterior mostramos la manera de elaborar la matriz de evaluación, los criterios para elaborar los conceptos que van a ser evaluados, así como los criterios para calificar cada concepto.

10.8 Matriz DOFA

Éste es un método moderno de análisis y diagnóstico administrativo de gran utilidad para la evaluación de un centro de cómputo, debido a que no sólo permite recopilar información más versátil, sino que admite evaluar el desempeño de los sistemas computacionales; asimismo, por medio de este documento se puede tener una apreciación preliminar sobre las *fortalezas y debilidades* del propio centro de información de la empresa, y se pueden analizar sus posibles *amenazas y áreas de oportunidad;* con dicho análisis, el auditor evalúa el cumplimiento de la misión y objetivo general del área de sistemas computacionales de la empresa.

La matriz DOFA[18] es un acrónimo de Debilidades, Oportunidades, Fortalezas y Amenazas de la empresa, las cuales se estudian cada una por separado en cuanto a su presencia interna y a la influencia que la empresa recibe del exterior, y conforme a los siguientes criterios:

10.8.1 Explicación de la matriz DOFA

Mediante esta matriz de Debilidades, Oportunidades, Fortalezas y Amenazas se estudian las influencias que afectan el comportamiento de una empresa; tanto de las que recibe de su ambiente interno, como del ambiente externo. Concretamente, por medio de la aplicación de esta matriz se pueden realizar el *análisis y diagnóstico* de todas las Fortalezas y Debilidades internas de una empresa, así como el *análisis y diagnóstico* de todos los factores externos que rodean a la empresa y que pueden convertirse en áreas de Oportunidad y Amenazas e influir en su comportamiento.

La conceptualización de esta matriz es que permite analizar todos los factores que intervienen en el desarrollo de las actividades de una empresa, ubicándonos en planos específicos que, de alguna manera, influyen en su entorno. Para cada uno de esos factores tenemos que considerar los siguientes aspectos:

Los factores de carácter interno

- *Misión, visión y objetivo*
- *Factor humano*
- *Cultura empresarial*
- *Bienes y servicios*
- *Estrategias*
- *Estructura de organización*
- *Idiosincrasia, valores y costumbres*
- *Filosofía de calidad*
- *Finanzas y economía*

Los factores de carácter externo

- *Clientes*
- *Canales de distribución*
- *Proveedores*
- *Competencia*
- *Tecnología*
- *Influencia social*
- *Influencia política*
- *Influencia económica*
- *Influencia cultural*

Repercusión externa dentro del ámbito de influencia

- *Ambiente local*
- *Ambiente regional*
- *Ambiente nacional*
- *Ambiente internacional*

Con el estudio de los factores anteriores, un auditor de sistemas, o de cualquier disciplina, puede realizar el análisis de las fortalezas y debilidades que afectan internamente a la empresa, así como el análisis de las influencias externas que se pueden convertir en áreas de oportunidad y amenazas para ésta, con el fin de realizar el diagnóstico de los siguientes factores de la empresa:

Diagnóstico y repercusión de sus factores internos:

- *Los puntos fuertes para fortalecerlos aún más.*
- *Los puntos débiles para reducir su debilidad y convertirlos en fortalezas de la empresa.*

Diagnóstico y repercusión de sus factores externos:

- *Las áreas de oportunidad para ampliarlas y fortalecerlas.*
- *Las amenazas para reducirlas o proteger a la empresa de sus influencias.*

Todos estos factores se estudian desde el punto de vista de la *misión, visión y objetivo general* que determinan el camino que la empresa debe seguir, y de acuerdo con la *cultura empresarial, estrategias* y al *factor humano* de que ésta dispone para ofrecer sus *bienes y servicios* al mercado; asimismo, todos estos factores se enmarcan en una *estructura de organización* acorde con las necesidades y características de la empresa, y de acuerdo con la *idiosincrasia, valores y costumbres* de funcionarios, empleados, proveedores y clientes que repercuten, directa o indirectamente, en las actividades de la institución; sin perder de vista la *filosofía de calidad* que se ofrece en los *bienes y servicios*, y el entorno *financiero y económico* que es la razón de existir de la empresa.

10.8.1.1 Los factores de carácter interno

Estos factores que afectan el comportamiento de la empresa se deben estudiar desde orientaciones muy específicas, las cuales serán determinadas directamente por el tipo de empresa y por la influencia que ésta reciba de los factores externos de carácter local, regional, nacional e incluso internacional que hacen necesario un análisis y diagnóstico muy particulares para cada empresa; sin embargo, para la explicación del comportamiento de esta matriz, podemos establecer los siguientes factores generales que repercuten en el comportamiento interno de una empresa:

Misión, visión y objetivo

Es el estudio de los elementos fundamentales que son la razón de existir de la empresa:

- ***La misión:*** *Es la facultad, comisión o tarea encomendada a un grupo de personas para desempeñar lo que es la razón de ser de una empresa y establecer el porqué de su existencia, hacia qué rumbo debe seguir para alcanzar sus metas.*

- ***La visión:*** *Es la forma en que se ve la empresa a sí misma, desde el punto de vista particular del propósito que tiene como agrupación de funcionarios y empleados.*
- ***El objetivo general:*** *Es el planteamiento pleno del fin que la empresa pretende alcanzar; dicho objetivo se establece generalmente a largo plazo y de manera global, para que todos los integrantes de la empresa se apeguen a él.*

Estas partes no pueden presentarse por separado, sino que se conjuntan entre sí para determinar el rumbo que debe seguir la empresa.

Factor humano

Es el recurso más importante de cualquier empresa, debido a que este factor es el que establece, diseña, realiza y supervisa —de acuerdo con los niveles de jerarquía— el cumplimiento de todas las funciones, actividades y operaciones que requiere la empresa para satisfacer su objetivo, cumplir su misión y alcanzar su visión de sí misma. Es decir, el factor humano le da origen y vida a la empresa, determinando y realizando lo que se pretende alcanzar.

Cultura empresarial

La cultura es el cúmulo de conocimientos de una persona, comunidad, sociedad o país, que conduce a un sistema de creencias, valores, tradiciones y modos de comportamiento del propio individuo y del conjunto de ellos. Para el caso que nos ocupa, definiremos la cultura empresarial de la siguiente manera:

> *Es el conjunto de conocimientos que aporta cada una de las personas que conforman una empresa, a través del cual contribuye al fortalecimiento del sistema de creencias, valores, tradiciones y modos de comportamiento de todo el grupo.*

Bienes y servicios

Es lo que aporta la empresa a la sociedad para satisfacer las necesidades de las personas e instituciones (clientes); esta aportación se ofrece en forma de bienes y servicios por separado, o de bienes y servicios juntos.

Estrategias

Es el plan global, generalmente a largo plazo, mediante el cual se coordinan todas las actividades de la empresa para cumplir con éxito la misión, visión y objetivos de la misma. Esto se realiza a través de la acción coordinada del factor humano y los recursos de la empresa.

Estructura de organización

Es la conformación de la estructura de puestos, jerarquías, niveles de autoridad, funciones y relaciones formales de comunicación y descripción de puestos que se adop-

tan en una empresa, con el propósito de realizar todas las funciones, actividades y operaciones requeridas para cumplir con la misión, visión, objetivos y estrategias que son el propósito fundamental de la empresa, es decir, proporcionar a la sociedad los bienes o servicios que produce.

Idiosincrasia, valores y costumbres

En conjunto, estos aspectos son la mística de actuación de cada uno de los integrantes de la empresa, quienes los aportan de manera individual y se aceptan como la forma de actuar de todos.

- **La idiosincrasia:** *Es la forma de ser, el temperamento y la cultura específica que caracterizan a una persona, institución, sociedad o país, y que determinan su forma de actuar dentro de un contexto social.*
- **Los valores:** *Son las cualidades de orden material que determinan los bienes de la cultura y los bienes vitales o espirituales del individuo.*[19]
- **Las costumbres:** *Es el conjunto de cualidades, usos, prácticas y maneras habituales de proceder que definen el carácter de una persona, una institución, una sociedad o una nación.*

En conjunto, estos aspectos son los que determinan las peculiaridades y características de comportamiento de la empresa y de los individuos que la conforman.

Filosofía de calidad

Es la forma de conceptualizar la calidad, propiedades y cualidades que se les atribuyen a los bienes y/o servicios que se ofrecen a los individuos y la sociedad, sean clientes, empresas o proveedores. Incluso podemos interpretar la filosofía de calidad como las cualidades y propiedades que sobresalen de entre los bienes, servicios, actividades, operaciones y funciones que se realizan en la misma empresa.

Finanzas y economía

Es el aspecto con el cual se cuantifican los esfuerzos de la empresa para obtener utilidades dentro de un marco económico; este aspecto estará determinado por todas las acciones realizadas para la obtención de dividendos y por las unidades de inversión que aporta la empresa.

Con el estudio de cada uno de los anteriores factores de carácter interno, el auditor de sistemas computacionales (o de cualquier rama) podrá emitir un diagnóstico adecuado sobre las fortalezas y debilidades de la empresa, en el cual puede precisar el comportamiento interno de la empresa y sus posibles repercusiones en la misma.

En el análisis y diagnóstico internos, se determinan las fortalezas que tiene la empresa, con el propósito de establecer las medidas tendientes a mantenerlas, incrementarlas y fortalecerlas; también se determinan las debilidades internas de la empresa mediante un estudio detallado, y se hace un diagnóstico sobre las áreas donde se pre-

sentan esas debilidades, así como sobre sus repercusiones, con el propósito de establecer las medidas tendientes a solucionar o al menos disminuir dichas debilidades.

En una auditoría de sistemas computacionales, un estudio de las debilidades y fortalezas del área de sistemas bien aplicado permite diagnosticar el comportamiento interno de la función informática de la empresa, en cuanto a la misión, visión y objetivo del área, y en cuanto al comportamiento de su factor humano, su cultura de servicio, su idiosincrasia y cada uno de los factores analizado anteriormente. Todo esto ayudará a identificar las debilidades del área, a fin de solucionarlas o disminuirlas, así como sus fortalezas, a fin de incrementarlas o al menos mantenerlas. De ahí la importancia de este análisis del factor interno.

10.8.1.2 Los factores de carácter externo

Así como los factores de carácter interno afectan el comportamiento de la empresa y tienen que ser estudiados desde puntos de vista muy específicos, los factores externos, ya sean de carácter local, regional, nacional e incluso internacional, también tienen que ser analizados en cuanto a su influencia en las empresas, debido a que las fuertes repercusiones de estos factores hacen necesario un análisis y diagnóstico muy particulares para cada empresa, por el grado de influencia y trascendencia que tienen en la misma.

Para la explicación del comportamiento de esta matriz, desde el punto de vista externo, podemos establecer los siguientes factores externos que repercuten en el comportamiento de una empresa.

Clientes

Son los compradores potenciales de los bienes o servicios que ofrece la empresa, quienes están dispuestos a adquirirlos si se satisfacen sus expectativas de calidad y utilidad del bien o servicio que adquieren. Los clientes son la influencia fundamental en las actividades de la empresa, su principal fuente de ingresos y su razón de existir.

Evidentemente, ésta es una de las principales influencias externas que repercuten en el comportamiento de la empresa y, por lo tanto, es de suma importancia en el análisis y diagnóstico de la misma.

Canales de distribución

Es la forma en que se hacen llegar a los clientes los bienes o servicios que ofrece la empresa; estos canales de distribución pueden tener muchas modalidades, de acuerdo con las características del producto, el mercado al cual se accede y las peculiaridades de los compradores.

También ejercen cierto tipo de influencia en la actuación de la empresa, ya que tienen influencia de la misma región o de otras regiones; por esta razón deben ser analizados.

Proveedores

Dentro del contexto global en el que conviven actualmente todas las empresas, cualquier empresa se convierte en cliente de los proveedores y al adquirir bienes o servicios de éstos, inevitablemente recibe cierta influencia del comportamiento de cada uno de esos proveedores. Por esta razón, también se tiene que analizar la manera en que pueden influir los proveedores en el comportamiento de la empresa y en la actitud de sus trabajadores. Es evidente que para hacer el análisis y diagnóstico de los factores externos de la empresa se tiene que estudiar ampliamente la influencia externa.*

Competencia

El mercado actual es muy extenso y existen muchas empresas que ofrecen un mismo producto o servicio; por esta razón, el estudio de la competencia es uno de los aspectos más importantes en el análisis de las amenazas y áreas de oportunidad, ya que se tienen que estudiar las posibles repercusiones de las instituciones y personas que ofrecen los mismo bienes o servicios que la empresa evaluada, en cuanto a la calidad del producto o servicio, sus precios, uso de tecnologías, herramientas e instrumentos de fabricación, las formas en que hacen llegar las ofertas de sus bienes o servicios, las formas en que distribuyen sus productos y todos los demás aspectos de la competencia que repercutirán en la empresa.

Es más que obvio que al hacer el análisis y diagnóstico de la empresa se debe estudiar ampliamente la influencia de estos elementos en su comportamiento, ya que pueden determinar sus áreas de oportunidad y amenazas. En una auditoría de sistemas de cómputo, esta influencia se debe analizar a fondo, ya que el servicio, mantenimiento, la asesoría, el *outsourcing* y otros aspectos pueden tener gran influencia en los usuarios de los sistemas.

Tecnología

La entendemos como *el conjunto de elementos técnicos, herramientas y procedimientos específicos mediante los cuales se puede realizar con eficiencia y eficacia un arte, una especialidad o una actividad productiva;* para el caso de los factores externos que afectan a las empresas, la definiremos como *la repercusión que tienen los cambios que va sufriendo el conjunto de elementos, procedimientos y herramientas técnicas mediante los cuales se realizan las actividades de la empresa*.

* Debido a lo dinámico de los cambios en al ambiente de sistemas computacionales, esta influencia es muy palpable, ya que los cambios en el hardware, software, aplicaciones y otros aspectos ejercen una notable influencia en las actitudes y conducta de los consumidores y usuarios de sistemas. Por ejemplo, salió al mercado la nueva versión de Windows 2000 y muchas empresas tratan de instalarlo de inmediato en sus sistemas de cómputo. Lo mismo ocurrió con Office 2000, los programas de aplicación, lenguajes de programación y un sinnúmero de cambios que influyen en este comportamiento. Hoy está en boga el comercio a través de Internet y muchas empresas empiezan a realizar las acciones necesarias para ingresar a este mercado.

Es evidente que las constantes modificaciones tecnológicas (sean locales, regionales o globales) que sufren todos los procesos de producción de bienes o servicios influyen de manera externa en la empresa. Las modificaciones científicas-tecnológicas y los ininterrumpidos cambios técnicos repercuten forzosamente en todas las instituciones; por esta razón, dichos cambios tienen que ser analizados para vislumbrar las posibles amenazas y áreas de oportunidades que tiene la empresa ante estos cambios tecnológicos.*

Influencia social

Al estar inmersa dentro de una sociedad, la influencia que la empresa recibe de su entorno social es determinante, debido a que en ella se concentran los aspectos sociales de sus propios trabajadores, los de sus clientes y proveedores y los de su entorno regional.

Es obvio que esta influencia social tendrá profundas repercusiones en el comportamiento de la empresa; por esta razón, dicha influencia se tiene que estudiar al hacer el análisis y diagnóstico de los factores sociales que influyen en la empresa, para determinar sus ventajas y desventajas ante las demás empresas.

Influencia política

Es obvio que cualquier empresa pertenece a una sociedad con preferencias y comportamientos políticos muy particulares; por esta razón, el análisis de todos los factores relacionados con el entorno político del lugar donde se asienta la empresa debe hacerse desde el punto de vista de la repercusión que tendrán dichos factores en el comportamiento interno y externo de la misma. Ninguna empresa, ni las personas que la integran, por simpatía o conveniencia, pueden abstraerse de las influencias políticas que repercuten en la sociedad y la región.

Es muy importante hacer el análisis de este factor para determinar las áreas de oportunidad de la empresa, así como sus posibles amenazas.

Influencia económica

El comportamiento del mundo actual está muy influido por los factores económicos, no sólo de la región o el país al que pertenecen las empresas, sino por los de un mundo globalizado que influye grandemente en las decisiones económicas de una nación, de una sociedad y de sus individuos y, por consecuencia, de las empresas.

* Los cambios científico–tecnológicos en el ambiente de sistemas han cobrado una importancia tal, que hoy en día las empresas que no están a la vanguardia en sistemas corren el grave riesgo de quedar obsoletas, e incluso fuera del mercado; es evidente que, debido a estos cambios, las empresas admiten y ejercen una influencia recíproca de carácter externo que se debe tomar en cuenta. Por ejemplo, en el año 2001 una empresa que no utilice Internet para sus comunicaciones está fuera del contexto actual, pues el comercio electrónico ya es una realidad. Sin embargo, en el año de 1995 apenas se empezaba a considerar la influencia de Internet en el contexto global, y comprar o vender por este medio aún no creaba expectativas importantes.

Esta simple razón es la que da pie al estudio de las amenazas y oportunidades de la empresa, en cuanto a sus factores económicos; sin embargo, este análisis debe profundizar en las repercusiones que pueden tener las políticas económicas, los aspectos bancarios, las bolsas de valores, las paridades monetarias y en sí todos los factores económicos que pueden repercutir en la empresa, los cuales son evidentemente de carácter externo, y no sólo de impacto regional sino global.

Influencia cultural

La cultura es el cúmulo de conocimientos de una persona, comunidad, sociedad o país, que conduce a un sistema de creencias, valores, tradiciones y modos de comportamiento del propio individuo y del conjunto de ellos (sociedad). Para el caso del estudio de la matriz DOFA, se tiene que tomar en cuenta la influencia de la cultura externa en la empresa, debido a que en el actual contexto mundial los medios de comunicación han influido enormemente los sistemas culturales regionales y nacionales, en cuanto a sus creencias, valores, actitudes, idiosincrasia y formas de conducta grupal. Esto se debe a las extraordinarias facilidades de comunicación (cine, radio, televisión, Internet, libros, prensa escrita, etcétera) que permiten una amplia difusión, conocimiento y adopción de diferentes aspectos culturales por parte de muchas personas de diferentes partes del mundo. Evidentemente, estas influencias también han impactado la conducta cultural de las empresas y de sus empleados, creando serias amenazas y fortalezas en su actuación; incluso ya se habla de transculturación.*

Con el análisis de cada uno de los factores externos que repercuten en las empresas, el auditor de sistemas computacionales (o de cualquier disciplina) puede identificar las áreas de oportunidad que tiene la empresa en estudio, con el propósito de fomentar su aprovechamiento y utilidad, y puede identificar las amenazas que provienen del exterior. La empresa estará en condiciones de analizar esas amenazas para enfrentarlas, desviarlas o al menos disminuir su repercusión en sus actividades.

Las amenazas y áreas de oportunidad del entorno exterior tienen una enorme repercusión en el comportamiento del área de sistemas de la empresa, y no sólo en lo relacionado con la tecnología, sino en el comportamiento de sus empleados, usuarios y proveedores. De ahí la enorme importancia de la participación del auditor, ya que con el estudio de estos factores puede identificar las amenazas del contexto exterior para combatirlas o reducirlas, e identificar las áreas de oportunidad para incrementarlas y fortalecerlas.

* "Proceso de difusión o de influencia de los rasgos culturales de una sociedad cuando entra en contacto con otra que se encuentra bastante menos evolucionada." Pequeño Larousse [...] En el ambiente de sistemas computacionales es evidente esta transculturación, debido a la constante influencia recibida de las culturas en donde se desarrollan estos sistemas. En la actualidad recibimos tal influencia que no sólo afecta la conducta de los usuarios de sistemas, sino también el lenguaje utilizado en estas áreas (*bootear* de *boot*, por ejemplo), el desarrollo de los sistemas, las negociaciones y muchas otras cosas más.

10.8.1.3 Repercusión externa dentro del ámbito de influencia

Para complementar el análisis de las áreas de oportunidad y amenazas de la empresa, así como el análisis de sus fortalezas y debilidades, es necesario determinar cómo influye el ambiente en el que se desenvuelve la empresa, ya que este aspecto es quizás el que más va a influir, de manera directa, en la empresa y en sus integrantes. Por esta razón, cada uno de los siguientes ambientes se debe estudiar por separado.

ambiente local

Es específicamente el lugar donde se encuentra ubicada la empresa, la cual está directamente influida por el barrio, colonia, poblado o región local de donde provienen e interactúan la mayoría de sus empleados; es obvio que esto influirá notablemente en las acciones y comportamiento de los integrantes de la empresa.

ambiente regional

Además del ámbito local, también se debe estudiar el impacto que tiene la región donde se localiza la empresa, ya que este aspecto puede llegar a influir de manera notable en las actividades y comportamiento de sus integrantes. Se dice que el comportamiento de los sureños no es igual al de los norteños, y que la actitud de los costeños no es igual a la de los habitantes de una ciudad, etcétera.

ambiente nacional

Es el comportamiento global de toda una nación, con su amalgama y mosaico de comportamientos, costumbres, valores, folclor y culturas que se conjuntan en un solo comportamiento nacional. Todos estos aspectos en conjunto pueden ser identificados dentro de un mismo comportamiento étnico y cultural específico de un país.

ambiente internacional

Es el ambiente mundial que afecta a la empresa, así como la manera de interactuar de sus integrantes con los integrantes de otras entidades y regiones, lo cual también afecta a la empresa.

El estudio de cada uno de los ambientes que influyen en la empresa es el factor que permitirá establecer, de la manera más precisa posible, las *Fortalezas y Debilidades* de la empresa, así como sus *áreas de Oportunidad y Amenazas*.

10.8.2 Aplicación de la matriz DOFA en la auditoría de sistemas computacionales

El fundamento para la aplicación de esta matriz de Debilidades, Oportunidades, Fortalezas y Amenazas en una auditoría de sistemas computacionales, es que mediante dicha matriz se pueden estudiar las influencias que afectan el comportamiento del área de sistemas computacionales de una empresa, tanto las que recibe de su ambiente in-

terior, como las de su ambiente exterior, ya sean de la propia empresa o de sus proveedores, desarrolladores o del entorno donde se encuentra establecida.

Concretamente, por medio de su aplicación se pueden realizar el *análisis y diagnóstico internos* de todas las *Fortalezas y Debilidades* de los sistemas computacionales de la empresa, así como el *análisis y diagnóstico externos* de todos los factores que se pueden convertir en sus *áreas de Oportunidad y Amenazas*.

El uso de esta matriz permite analizar planos específicos de influencia en el servicio de cómputo que se proporciona a la empresa, mismos que influyen en el comportamiento de los integrantes del área de sistemas, en los usuarios y, por consiguiente, en la prestación de este servicio computacional.

Los factores a estudiar en la auditoría de sistemas computacionales serán:

Los factores de carácter interno en el área de sistemas

- *Misión, visión y objetivo del área de sistemas*
- *Factores humanos que influyen en el área de sistemas*
- *Cultura informática del área de sistemas y de la empresa*
- *Sistemas computacionales, muebles, equipos y bienes informáticos*
- *Servicios de cómputo que proporciona el área de sistemas*
- *Estrategias de servicio computacional*
- *Estructura de organización del área de sistemas*
- *Idiosincrasia, valores y costumbres del área de sistemas*
- *Filosofía de calidad del servicio de cómputo*

Los factores de carácter externo en el área de sistemas

- *Usuarios de los sistemas computacionales*
- *Canales de distribución de los servicios de cómputo*
- *Proveedores y distribuidores*
- *Competencia intercomputacional*
- *Desarrollo de la tecnología informática*
- *Influencia social del ambiente informático*
- *Influencia política del ambiente informático*
- *Influencia económica del ambiente informático*
- *Influencia cultural del ambiente informático*

Repercusión externa dentro del ámbito de influencia

- *Ambiente del área de sistemas*
- *Ambiente de la empresa*
- *Ambiente regional y nacional*
- *Ambiente internacional*

Explicaremos la aplicación específica de esta matriz para la auditoría de sistemas computacionales, después de analizar brevemente cada uno de los siguientes factores.

10.8.2.1 Los factores de carácter interno en el área de sistemas

Será el análisis del área de sistemas con el propósito de identificar sus fortalezas y debilidades en la prestación del servicio de cómputo para la empresa, para incrementar dichas fortalezas, reforzarlas o al menos mantenerlas de la misma forma, así como solucionar las debilidades, o al menos reducir su repercusión en la prestación del servicio. Contando con lo anterior, el auditor planteará plenamente las causas de dichas fortalezas y debilidades, y propondrá soluciones, conforme al formato de situaciones encontradas establecido en el capítulo 7.

El auditor debe realizar el análisis y diagnóstico de las fortalezas y debilidades de los factores internos del área de sistemas, mediante los factores que analizaremos a continuación.

Misión, visión y objetivo del área de sistemas

Es la clara identificación de la razón de existir del centro de cómputo de la empresa, misma que se determina por su misión, así como por la visión que se tiene de dicho centro y por el objetivo que se pretende satisfacer.

En forma general, estos factores se pueden considerar de la siguiente manera:

- **Misión de un área de sistemas**: *Área creada para satisfacer las necesidades computacionales de la empresa, por medio del servicio de captura de datos, procesamiento de información y emisión de información útil para las demás áreas de la institución, así como para el desarrollo de sistemas tendientes a satisfacer las necesidades de cómputo de los usuarios.*
- **Visión de un área de sistemas**: *Área de servicio que contribuye al procesamiento de la información para la mejor toma de decisiones de los usuarios, así como al respaldo, custodia y protección de la información, los bienes informáticos y los sistemas computacionales de la empresa, para el mejor desarrollo de sus actividades.*
- **Objetivo de un área de sistemas**: *Proporcionar el servicio de procesamiento de información con eficacia y eficiencia, a fin de satisfacer las necesidades de los usuarios, en cuanto al procesamiento, diseño, implantación y mantenimiento de sus sistemas, así como resguardar, custodiar y proteger la información, programas y bienes informáticos a su cargo.*

El auditor de sistemas es el responsable de verificar que el área de sistemas contribuya adecuadamente en las actividades de la empresa, así como de verificar que dicha área proporcione el servicio de manera eficaz.

Factores humanos que influyen en el área de sistemas

Son los factores de mayor influencia en las fortalezas y debilidades del centro de información de la empresa, y debemos distinguir cinco factores humanos que repercuten en

el desarrollo de las funciones, actividades y operaciones del área de sistemas; (ver figura 10.3) éstos son:

- Los directivos del área de sistemas
- El personal del área de sistemas
- Los usuarios del sistema
- Los asesores y consultores
- Los proveedores y distribuidores

Figura 10.3 *Factor humano en el área de Sistemas.*

Dentro de un estricto análisis de los factores internos del área de sistemas, los dos primeros son los que realmente pertenecen a ella y, por lo tanto, de ellos obtendrá sus fortalezas y debilidades. Sin embargo, en la práctica, los usuarios también se consideran como parte del área de sistemas, y también serán contemplados para hacer este análisis y diagnóstico de los factores internos. Los otros dos serán considerados para el análisis del factor externo.

Es responsabilidad del auditor tomar en cuenta estos factores humanos para emitir su opinión respecto a las fortalezas y debilidades del centro de cómputo, considerando su importancia en el servicio de cómputo que se proporciona a las demás áreas de la empresa.

Cultura informática del área de sistemas y de la empresa

Es el conocimiento, costumbres, valores, creencias y manera de actuar de quienes participan en la función informática de la empresa, tanto del personal del área de sistemas, como de los usuarios del sistema pertenecientes a las demás áreas. En conjunto, este personal integra la cultura informática que lo identifica como empresa.

Sistemas computacionales, muebles, equipos y bienes informáticos

Es la identificación de las debilidades y fortalezas del centro de cómputo, en cuanto a la capacidad de cómputo de la empresa, sus actualizaciones, utilidad y satisfacción de las necesidades computacionales de los usuarios, así como respecto a su plataforma de servicios, actualización de sus sistemas computacionales, incluyendo el hardware, software, periféricos, instalaciones, mobiliario, equipos y demás bienes informáticos del centro de cómputo y de las demás áreas de la empresa.

Servicios de cómputo que proporciona el área de sistemas

Partiendo de que la principal función del área de sistemas es proporcionar los servicios computacionales para las demás áreas de la empresa, se deben identificar plenamente las fortalezas en la prestación de este servicio para fortalecerlas, así como sus debilidades en el servicio a fin de solucionarlas.

Ésta es quizá una de las acciones más importantes del auditor de sistemas computacionales, ya que permite identificar, mediante su informe y diagnóstico, la calidad de servicios que se proporcionan a los usuarios y a las demás áreas de una empresa.

Estrategias de servicio computacional

Son todos los planes, políticas y lineamientos que se adoptan para satisfacer eficaz y eficientemente las necesidades de cómputo de los usuarios, de tal manera que se cumpla con la misión, visión y objetivos del área de sistemas.

El auditor de sistemas computacionales debe hacer una evaluación efectiva de la existencia, difusión y cumplimiento de esta estrategia del servicio de cómputo.

Estructura de organización del área de sistemas

Es la estructura de los puestos, funciones, canales de comunicación, líneas de autoridad y jerarquías que se adoptan en el centro de cómputo para proporcionar este servicio a las demás áreas de la empresa, incluyendo la descripción de puestos, delimitación de funciones y actividades, asignación de niveles de autoridad y responsabilidad para cada unidad administrativa que integra esta área.

El auditor de sistemas debe evaluar si esta estructura de organización fortalece al área o si, por el contrario, la debilita para el cumplimiento de su cometido.

Idiosincrasia, valores y costumbres del área de sistemas

Similar a la cultura informática, es la identificación de la manera de actuar de cada uno de los integrantes del área de sistemas de la empresa; es decir, la forma de ser, el temperamento y cultura con las que se conduce una persona en el área, la empresa, la sociedad o el país. También se relacionan con el conjunto de cualidades, usos, prácticas y maneras habituales de proceder que definen el carácter de las personas. En conjunto, estos aspectos determinan las peculiaridades y características de comportamiento del personal del área de sistemas de la empresa.

Filosofía de calidad del servicio de cómputo

Es la forma en que se proporcionan los servicios de cómputo a las demás áreas de la empresa, en cuanto a la oportunidad, confiabilidad, veracidad, suficiencia y seguridad en el procesamiento de la información, así como en su protección y custodia, y en cuanto a la eficiencia y eficacia de los sistemas computacionales de la empresa.

Contando con el análisis de todos los aspectos anteriores, el auditor de sistemas computacionales estará en posibilidades de identificar y evaluar las fortalezas y debilidades del área de sistemas, a fin de emitir una opinión fundamentada sobre las mismas. Con ello se contribuye a incrementar esas fortalezas y solucionar las debilidades observadas, (ver figura 10.4).

10.8.2.2 Los factores de carácter externo en el área de sistemas

Es el análisis y diagnóstico de las amenazas que pueden repercutir en el funcionamiento del área de cómputo de la empresa, así como de sus áreas de oportunidad para proporcionar el servicio de cómputo de manera más eficaz y eficiente a las demás áreas de la empresa.

Estas amenazas y áreas de oportunidad se pueden identificar mediante el estudio de los siguientes factores de carácter externo:

- *Misión, visión y objetivo del centro de cómputo*
- *Factores humanos que influyen en el área de sistemas*
- *Cultura informática del área de sistemas y de la empresa*
- *Sistemas computacionales, muebles, equipos y bienes informáticos*
- *Servicios de cómputo que proporciona el área de sistemas*
- *Estrategias de servicio computacional*
- *Estructura de organización del área de sistemas*
- *Idiosincrasia, valores y costumbres del área de sistemas*
- *Filosofía de calidad del servicio de cómputo*

Figura 10.4 *Factores externos al área de sistemas.*

Usuarios de los sistemas computacionales

Es el análisis de las oportunidades que se tienen con los usuarios de los sistemas computacionales de la empresa, en cuanto a su manejo, operatividad y desarrollo, así como de las amenazas que puede haber para el funcionamiento adecuado de los sistemas computacionales. El auditor deberá evaluar la repercusión de ambos aspectos en el servicio que proporciona el área de sistemas de la empresa.

Canales de distribución de los servicios de cómputo

Es la manera en que se distribuyen los servicios de cómputo de la empresa, ya sea mediante una red de cómputo, sistemas descentralizados a cargo del usuario y las áreas de servicios, en forma centralizada en un área específica de computación o por cualquier otra forma. En este caso, la función fundamental del auditor de sistemas es evaluar las áreas de oportunidad en la prestación del servicio, así como sus amenazas.

Proveedores y distribuidores

Es la influencia externa que recibe el área de sistemas a través de quienes le proveen los sistemas computacionales, el equipo de cómputo (hardware), los sistemas operativos, lenguajes y programas de aplicación (software), o de quienes le proveen el mobiliario, mismos que se pueden convertir en verdaderas áreas de oportunidad o en amenazas para la prestación del servicio de cómputo.

El auditor deberá saber identificar la repercusión de estas personas en la prestación del servicio de cómputo del área, ya que en la época actual los factores externos influyen mucho (positiva o negativamente) en el área de sistemas de las empresas. Debido a los constantes cambios en la tecnología informática y a los nuevos desarrollos de sistemas, redes y telecomunicaciones que se dan en todo el mundo, la participación de estas personas en el área de sistemas a veces es muy importante, pero otras sólo son requeridos para la adquisición de nuevos sistemas.

Competencia intercomputacional

En lo relacionado con la competencia, encontramos que la matriz DOFA se puede aplicar al considerar las innovaciones que a diario se presentan en los sistemas computacionales, ya sea en sus componentes, en el hardware, el software, las telecomunicaciones, los equipos, mobiliarios y en cualquier otro aspecto; esto, porque ya estamos muy acostumbrados a los continuos cambios tecnológicos, que con alarmante frecuencia, hacen que las áreas de sistemas busquen estar siempre a la vanguardia informática, lo cual las conduce a una constante competencia para obtener lo más avanzado en sistemas.

En cuanto al sentido de competencia o capacidad, el auditor deberá aplicar esta matriz para determinar las fortalezas y debilidades del área de sistemas en relación con su capacidad para proporcionar este servicio con eficiencia, eficacia, calidad, oportunidad, confiabilidad, suficiencia y los demás atributos que debe tener la información; asimismo, deberá aplicar dicha matriz para determinar las amenazas y áreas de opor-

tunidad del área de sistemas y de la propia empresa, para evaluar el funcionamiento del servicio de cómputo suministrado a todas las áreas de la empresa.

En ambos casos, el auditor de sistemas debe valorar perfectamente los resultados de la matriz de fortalezas y debilidades que son producto de influencias externas al área de sistemas, e incluso de las que provienen de la propia empresa, la región y el país; pero inevitablemente debe enfocar su análisis al aspecto meramente informático, ya sea por los constantes cambios tecnológicos o por la manera en que se brinda el servicio de computación a las demás áreas de la empresa. Asimismo, el auditor debe valorar las áreas de oportunidad que surgen con la nueva tecnología y la repercusión de ésta en la prestación de los servicios de cómputo, pero también debe considerar las posibles desventajas de estos avances tecnológicos en dicha prestación de servicios.

Contando con este estudio, el auditor podrá identificar y sacar ventaja de las fortalezas y áreas de oportunidad del centro de cómputo y mostrará las debilidades y amenazas para determinar y proponer alternativas de solución.

Desarrollo de la tecnología informática

Similar al punto anterior, con aplicación de la matriz DOFA sirve para evaluar las fortalezas y debilidades que surgen en el área de sistemas al adquirir nuevas tecnologías de cómputo, pero también sirve para valorar las oportunidades del área y amenazas del exterior producidas por los constantes y continuos cambios tecnológicos en cómputo.

Al aplicar esta matriz, el trabajo del auditor consiste precisamente en hacer el análisis y diagnóstico de esas fortalezas y debilidades del área, así como de sus oportunidades y amenazas externas, con el fin de evaluar su funcionamiento actual.

Influencia social del ambiente informático

Al pertenecer el área de sistemas a una empresa, y ésta a su vez a una sociedad, dentro del contexto mundial, la influencia que esta área recibe de su entorno social es determinante, cualquiera que sea, debido a que en ella coinciden los aspectos sociales de sus trabajadores con los de las demás áreas de la empresa; además, quiérase o no, el comportamiento de sus trabajadores se ve influido por el de sus clientes y proveedores, sean del barrio, de la región o del entorno global.

Es obvio que esta influencia social tendrá profundas repercusiones en el comportamiento social de los integrantes de esta área; por esta razón haremos un análisis y diagnóstico de los factores sociales que influyen en dicha área, con el fin de determinar sus ventajas y desventajas ante las demás áreas de la organización, e incluso ante otras empresas.

Influencia política del ambiente informático

Es obvio que al pertenecer una empresa a una sociedad, dicha empresa debe estar influida por las preferencias y el comportamiento político de esa sociedad; por esta razón es necesario hacer el análisis de todos los factores (internos y externos) referentes

al entorno político de la sociedad a la que pertenece la empresa; sin embargo, también es necesario analizar la repercusión que dicho comportamiento político tendrá en el comportamiento interno del área de sistemas computacionales, así como en su comportamiento hacia las demás áreas de la empresa. Ninguna empresa ni persona que integran una sociedad pueden abstraerse de las influencias políticas de esa sociedad, de la región, del país, ni del ambiente mundial.

Es evidente que el análisis del factor político ayuda a determinar las fortalezas y debilidades del área de sistemas y sus áreas de oportunidad dentro de la empresa, así como sus posibles amenazas.

Influencia económica del ambiente informático

El comportamiento ante la influencia económica en el área de sistemas es el mismo que en todas las demás áreas de la empresa. Este comportamiento está altamente influido por los factores económicos, no sólo de la región o del país en donde se asienta la empresa, sino por los de un mundo globalizado que influye enormemente en las decisiones económicas de una nación, de una sociedad y de sus individuos y, por consecuencia, de las empresas.

Influencia cultural del ambiente informático

Aquí se considera el cúmulo de conocimientos de los empleados del área de sistemas, el cual conduce al sistema de creencias, valores, tradiciones y modos de comportamiento del propio individuo y del conjunto de ellos. Para el caso del estudio de la influencia de la cultura en el área de sistemas y en la empresa, es necesario considerar la enorme difusión que existe actualmente en el ámbito mundial en materia de sistemas computacionales, lo cual hace que cada día se considere más pequeño el mundo informático.

Además, las facilidades de comunicación actuales (cine, radio, televisión, Internet, prensa escrita, libros, revistas especializadas, etcétera) hacen que la cultura de sistemas computacionales sea una de las áreas con mayor difusión, más conocidas y adoptadas por muchísimas personas de diferentes partes del mundo. Evidentemente, con esto se han llegado a impactar las conductas culturales de los integrantes del área de sistemas de las empresas, creando así serias amenazas y fortalezas en este renglón.

10.8.2.3 Repercusión externa dentro del medio de influencia

Con la aplicación de la matriz DOFA, el auditor puede estudiar la repercusión de la influencia externa en el área de sistemas, a fin de identificar las influencias que se pueden convertir en áreas de oportunidad o amenazas para la prestación eficiente del servicio de cómputo en la empresa.

Dicho estudio se tiene que realizar forzosamente en dos sentidos: por un lado, la influencia que ejercen las demás áreas de la empresa, consideradas en estricto sentido como ajenas al centro de cómputo, con el fin de evaluar el grado de repercusión de di-

cha influencia en su funcionamiento actual. Por otro lado, la influencia de los agentes externos a la empresa, pero que tienen injerencia en el área de sistemas; en este caso deben ser considerados los proveedores de sistemas, desarrolladores externos, asesores, usuarios externos, los posibles contactos relacionados con los sistemas pero ajenos a la empresa, e incluso los medios de difusión escritos, de radio, televisión o Internet.

Estos factores, que ya hemos estudiado, son los siguientes:

- *Medio ambiente del área de sistemas*
- *Medio ambiente de la empresa*
- *Medio ambiente regional y nacional*
- *Medio ambiente internacional*

10.8.3 Propuesta de una matriz DOFA para una auditoría de sistemas computacionales

El siguiente ejemplo sirve para mostrar el diseño de una matriz aplicable a los funcionarios y empleados del área de sistemas y, de ser necesario, a los usuarios de los sistemas; esta matriz se puede aplicar ya sea mediante la técnica de entrevista o mediante cuestionarios de tipo abierto, debido al tipo de interrogantes que se tienen que responder.

El diseño de esta matriz consta de dos partes, una es la identificación y la explicación de los aspectos que serán utilizados en este análisis, y la otra comprende las respuestas a la investigación sobre las fortalezas y debilidades internas del área de sistemas, así como a las amenazas y oportunidades externas que afectan a esta área.

"AUDITORÍA EN SISTEMAS COMPUTACIONALES"

MATRIZ DE EVALUACIÓN DE FORTALEZAS, DEBILIDADES, OPORTUNIDADES Y AMENAZAS QUE IMPACTAN AL ÁREA DE SISTEMAS DE LA EMPRESA_____

Fecha:_____/_____/_____

Entrevistado: _____

Área o Departamento: _____

Puesto: _____

Con la finalidad de efectuar un estudio del funcionamiento del área de sistemas de la empresa, se solicita su valiosa respuesta para las siguientes preguntas:

(Guía de preguntas para realizar una entrevista)

1. ¿Conoce la misión, visión y objetivo general del área de sistemas computacionales de su empresa? Describa brevemente cada uno de ellos, y si en su opinión es necesario modificarlos o eliminarlos, coméntelo también.
2. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las fortalezas del área de sistemas y sus sugerencias para aumentarlas:
3. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las debilidades del área de sistemas y sus sugerencias para corregirlas o disminuirlas:
4. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las oportunidades del área de sistemas y sus sugerencias para aprovecharlas:
5. Considerando las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, mencione las amenazas al área de sistemas y sus sugerencias para evitarlas o disminuirlas:
6. Considerando su estancia en el área y las funciones, actividades y operaciones que realiza con los sistemas computacionales de la empresa, señale cuál cree que sea la cultura informática del área y de la empresa:
7. ¿Cree que en la empresa existen estrategias para la prestación del servicio informático?
8. ¿Conoce el lugar que ocupa en el organigrama del área de sistemas? ¿Cree que dicha estructura es adecuada para satisfacer la prestación del servicio informático en la empresa?
9. Considerando su estancia en el área de sistemas computacionales de la empresa, ¿cuál es, a su juicio, la idiosincrasia del área de sistemas?, ¿cuáles son los valores y las costumbres informáticas de esta área? Comente sus cambios y modificaciones:
10. ¿Conoce la filosofía de calidad del área de sistemas computacionales?, ¿qué opinión tiene de ella?
11. ¿Qué influencia ejercen en el cumplimiento de su trabajo los usuarios de los sistemas computacionales de la empresa?
12. ¿Qué influencia ejercen en el cumplimiento de su trabajo los clientes del área de sistemas computacionales de la empresa?
13. ¿Qué influencia ejercen en el cumplimiento de su trabajo los proveedores del área de sistemas computacionales?
14. De acuerdo con su experiencia en sistemas computacionales, ¿existe competencia en la función informática que desarrolla esta área para toda la empresa? Amplíe si es necesario.
15. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter social ejercen en el cumplimiento de su trabajo sus compañeros?

16. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter social ejerce en el cumplimiento de su trabajo la comunidad donde la empresa realiza sus actividades?
17. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter social ejerce en el cumplimiento de su trabajo la región geográfica donde la empresa realiza sus actividades?
18. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter social ejerce en el desarrollo de su trabajo la nación de donde es originaria la empresa?
19. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter político ejercen en el desarrollo de su trabajo sus compañeros?
20. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter político ejerce en el desarrollo de su trabajo la comunidad donde la empresa realiza sus actividades?
21. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter político ejerce en el desarrollo de su trabajo la región geográfica donde la empresa realiza sus actividades?
22. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter político ejerce en el desarrollo de su trabajo la nación de donde es originaria la empresa?
23. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter económico ejercen en el desarrollo de su trabajo sus compañeros?
24. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter económico ejerce en el desarrollo de su trabajo la comunidad donde la empresa realiza sus actividades?
25. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter económico ejerce en el desarrollo de su trabajo la región donde la empresa realiza sus actividades?
26. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter económico ejerce en el desarrollo de su trabajo la nación de donde es originaria la empresa?
27. De acuerdo con su experiencia en sistemas computacionales y antigüedad en la empresa, ¿qué influencia de carácter cultural ejercen en el desarrollo de su trabajo sus compañeros?
28. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter cultural ejerce en el desarrollo de su trabajo la comunidad donde la empresa realiza sus actividades?
29. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter cultural ejerce en el desarrollo de su trabajo la región donde la empresa realiza sus actividades?

30. De acuerdo con su experiencia en sistemas computacionales, ¿qué influencia de carácter cultural ejerce en el desarrollo de su trabajo la nación de donde es originaria la empresa?
31. De acuerdo con su experiencia en sistemas computacionales y antigüedad en el área de sistemas, ¿qué influencia de carácter social, político, económico y cultural ejerce en el desarrollo de su trabajo el exterior de nuestro país?

Técnicas especiales de auditoría de sistemas computacionales

11

Estructura del capítulo:

Objetivos del capítulo

Dar a conocer las técnicas, métodos y herramientas especiales que pueden ser aplicables en la auditoría de sistemas computacionales, a fin de que el lector conozca su forma de aplicación y funcionamiento en la evaluación de los aspectos técnico-computacionales de las empresas y, contando con ese conocimiento, pueda aplicar dichas herramientas para cualquier otra necesidad específica de auditoría de sistemas.

Introducción del capítulo

En la auditoría de sistemas computacionales se utilizan múltiples herramientas y técnicas tradicionales de la auditoría que permiten hacer una eficiente revisión al funcionamiento de los sistemas de cómputo, a su gestión informática y a los diferentes aspectos del ambiente de sistemas. Sin embargo, como profesional especializado en la evaluación de los sistemas de cómputo, el auditor de sistemas también debe conocer y utilizar otras herramientas, técnicas y procedimientos específicos del área de informática, los cuales le ayudan a examinar y evaluar con mayor eficiencia los aspectos propios de la actividad computacional.

11.1 Guías de evaluación

Las guías de auditoría son las herramientas más utilizadas y quizá las más importantes en cualquier auditoría de sistemas computacionales; estas guías son un documento formal que indica el procedimiento de evaluación que debe seguir el auditor; asimismo, en este instrumento se indican todos los puntos, aspectos concretos y áreas que deben ser revisados, así como las técnicas, herramientas y procedimientos que deben ser utilizados en la auditoría de sistemas computacionales.

La guía de evaluación es una herramienta de carácter formal, en la cual se anotan todos los asuntos que serán evaluados durante la auditoría, ya sea el centro de cómputo, el sistema computacional, la gestión informática o cualquier otro aspecto. En este documento también se anota la forma en que cada uno de los puntos que serán evaluados y como deben ser analizados, determinando, hasta donde sea posible, tanto la técnica que se va a utilizar como el método a seguir para dicha evaluación; también se anota la ponderación o peso específico que se dará a cada uno de esos puntos. *En este capítulo también analizaremos lo relacionado con la ponderación.*

Para cualquier auditor, con experiencia o sin ella, la guía de evaluación es un documento que le permitirá realizar, en forma eficiente y efectiva, su reconocimiento de auditoría para cualquier aspecto relacionado con los sistemas computacionales, ya que en esta guía se le indica todo el procedimiento que debe seguir, los puntos que debe evaluar y las herramientas que debe utilizar para hacer su revisión, incluyendo la manera de aplicarlas. Es decir, mediante este documento el auditor puede hacer el seguimiento paso a paso de todos los procedimientos para evaluar los puntos que tenga que evaluar.

Evidentemente, la utilidad de este documento estará determinada por la calidad, contenido y profundidad de los aspectos que abarque.

Antes de continuar, es conveniente ver algunas definiciones sobre esta herramienta:

Guías

"El que acompaña a otro para presentarle el camino... Persona que dirige a otra [...] Lo que dirige [...] Libro de indicaciones [...]"[1]

"[...] Lo que dirige o sirve de orientación [...] Libro, folleto con datos, explicaciones o normas de una determinada materia, para información del usuario."[2]

Evaluación

"Acción o efecto de evaluar. Valoración que se hace de las aptitudes y méritos de una persona o de los conocimientos [...]"[3]

Evaluar

"Señalar el valor de una cosa. Calcular el valor que puede tener."[4]

"Valorar. Fijar el valor de una cosa."[5]

"Calcular el valor de una cosa. Valorar. Valuar."[6]

Valor

"Del latín **valor***:* Lo que vale una persona o cosa *[...] Importancia [...] Determinación de una cantidad [...]"*[7]

"Grado de calidad, mérito, utilidad o precio que tienen personas y cosas [...] Significación y alcance de algo [...] Eficacia o virtud de las cosas para producir efectos. Precio equivalente a una cosa [...]"[8]

Valorar

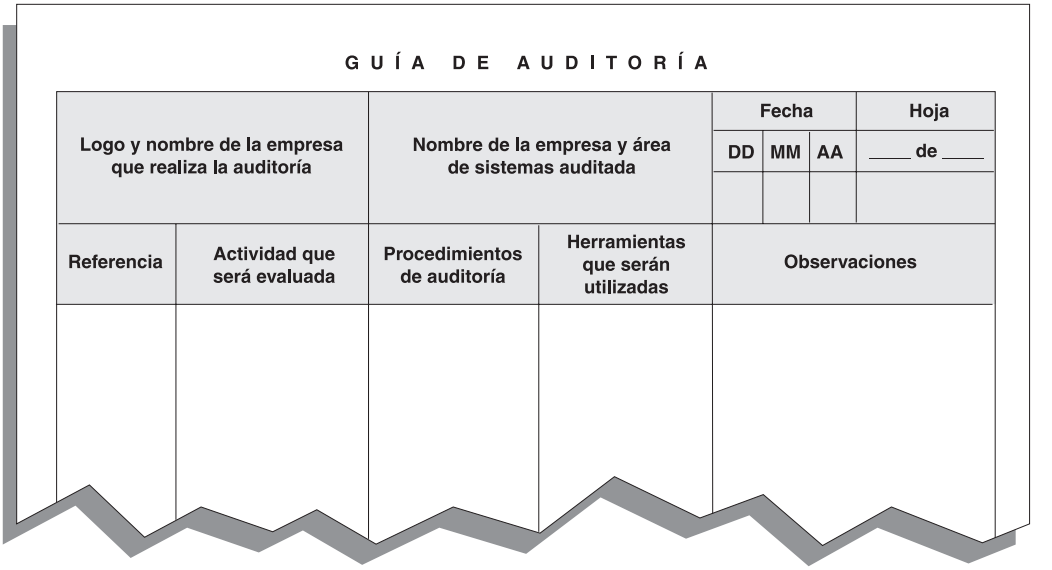
"Señalar precio a una cosa. Atribuir determinado valor o estima a personas o cosas. Hacer que aumente el valor de una cosa."[9]

De acuerdo con estas definiciones, a continuación presentaremos la siguiente definición para guía de evaluación de auditoría:

> *Es un documento formal, mediante el cual el auditor va siguiendo un procedimiento concreto que le permite hacer su revisión de auditoría de sistemas, y en*

el cual se le indican los puntos que debe revisar, las técnicas y métodos que debe seguir, así como el peso específico que cada uno de esos puntos tendrá en su evaluación. Con ello se cubren todos los aspectos que deben ser evaluados.

La guía de auditoría es un documento básico en una auditoría de sistemas, mediante el cual se puede hacer una buena revisión de las áreas de sistemas, de la gestión informática y en sí de todos los aspectos del sistema. Además es muy útil para cualquier auditor, independientemente de su experiencia y conocimientos en este tipo de auditorías, ya que con su aplicación puede estandarizar los procedimientos de revisión y evaluación.



GUÍA DE AUDITORÍA

Logo y nombre de la empresa que realiza la auditoría		Nombre de la empresa y área de sistemas auditada		Fecha			Hoja
				DD	MM	AA	____ de ____
Referencia	**Actividad que será evaluada**	**Procedimientos de auditoría**	**Herramientas que serán utilizadas**	**Observaciones**			

Figura 11.1 *Ejemplo de formato de guías de evaluación.*

Debido a la importancia y gran utilidad de esta guía para una auditoría de sistemas computacionales, a continuación haremos un breve análisis de su contenido, así como de la forma de utilizarla:

Encabezado

Cualquier documento de auditoría de sistemas computacionales debe contener invariablemente una identificación en la cual se indiquen, como mínimo, los siguientes puntos:

Empresa responsable de realizar la auditoría

Aquí van impresos el logotipo y nombre de la empresa responsable de realizar la auditoría, según las normas y costumbres sobre este aspecto.

Nombre de la empresa y área de sistemas auditada

Aquí se anotan el nombre de la empresa y el nombre completo del área de sistemas auditada.

Fecha

Aquí se anota la fecha en que se iniciará la auditoría. Es preferible anotarla en el formato de día, mes y año, conforme a la figura.

Hoja

Para llevar el orden adecuado, es necesario numerar las hojas con el formato número de hoja y el total de las mismas; así el auditor responsable de la revisión puede llevar el control numérico de la guía.

Como ejemplos tenemos:

Hoja 5 de 26. Aquí es la hoja 5 de 26

Hoja 9.1 de 40. Aquí la hoja es la que sigue de la hoja nueve, pero que fue necesario insertar, y para no alterar el total de hojas, se inserta como hoja 9.1

Referencia

Para un control adecuado del contenido de la guía, es muy conveniente asignar un número continuo, nemotécnico o de referencia, para señalar el punto a que se refiere la evaluación. Esto permite hacer un seguimiento adecuado de los puntos que van a ser evaluados y ayuda a establecer los procedimientos que se deben utilizar en caso de encontrar desviaciones en algún punto.

Actividad que será evaluada

Aquí se anotan, lo más clara y detalladamente posible, los puntos que el auditor debe analizar, explicando específicamente cada uno de los aspectos, actividades, funciones o puntos que serán evaluados.

Procedimientos de auditoría

De acuerdo con lo anotado en las actividades que serán evaluadas, en esta columna se anotan los procedimientos a seguir para realizar la evaluación. En esta parte se especifican los procesos, pasos y demás instrucciones que servirán de guía para evaluar lo especificado en la columna anterior; se pueden anotar tantos procedimientos como sean necesarios durante la evaluación.

Herramientas que serán utilizadas

De acuerdo con el contenido de las columnas anteriores, en esta columna se anotan las herramientas, técnicas, procedimientos o instrumentos que serán utilizados en la evaluación. Es costumbre detallar el contenido concreto de estas herramientas, y se pueden anotar tantas herramientas como sean necesarias para la evaluación.

Observaciones

Se podría dar el caso de que hubiera necesidad de hacer aclaraciones; entonces se puede utilizar esta columna para realizarlas, de acuerdo con el punto evaluado.

Ejemplo de guía de auditoría.

Auditores de Sistemas Asociados	Empresa: Comercializadora, S.A. Área: Centro de servicios de sistematización	DD 21	MM 07	AÑO 2002	Hoja 1 de 12

Ref.	Actividad que será evaluada	Procedimientos de auditoría	Herramientas que serán utilizadas	Observaciones
SAS-01	Evaluar la seguridad en el acceso de usuarios de la red y la validez de sus atributos.	Solicitar la asignación de una terminal para entrar al sistema y accesar información, cambiar datos, bases de datos, instrucciones y programas, hasta donde lo permita el sistema. Ingresar al administrador y cambiar privilegios, atributos y contraseñas de varios usuarios.	Observación participativa, oculta. Pruebas al sistema y las bases de datos. Experimentación en la seguridad del sistema. Revisión documental (electromagnética).	El sistema no debe permitir ningún acceso. Obtener respaldo previo del sistema y los movimientos previos a la prueba. Documentar los accesos y cambios que se realicen al sistema.
SAS-02	Evaluar la seguridad de los niveles de acceso de usuarios.	Entrar al sistema de red sin ninguna autorización y accesar a la información, alterar bases de datos o cambios al sistema, hasta donde permita el sistema. Entrar al sistema y dar de alta a distintos accesos sin tener autorización. Solicitar a un usuario, sin forzarle, que ingrese a un nivel que no le corresponda y verificar si el sistema le permite la operación.	Observación participativa, oculta. Pruebas al sistema y las bases de datos. Experimentación en la seguridad del sistema. Revisión documental (electromagnética).	El sistema no debe permitir ningún acceso. Obtener respaldo previo del sistema y los movimientos previos a la prueba. Documentar los accesos y cambios que se realicen al sistema.
SAS 03	Evaluar la confiabilidad en la administración de la contraseña.	Ingresar al sistema de red sin contraseña. Reiniciar el sistema y utilizar teclas F5 o F8 al encender	Observación participativa, oculta. Pruebas al sistema y las bases de datos.	El sistema por ningún medio debe permitir el acceso sin contra-seña y al tercer

Continúa

Continuación

		el sistema, e ingresar sin contraseña. Entrar al sistema con disco de arranque externo e ingresar sin contraseña. Tratar de accesar al sistema alterando tres veces la contraseña y observar las acciones del sistema.	Experimentación en la seguridad del sistema. Revisión documental (electromagnética).	intento bloquea la terminal Obtener respaldo previo del sistema y los movimientos previos a la prueba. Documentar los accesos y cambios que se realicen al sistema.
SAS-04	Evaluar la administración y control de la bitácora de acceso a los usuarios del sistema.	Solicitar la asignación de una terminal para entrar al sistema y realizar diversas actividades de las autorizadas, verificando documentalmente que se tengan registradas éstas en la bitácora. Hacer una revisión a la bitácora y verificar la información de los usuarios: la fecha, hora de ingreso y salida del sistema, registro de sus actividades y cualquier incidencia durante su estancia. Monitorear aleatoriamente usuarios y evaluar si las actividades que realizan están registradas en la bitácora. Si es necesario, aplicar encuestas y entrevistas sobre el control de la bitácora de acceso. Evaluar los derechos y obligaciones de los usuarios, en el manual de usuarios o reglamento del área de cómputo, en cuanto a su cumplimiento y registro de incidencias en la bitácora. Verificar que se cumpla con los tiempos límite de acceso y sus registros en la bitácora.	Observación participativa, oculta. Revisión documental a los registros y el sistema de cómputo. Experimentación en la seguridad del sistema. Entrevista con administrador del sistema, los usuarios y personal del área	

Continúa

Continuación

SAS-05	Evaluar el adecuado cumplimiento de las funciones del administrador del sistema de red.	Entrevistar al administrador respecto al cumplimiento de sus funciones, apoyados en el manual de organización, el manual de procedimientos y de operación, Encuestas entre el personal del área y los usuarios del sistema.	Entrevista con administrador del sistema, los usuarios y personal del área. Encuestas a los empleados y usuarios del sistema.	Llevar previamente elaborado el cuestionario de la entrevista y los cuestionarios de la encuesta.
SAS-06	Evaluar el registro histórico de las incidencias de seguridad de acceso al sistema de red.	Hacer la revisión documental a cada una de las bitácoras de incidencias de tres meses, un semestre y un año anteriores y evaluar la magnitud, impacto y solución a las mismas. Evaluar, mediante entrevista o encuesta, a los empleados y usuarios del área, sobre las incidencias ocurridas en esas épocas, y obtener sus opiniones sobre la confiabilidad del registro de incidencias en las bitácoras pasadas.	Revisión documental histórica a las bitácoras anteriores. Entrevista y encuesta con empleados y usuarios.	Elegir aleatoriamente los días y las incidencias a revisar.
SFA-01	Evaluar las medidas de seguridad para el acceso físico del personal y los usuarios del sistema.	Tratar de ingresar al área de sistemas sin ninguna identificación y evaluar las incidencias. Tratar de ingresar al área de sistemas con la identificación de cualquier empleado y evaluar las incidencias. Evaluar actuación del personal encargado de la entrada y las medidas de seguridad, y vigilancia y del área de sistemas. Entrevistas y cuestionario a los directivos, empleados y usuarios del sistema, para obtener su opinión sobre las medidas de seguridad del área.	Observación participativa, directa y oculta para el acceso al área. Entrevista y encuestas a directivos, empleados y usuarios del área. Revisión documental a reportes y bitácoras de acceso.	Las pruebas de ingreso pueden ser efectuadas por el auditor o por terceros ajenos al área.

Continúa

Continuación

		Verificar los cambios de turno del personal de vigilancia del área de sistemas. Revisar los reportes de novedades del personal de vigilancia y las bitácoras de acceso, así como su oportunidad y suficiencia en el registro.		
SFS-02	Evaluar las medidas de seguridad para el control de acceso y salida de los bienes informáticos del área de sistema.	Revisar los reportes de novedades de salidas y entradas de bienes y evaluar sus contenidos, oportunidades, justificaciones e incidencias. Revisar las bitácoras de entradas y salidas de bienes del área de sistemas, así como el correcto registro de sus contenidos, su oportunidad, y las justificaciones e incidencias. Revisar los controles, formatos y registros documentales de las salidas y entradas de bienes en el área de sistemas. Entrevistas y cuestionario a los directivos, empleados y usuarios del sistema, para obtener su opinión sobre las medidas de seguridad, el registro y la solución de incidencias del área. Tratar de introducir un bien sin notificarlo a vigilancia y sin ninguna autorización. Tratar de sacar un bien sin notificarlo a vigilancia y sin ninguna autorización. Evaluar si existen detectores de metales, aduanas de revisión o cualquier otra medida de revisión para la	Observación participativa, directa y oculta para el acceso al área Entrevista y encuestas a directivos, empleados y usuarios del área. Revisión documental a reportes y bitácoras de acceso. Experimentación al tratar de introducir y de sacar bienes informáticos.	Las pruebas de ingreso pueden hacerlas el auditor o terceros ajenos al área.

Continúa

Continuación

		entrada y salida de bienes del área.		
SFS-03	Evaluar los reportes de incidencia y las acciones preventivas y correctivas en su solución, en el acceso físico de los usuarios.	Revisar los controles, formatos y registros documentales de las salidas y entradas de bienes en el área de sistemas. Entrevistas y cuestionario a los directivos, empleados y usuarios del sistema, para obtener su opinión sobre las medidas de seguridad, el registro y la solución de incidencias del área.	Observación participativa, directa y oculta para el acceso al área Entrevista y encuestas a directivos, empleados y usuarios Revisión documental a reportes y bitácoras de acceso.	
SPC-01	Evaluar los planes de contingencias del área de sistemas.	Solicitar el plan de contingencia y evaluar su correcta elaboración, la asignación de funcionarios responsables, funciones y medidas preventivas y correctivas. Evaluar que el plan de contingencias contenga acciones a realizar antes, durante y después de un siniestro, así como los responsables de las mismas. Evaluar la vigencia, constante actualización, disponibilidad y difusión del plan de contingencias entre directivos, empleados y personal del área de sistemas. Entrevistas y cuestionario a los directivos, empleados y usuarios del sistema, para obtener su opinión sobre el plan de contingencias, su utilidad, conocimiento, difusión y actualización.	Revisión documental a reportes y bitácoras de acceso. Entrevistas y encuestas a directivos, empleados y usuarios.	
SPC-02	Evaluar la realización de simulacros en el	Revisar las bitácoras de elaboración de simulacros y evaluar el registro de	Revisión documental a reportes y bitácoras de acceso.	Si existiesen incidencias verdaderas y no

Continúa

Continuación

	área de sistemas.	incidencias, cumplimiento de actividades, objetivos y correcciones a las medidas preventivas y correctivas. Entrevistas y cuestionario a los directivos, empleados y usuarios del sistema, para obtener su opinión sobre el plan de contingencias, su utilidad, conocimiento, difusión y actualización. Obtener los reportes de novedades, incidencias y medidas correctivas, derivadas de los simulacros y evaluar las modificaciones al plan de contingencias. Evaluar que el plan de simulacros contenga acciones preventivas para realizar el simulacro y correctivas para después del mismo. Así como la correcta documentación de su realización.	Entrevista y encuestas a directivos, empleados y usuarios.	simulacros, aplicar estos mismos puntos.

La guía de evaluación a la seguridad que expusimos como ejemplo está diseñada para evaluar la seguridad en el acceso al sistema (SAS-00), Seguridad física a las áreas de sistemas (SFA-00) y Seguridad en el plan de contingencias del área de sistemas SPC-00), la cual contempla algunos de los principales aspectos de seguridad informática que debe revisar el auditor, adaptando los puntos de la misma a las necesidades de revisión de la seguridad en la empresa donde se realice esta revisión.

11.2 Ponderación

La ponderación es una técnica especial de evaluación, mediante la cual se procura darle un peso específico a cada una de las partes que serán evaluadas; su objetivo es tratar de compensar el valor que les asignamos a las actividades o tópicos que tienen poca importancia en la evaluación, en relación con los que tienen mayor importancia.

Esta técnica de evaluación permite equilibrar las posibles descompensaciones que existen entre las áreas o sistemas computacionales que tienen mayor peso e importancia y las áreas o sistemas que tienen poco peso e importancia en la evaluación. Lo que se busca con la ponderación es que todas las áreas tengan un valor similar, respetan-

do en cada caso el peso e importancia representativos que tienen para el sistema computacional o para todo el centro de cómputo.

Para un mejor entendimiento de esta técnica, a continuación presentaremos un breve ejemplo cotidiano de una ponderación y seguiremos con otro ejemplo gráfico y haremos un breve análisis de la utilidad de esta herramienta:

Ejemplo gráfico de una evaluación de sistemas

Primer paso. En la columna 1 se anotan las áreas o aspectos de sistemas que serán evaluados, y en la columna 2 se establece un peso porcentual específico para cada factor; el auditor establece ese peso a su libre albedrío (vea el cuadro 1).

En este primer paso se eligen los factores más importantes que se van a evaluar (los de mayor jerarquía o los que pueden ser representantes de un grupo o sector), a fin de darle a cada uno de esos factores un valor porcentual (peso específico), el cual representará la importancia de ese factor en la evaluación. La suma total de los factores primarios siempre debe ser 100% (columna 3).

Cuadro 1

Columna 1	Columna 2	Columna 3
Factores primarios que serán ponderados	**Peso por factor**	**Valor % específico**
Evaluación de la gestión informática del centro de cómputo		**100%**
1. Objetivos del centro de cómputo	10%	
2. Estructura de organización	10%	
3. Funciones y actividades	15%	
4. Sistema de información	20%	
5. Personal y usuarios	15%	
6. Documentación de los sistemas	2%	
7. Actividades y operación del sistema	14%	
8. Configuración del sistema	4%	
9. Instalaciones del centro de cómputo	10%	
Peso total de la ponderación	100%	

Segundo paso. A cada uno de los factores elegidos como primarios se le designan actividades específicas que contribuyan a su evaluación total; en el ejemplo (cuadro 2), al factor primario 1 (Objetivos del centro de cómputo) se le agregan las actividades que pueden ayudar a evaluarlo (columna 1). De la misma manera, a cada una de las actividades señaladas se le da un peso específico (porcentual), el cual representará la importancia que tiene esa actividad dentro del factor primario (columna 2).

El total de esas actividades también debe sumar 100%, pero sólo dentro del grupo al cual pertenecen (objetivos del centro de cómputo).

También se le asignaron valores específicos (columna 2) a cada una de las actividades del factor primario indicado como número 1, el cual tiene un valor específico de 10% (columna 1). En el ejemplo se manejan los siguientes valores para cada actividad, y la suma total de esos valores es 100%:

- Establecimiento del objetivo general 25%
- Cumplimiento del objetivo general 30%
- Difusión del objetivo general 20%
- Derivación de objetivos secundarios 15%
- Seguimiento y control de objetivos 10%

Además, estos porcentajes se pueden hacer comparativos y asignar a cada actividad un peso ponderado (columna 3), el cual es el valor porcentual que la representa, en relación con el peso específico del factor primario. En este caso, ya que al factor primario se le asignó el valor de 10%, entonces cada uno de sus componentes representará un peso ponderado.

Siguiendo el mismo ejemplo tenemos lo siguiente: a la difusión del objetivo general se le asignó 20% y esto representa un valor ponderado de 2% (columna 3) en relación con el valor total de este punto (columna 4).

Cuadro 2

Columna 1	Columna 2	Columna 3	Columna 4
Actividades que van a ser evaluadas y ponderadas	**Peso por actividad**	**Peso por factor ponderar**	**Valor de ponderación**
1. Objetivos del centro de cómputo			**10.0%**
Establecimiento del objetivo general	25%	2.5%	
Cumplimiento del objetivo general	30%	3.0%	
Difusión del objetivo general	20%	2.0%	
Derivación de objetivos secundarios	15%	1.5%	
Seguimiento y control de objetivos	10%	1.0%	
Total del factor a ponderar	100%	10.0%	

A continuación presentamos la tabla de ponderación completa, tomando en cuenta los factores primarios indicados en el primer paso. Notemos que la suma de las actividades de cada factor siempre resultará 100% (columna 2) y que el valor ponderado (columna 3) representará el valor total de cada punto (columna 4).(*)

* Los valores porcentuales que presentamos aquí son arbitrarios, elegidos por preferencia y sólo como un ejemplo. En la práctica, el auditor responsable de la auditoría deberá asignar tanto los factores primarios que va a evaluar, como el valor que le asignará a cada factor. Además, también debe elegir las actividades y asignarles el valor que representen para cada uno de esos factores primarios.

Cuadro 3

Columna 1	Columna 2	Columna 3	Columna 4
Actividades que van a ser evaluadas y ponderadas	**Peso por actividad**	**Peso por factor ponderar**	**Valor de ponderación**
1. Objetivos del centro de cómputo			10.0%
Establecimiento del objetivo general	25%	2.5%	
Cumplimiento del objetivo general	30%	3.0%	
Difusión del objetivo general	20%	2.0%	
Derivación de objetivos secundarios	15%	1.5%	
Seguimiento y control de objetivos	10%	1.0%	
Total del factor a ponderar	100%	10.0%	
2. Estructura de organización			10.0%
Definición de estructura de organización	25%	2.5%	
Definición de funciones	25%	2.5%	
Descripción de puestos	20%	2.0%	
Definición de canales de comunicación	10%	1.0%	
Definición de niveles de autoridad	10%	1.0%	
Actualización de estructuras y puestos	5%	0.5%	
Evaluación periódica de funciones	5%	0.5%	
Total del factor a ponderar	100%	10.0%	
3. Funciones y actividades			15%
Definición de funciones	20%	3.0%	
Cumplimiento de las funciones	30%	4.5%	
Manuales e instructivos	10%	1.5%	
Métodos y procedimientos	15%	2.25%	
Cumplimiento de actividades	20%	3.0%	
Seguimiento de actividades	5%	0.75%	
Total del factor a ponderar	100%	15.00%	
4. Sistema de información			20%
Definición del sistema (software)	30%	6.0%	
Definición del equipo (hardware)	30%	6.0%	
Definición de instalaciones	15%	3.0%	
Evaluación de adquisiciones	10%	2.0%	
Interrelación de funciones	15%	3.0%	
Total del factor a ponderar	100%	20.0%	
5. Personal y usuarios			15%
Manejo del sistema	25%	3.75%	

Continúa

Continuación

Aprovechamiento del sistema	15%	2.25%	
Oportunidad en la información	10%	1.50%	
Asesoría interna a usuarios y personal	15%	2.25%	
Asesoría externa a personal del área	15%	2.25%	
Capacitación y desarrollo del personal	10%	1.50%	
Administración de prestaciones	10%	1.50%	
Total del factor a ponderar	100%	15.00%	
6. Documentación de los sistemas			2%
Manual de usuarios	30%	0.6%	
Manual técnico del sistema	40%	0.8%	
Manuales de capacitación	20%	0.4%	
Actualización de manuales	10%	0.2%	
Total del factor a ponderar	100%	2.0%	
7. Actividades y operación del sistema			14%
Definición del equipo (hardware)	30%	4.2%	
Definición de instalaciones	30%	4.2%	
Evaluación de adquisiciones	20%	2.8%	
Interrelación de funciones	20%	2.8%	
Total del factor a ponderar	100%	16.0%	
8. Configuración del sistema			4%
Definición del equipo (hardware)	25%	1.0%	
Definición del equipo (software)	25%	1.0%	
Adaptación de instalaciones	15%	0.6%	
Adaptación del medio ambiente	15%	0.6%	
Planes contra contingencias	20%	0.8%	
Total del factor a ponderar	100%	4.0%	
9. Instalaciones del centro de cómputo			10%
Adaptación de instalaciones	30%	3.0%	
Adaptación de medidas de seguridad	30%	3.0%	
Adaptación del medio ambiente	10%	1.0%	
Adaptación de las comunicaciones	20%	2.0%	
Mantenimiento del sistema	10%	1.0%	
Total del factor a ponderar	100%	10.0%	

En el punto número 6, Documentación de los sistemas, el valor ponderado del factor es 2.0% y los valores para cada una de sus actividades son: 30%, 40%, 20% y 10%, lo cual nos da un total de 100% (columna 2); mientras que el porcentaje del valor ponderado del factor es: 0.6%, 0.8%, 0.4% y 0.2%, respectivamente (columna 3).

Para el cálculo se aplica una regla de tres simple: si 2 es igual a 100%, ¿cuánto representará 30%? Se aplica la fórmula:

(2.0 * .30)/100 = .06, lo cual equivale a 0.6% del valor total de este factor.

Tercer paso. Se aplica esta guía de evaluación y se registran las calificaciones adjudicadas para cada una de las actividades propuestas (columna 5). Después, con esos resultados se obtienen los puntos alcanzados para cada actividad y para el total por cada factor primario (columna 6). Esto permite comparar los resultados con los valores establecidos inicialmente para cada actividad y emitir un juicio sobre su cumplimiento.

Veamos el ejemplo del cuadro 4 para el punto 6, **Documentación de los sistemas**.

Cuadro 4

Columna 1	Columna 2	Columna 3	Columna 4	Columna 5	Columna 6
Actividades que van a ser evaluadas y ponderadas	**Peso por actividad**	**Peso por ponderar**	**Valor de ponderación**	**Calificación**	**Porcentaje de puntos obtenidos**
6. Documentación de los sistemas			2.0%		
Manual de usuarios	30%	0.60%		.60	.36%
Manual técnico del sistema	40%	0.80%		.85	.68%
Manuales de capacitación	20%	0.40%		1.00	.40%
Actualización de manuales	10%	0.20%		.85	.17%
Total del factor a ponderar	100%	2.00%		.825	1.61%

Como podemos observar en el cuadro 4, el auditor asigna una calificación a cada actividad (columna 5), y con ella emite un criterio (cualitativo o cuantitativo) para evaluar el grado de cumplimiento de dicha actividad. Éste es un valor numérico, el cual representa la calificación que el auditor le otorga a cada uno de esos puntos de acuerdo con su desempeño. El total del factor a ponderar, se calcula sumando los valores y el resultado se divide entre el número de líneas.

El auditor debe establecer el criterio para evaluar el cumplimiento de cada uno de los puntos de esta guía de ponderación, según las herramientas, técnicas y demás procedimientos de auditoría que utilice. El valor más alto se otorga cuando no existen fallas o cuando el punto evaluado cumple totalmente con lo establecido. El valor desciende cuando el punto evaluado no cumple totalmente con lo establecido, y entre menos cumpla, más desciende.

Después de asentar esas calificaciones, el auditor hace el cálculo del porcentaje de puntos obtenidos por cada actividad (columna 6), el cual será el resultado de multiplicar el valor del peso ponderado (columna 3) por la calificación obtenida (columna 5). El resultado, en decimales, es el valor porcentual del grado de cumpli-

miento de cada actividad. Al final, el auditor obtiene el promedio aritmético de esa columna y lo anota.*

Cuarto paso. Después de haber obtenido las calificaciones y los valores de toda la guía de ponderación (columna 5), así como el porcentaje de los puntos obtenidos (columna 6), el responsable de la auditoría debe realizar un análisis profundo sobre cada uno de los resultados y valorar el grado de cumplimiento de cada una de las actividades. Es recomendable adoptar un criterio uniforme para calificar de la misma manera todos los puntos evaluados.

Para explicar esto utilizaremos resultados hipotéticos en el punto 8, Configuración del sistema; así encontraremos los siguientes valores para la calificación (columna 5) y el cálculo del porcentaje de los puntos obtenidos (columna 6). El criterio de calificación que utilizaremos es el siguiente:

Excelente 1.00% (para el cumplimiento más alto)
Bueno 0.80 (para un cumplimiento bueno sin llegar a ser excelente)
Regular 0.60 (para un cumplimiento mínimamente aceptable)
Deficiente 0.40 (para un cumplimiento malo y mucho peor de lo esperado)
Pésimo 0.20 (para el "incumplimiento" francamente desastroso)

Una vez obtenidas las calificaciones, promedios y sumas de cada uno de los factores, se comparan los resultados de cada factor con su peso específico. El propósito es que el auditor tenga un criterio numérico mediante el cual pueda tener los parámetros para comparar el grado de cumplimiento alcanzado por cada factor con el grado de cumplimiento esperado.

Cuadro 5

Columna 1	Columna 2	Columna 3	Columna 4	Columna 5	Columna 6
Actividades que van a ser evaluadas y ponderadas	Peso por actividad	Peso por ponderar	Valor de ponderación	Calificación	Porcentaje de puntos obtenidos
8. Configuración del sistema			4.0%		
Definición del equipo (hardware)	25%	1.0%		95%	0.95
Definición del equipo (software)	25%	1.0%		95%	0.95
Adaptación de instalaciones	15%	0.6%		80%	0.48
Adaptación del medio ambiente	15%	0.6%		50%	0.30
Planes contra contingencias	20%	0.8%		10%	0.08
Total del factor a ponderar	100%	4.0%		66%	2.6

* Algunas veces, por los resultados de las multiplicaciones, se pueden obtener resultados que no coinciden aritméticamente, como en el caso de este ejemplo, en donde la suma de la columna 6 nos da por resultado 1.61. Mientras que, si multiplicamos el valor del total ponderado de la columna 5 (2.0 por 8.25) el resultado es 1.65; la diferencia 0.04 no es significativa y se puede anotar el valor que más crea conveniente el auditor. Lo importante es la evaluación que se debe hacer de ese valor. Como se indica en el cuarto paso.

Como podemos observar, el total es un poco más que regular, **2.64% alcanzado en comparación con 4.0% del total esperado de este factor** (apenas se obtuvo 66% en comparación con 100% del esperado); esto nos haría juzgar que el cumplimiento de la configuración del sistema es mínimamente aceptable. Sin embargo, esto no es lo real ni tampoco lo más justo. Sería muy arbitrario e injusto calificar el cumplimiento del 95% de los dos primeros puntos (definición del hardware y definición del software) con 66% (cada uno de ellos casi alcanza el más alto cumplimiento); tampoco es nada equitativo "premiar" 10% del último; se esperaba .8% y sólo alcanzó 0.08% (éste no alcanza ni el cumplimiento mínimo señalado en la tabla).

En el ejemplo vemos que al factor Planes contra contingencias se le concede nulo o muy poco valor.

Por eso es muy útil esta guía de ponderación, ya que permite evaluar, lo más objetivamente posible, los resultados obtenidos en una auditoría, elegir los factores primarios que serán evaluados, las actividades que serán evaluadas en cada uno de ellos, así como darles un peso específico equitativo a todos esos factores. También permite hacer una verdadera valoración del grado de cumplimiento de cada factor y cada actividad.

Conviene indicar que esta técnica se puede aplicar en todo el ámbito de sistemas o en cada uno de los aspectos de sistemas que deban ser evaluados. Dicha aplicación se hará de acuerdo con las necesidades de la evaluación.

11.3 Modelos de simulación

Esta herramienta es una de las más utilizadas para el análisis y diseño de sistemas, pero también puede ser de mucha utilidad para la auditoría de sistemas computacionales, ya que mediante el uso de un modelo, conceptual o físico, se simula el comportamiento de un sistema computacional, de un programa, de una base de datos, de una operación, de una actividad o de cualquier tarea de sistemas que tenga que ser revisada, con el propósito de investigar cuál es, fue o será el comportamiento del fenómeno de sistemas en estudio, bajo ciertas condiciones y características concretas, en las que se presentan todas las simulaciones necesarias que se asemejen al medio ambiente real en donde actúa dicho fenómeno para valorar su auténtico aprovechamiento, sus eficiencias y deficiencias de funcionamiento, sus principales problemas, etcétera.

El uso de esta técnica de simulación es indispensable para el trabajo de los desarrolladores de nuevos sistemas, ya que permite elaborar un ambiente análogo al del nuevo sistema, con el fin de estudiar su posible comportamiento. Una vez estudiado el posible comportamiento del sistema, se pueden sacar conclusiones para corregir sus fallas de funcionamiento, así como sus principales problemas antes de implantar dicho sistema. De hecho, todos los analistas de sistemas utilizan modelos conceptuales antes de programar (codificar) un sistema computacional, mientras que los programadores elaboran su programación con base en estos modelos.

En el caso concreto de auditoría de sistemas computacionales, la simulación es la elaboración de modelos, conceptuales o físicos, muy similares a los sistemas institucionales de las empresas; inclusive pueden ser los mismos que éstas utilizan actualmente. Muchos se prueban con bases de datos ficticias o con datos reales pero sin validez.

El auditor hace pruebas en esos modelos de simulación, para verificar el comportamiento y funcionamiento de los sistemas computacionales, la forma en que se realiza el procesamiento de datos, la emisión de informes, la captura de datos o cualquier otro aspecto de dichos sistemas.

Esta simulación se puede hacer para evaluar cualquier fenómeno de sistemas computacionales, lo mismo para el análisis, diseño y programación de sistemas, para la instalación y liberación de un nuevo sistema, o para evaluar el comportamiento de las bases de datos, el comportamiento del hardware, el mobiliario y equipo, el diseño e instalación de una red de cómputo o cualquier otro aspecto de sistemas.

Incluso en el ambiente de seguridad se utiliza esta herramienta para hacer simulacros de alguna posible contingencia, con el propósito de capacitar al personal para que sepa cómo actuar en caso de siniestros. Los simulacros más comunes en una empresa son: simulacros de evacuación, de recuperación de archivos, de primeros auxilios, simulacros para combatir incendios, etcétera.

A continuación presentamos algunas definiciones de esta herramienta, con el fin de entender mejor su utilidad:

Simular

*"Del latín **simular**, de **similis**: Semejante. Aparentar, fingir."*[10]

Simulacro

"Imagen hecha a semejanza de una cosa [...] Cosa que forma la fantasía. Ficción, imitación, falsificación."[11]

Modelo

"Lo que se sigue, imita o reproduce [...] Representación en pequeño de una cosa. Ejemplar perfecto, digno de ser imitado."[12]

Para el caso de una auditoría de sistemas computacionales, definiremos la simulación de la siguiente manera:

> *La imitación formal del sistema computacional, mediante un modelo simulado, en cuanto al funcionamiento del hardware, software, información, instalaciones o aplicaciones, en la cual se representan sus principales características de operación, forma de captura, procesamiento de datos y emisión de resultados del sistema original, con el propósito de estudiar el comportamiento del sistema y evaluar su funcionamiento real. En estos modelos se pueden aplicar datos ficticios o datos reales, pero sin que esta simulación llegue a influir en la actividad normal del sistema original.*

El uso de modelos para la simulación es una de las principales formas de evaluación del funcionamiento de un sistema computacional, ya que permiten aplicar pruebas de su comportamiento, sin afectar su operación normal. Lo mismo sucede cuando se aplican para simular la operación de los sistemas computacionales, el acceso, manejo y protección de las bases de datos, el uso del software, hardware, datos, equipos e instalaciones, alguna contingencia de sistemas o cualquier otro tipo de pruebas que permitan imitar el funcionamiento del sistema original, con el propósito de compararlo con el sistema simulado.

Con dichas comparaciones se pueden sacar conclusiones importantes, sin afectar la operación normal de los sistemas de la empresa; además, estas simulaciones también ayudan a vislumbrar las posibles problemáticas del sistema computacional, sin afectar el funcionamiento del mismo.

Con el uso de modelos concretos o de pruebas de simulación también se pueden evaluar la integridad, seguridad y confiabilidad de la información contenida en las bases de datos originales, así como verificar la existencia de redundancias, alteraciones y comportamientos irregulares de la información contenida en esas bases de datos; además, también se puede simular, por medio de modificaciones controladas en el prototipo del sistema original, el acceso al sistema, la protección del mismo, el ingreso a las bases de datos, e incluso el comportamiento de los usuarios del sistema o el manejo de los datos. En algunos casos, cuando el sistema lo permite y con ello no se alteran sus datos originales, se pueden hacer todo tipo de pruebas de evaluación, ya sean con datos ficticios o con datos reales del sistema.

Si las pruebas de simulación lo requieren, se pueden hacer alteraciones controladas del funcionamiento normal del sistema, para medir el comportamiento y conducta de los datos, la operación o cualquier otro aspecto del sistema que se quiera evaluar. Tal y como se sugiere en la técnica de observación (sección 9.4 del capítulo 9), sólo que en lugar de aplicar la observación ahí señalada, aquí se realizan simulaciones del comportamiento o del medio ambiente del sistema con modelos similares al original.

Debemos señalar que el auditor responsable de la auditoría debe supervisar estrictamente la aplicación de esta herramienta, e incluso debe tomar las medidas preventivas, de seguridad y de control necesarias para salvaguardar la información antes de aplicar cualquier prueba o simulacro al sistema, con el propósito de contar con un respaldo del sistema original, por si su funcionamiento se llegara a alterar debido a las pruebas que se le realicen. La importancia de la simulación radica en que se pueden confeccionar pruebas controladas o libres que permiten realizar una buena evaluación al sistema, sin necesidad de alterar el funcionamiento del sistema original. En este tipo de observación se pueden hacer las pruebas en sistemas paralelos; uno es el propio sistema con datos reales o ficticios y el otro es un modelo semejante al sistema que será evaluado. Estas pruebas en sistemas paralelos se realizan con el propósito de comparar ambos resultados y, si es necesario, modificar la conducta del modelo para cotejarlo con el sistema original. Con los resultados se puede obtener información muy valiosa para emitir conclusiones sobre el comportamiento de ambos.

11.3.1 Simulación a través de modelos de metodología de sistemas

Debido a que existen muchos modelos de simulación para evaluar el comportamiento de un sistema, únicamente citaremos algunos; el propósito es ejemplificar las posibles aplicaciones de los modelos que se pueden utilizar como apoyo en la evaluación de sistemas. Asimismo, solamente presentaremos las principales etapas y fases de estas metodologías, sin entrar en mayores detalles, ya que cada desarrollo de sistemas es especial y sería irrelevante señalar ejemplos específicos para cada caso.

11.3.1.1 Ciclo de vida de los sistemas

Este modelo, también conocido como el ciclo de vida tradicional de los sistemas, es el que más se utiliza para el desarrollo de sistemas computacionales, ya que es considerado como la metodología fundamental y puede contener variaciones menores dentro de las fases que citaremos a continuación, siempre y cuando se conserven dentro del esquema que presentaremos:

- *Análisis del sistema actual*
- *Diseño conceptual del sistema*
- *Diseño detallado del sistema*
- *Programación*
- *Pruebas y correcciones*
- *Implantación del sistema*
- *Liberación del sistema*
- *Mantenimiento del sistema*

11.3.1.2 Metodología de Kendall & Kendall[13]

Los desarrolladores de sistemas computacionales tienen que utilizar forzosamente la metodología de estos autores, considerada como clásica para el análisis y diseño de los sistemas computacionales, ya que se aplica fácilmente y es muy completa. Los propios autores presentan las siete fases del desarrollo de sistemas, las cuales presentamos a continuación:

- *Identificación de problemas, oportunidades y objetivos*
- *Determinación de requerimientos de información*
- *Análisis de las necesidades del sistema*
- *Diseño del sistema recomendado*
- *Desarrollo del sistema*
- *Pruebas y mantenimiento de sistemas*
- *Implementación y evaluación del sistema*

11.3.1.3 Fases del desarrollo, según James Martín[14]

Antonio López-Fuensalida resume con gran acierto esta metodología de Martín, y también las de otros autores, en la cual presenta su método de desarrollo de sistemas como preámbulo; por esta razón tomaremos como válidos estos resúmenes de fases en el desarrollo de sistemas con herramientas CASE.*

- Planeación estratégica
  - *Marco del sistema*
  - *Funciones*
  - *Objetivos*
- Plan del sistema
  - *Procedimientos*
  - *Datos*
- Análisis
- Diseño
- Construcción
- Implantación
- Mantenimiento
- Reingeniería

11.3.1.4 Ciclo de vida de los sistemas, según Yourdon[15]

El mismo autor cita las aportaciones de Yourdon en tres grandes niveles: Conceptual, Lógico y Físico, y dentro de cada uno de ellos señala las fases de desarrollo de la siguiente manera:

- Nivel conceptual
  - *Especificaciones*
- Nivel lógico
  - *Análisis lógico*
- Nivel físico
  - *Diseño físico*
  - *Implantación*
  - *Mantenimiento*

11.3.1.5 Análisis y diseño, según Jackson

El mismo autor conceptualiza las aportaciones de Jackson en tres grandes etapas: Análisis conceptual, Diseño externo y Diseño interno, y coloca otras dentro de cada fase conforme al siguiente modelo:

* Computer Aided Software Engineering: Ingeniería de Software Asistida por Computadora.

- *Análisis conceptual*
- Especificaciones del modelo de la realidad
  - *Identificar entidades y relaciones*
  - *Definir estructura de las entidades*
  - *Crear modelo inicial*
- *Diseño exterior*
- Especificación de funciones de la aplicación
  - *Añadir funciones del modelo*
  - *Determinar momentos de Ejecución*
- *Diseño interior*
- Implementación
  - *Implementar el modelo*

11.3.1.6 Las fases de un proyecto para MERICE[16]

López-Fuensalida cita las cuatro etapas para el desarrollo de proyectos informáticos y dentro de cada etapa propone fases para elaborar un proyecto:

- *Etapa 1: Estudio preliminar*
  - Fase 1: Recogida de datos
    - *Recogida inicial*
    - *Estudio de la situación actual*
    - *Síntesis y crítica de la situación actual*
  - Fase 2: Concepción de la nueva solución
    - *Objetivos a alcanzar*
    - *Descripción de soluciones*
  - Fase 3: Evaluación y plan de desarrollo de las fases
    - *Evaluación de la nueva solución*
    - *Plan de desarrollo*
- *Etapa 2: Estudio detallado*
  - Fase 1: Concepción general
  - Fase 2: Concepción detallada de fases
    - *Realización de las especificaciones detalladas de los procesos*
  - Fase 3: Plan de desarrollo
- *Etapa 3: Realización*
  - Fase 1: Estudio técnico
  - Fase 2: Producción

- *Etapa 4: Puesta en marcha*
  - Fase 1: Preparación de recursos
  - Fase 2: Recepción y lanzamiento de sistemas

11.3.1.7 Metodología SSADM**

"La metodología consiste en una estructuración de los pasos a seguir en el desarrollo de un proyecto informático en las fases iniciales del ciclo de vida del mismo y en la descripción de unas técnicas y formalismos sobre las que se basan los trabajos para realizar cada fase [...]"[17]

Esta metodología contiene una estructuración jerárquica de fases, tal y como se indica en el siguiente esquema (figura 11.2):

Figura 11.2 *Esquema de estructuración jerárquica*

A su vez, estos puntos se contemplan dentro de las siguiente fases:

- Fase 1: Estudio de viabilidad
  - *Etapa 01: Definición del problema*
  - *Etapa 02: Identificación del proyecto*
- Fase 2: Análisis
  - *Etapa 1: Análisis del sistema actual*
  - *Etapa 2: Especificación de requerimientos*
  - *Etapa 3: Selección de opciones técnicas*
- Fase 3: Diseño
  - *Etapa 4: Diseño de datos*
  - *Etapa 5: Diseño de procesos*
  - *Etapa 6: Diseño físico*

** (Structured System Analysis and Design Method *(Método de Análisis y Diseño Estructurado de Sistemas)*.

Después de que el estudio de viabilidad es aprobado, las etapas se realizan cronológicamente conforme al siguiente proceso (ver figura 11.3):

1. Análisis del sistema actual
2. Especificación de requerimientos
3. Selección de opciones técnicas
4. Diseño de datos
5. Diseño de procesos
6. Diseño físico

El siguiente modelo de entidad/relación también se puede aplicar para el diseño de las bases de datos (ver la figura 11.3):

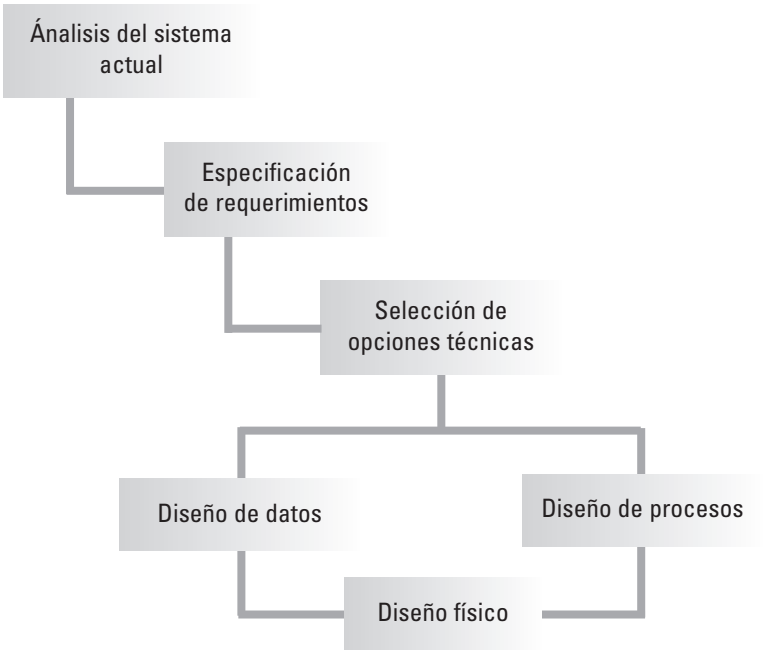


Figura 11.3 *Modelo de entidad*

11.3.2 Simulación a través de diagramas de flujo de sistemas

En este tipo de simulaciones se utilizan diagramas con símbolos universalmente aceptados, los cuales tienen un significado específico y determinado previamente por convención, a fin de que todos los entiendan de la misma forma.

A continuación mostraremos un ejemplo de este tipo de modelos, el cual es un diagrama de flujo para programación BASIC; debemos señalar que en este capítulo también trataremos la diagramación, ya que es una de las técnicas especiales de auditoría de sistemas computacionales:

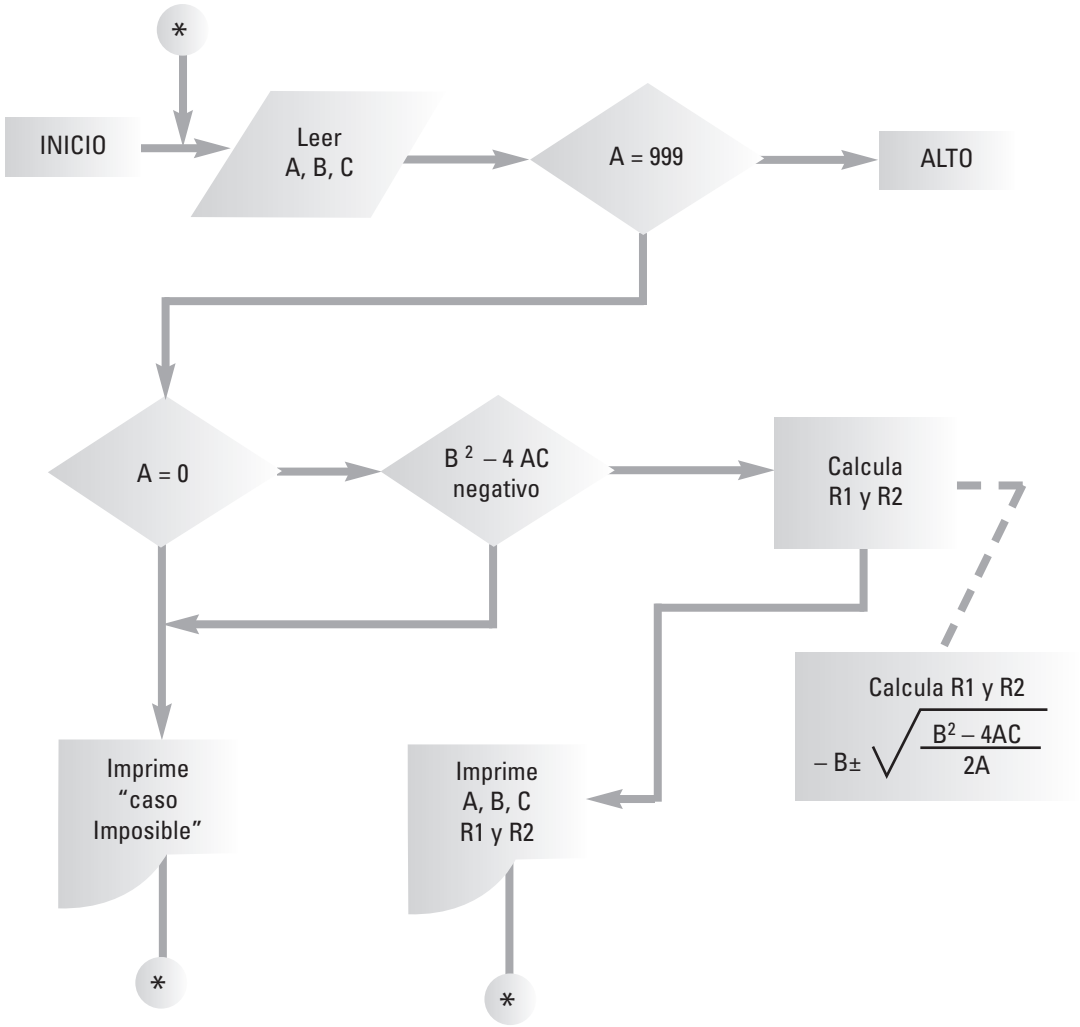


Figura 11.4

11.3.3 Simulación a través del diseño de circuitos lógicos

Éstos son diagramas de conexiones de circuitos lógicos, los cuales nos muestran gráficamente como se solucionan los problemas de redes lógicas combinatorias de salida o entrada, establecidos a través de operaciones matemáticas con álgebra booleana. Esta técnica se utiliza principalmente para simular representaciones analógicas de una computadora, de sus circuitos y de sus operaciones mediante el álgebra booleana. En este ejemplo se ven las soluciones de una suma X = A + B + C y la tabla donde se presentan todos los posibles resultados de estos circuitos. (ver figura 11.4)

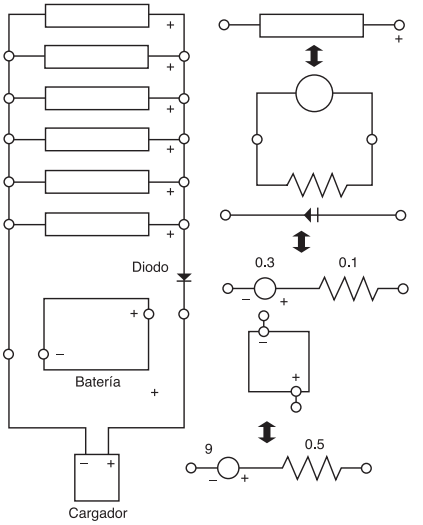


Figura 11.5

En el siguiente ejemplo se toma el diagrama de los teoremas booleanos[18] del autor Ronald J. Tocci, con el único propósito de mostrar el uso de este tipo de modelos de circuitos lógicos:

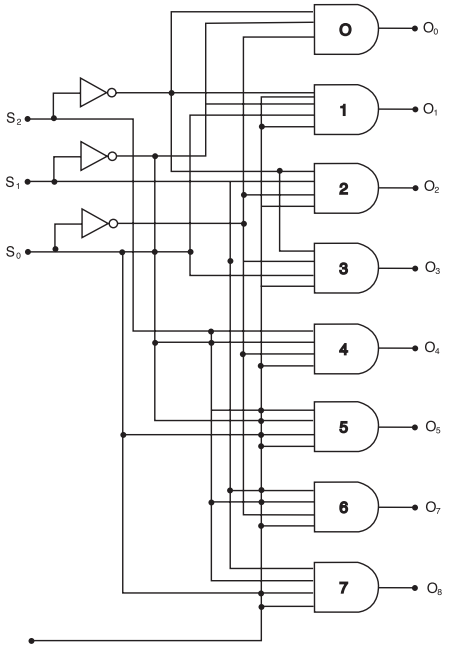


Figura 11.6

11.3.4 Simulación a través de otros documentos gráficos

Es evidente que se puede utilizar un sinnúmero de modelos gráficos, conceptuales o físicos para simular el comportamiento de un sistema computacional; incluso los planes, diagramas de planeación y control de proyectos, así como otros documentos de apoyo para la gestión administrativa se pueden tomar como ejemplos de modelos de simulación utilizables en una auditoría de sistemas computacionales; por esta razón, a continuación mencionaremos únicamente algunos de los posible modelos de sistemas que se pueden utilizar para simular el comportamiento de cualquier fenómeno de sistemas computacionales que se desee evaluar:

- Modelos para planeación y control de proyectos:
  - Gráfica de Gantt
  - Método de la ruta crítica
  - Pert costo/tiempo
  - Project
  - Gráficas de proyecciones financieras
  - Gráficas de líneas de tiempo
  - Tablas de decisiones
  - Árboles decisionales
- Modelos de simulación de flujos de datos
  - Diagrama de flujo de datos
  - Diagrama entidad/relación
  - Diagrama de contexto
  - Diagrama de datos lógicos
  - Diagrama de datos físicos
  - Diseño de bases de datos
  - Diagrama de modelos de datos
  - Diagramas HIPO (tabla visual de contenido VTOC, diagramas de panoramas y diagramas de detalles)
  - Diagramas de códigos (seudocódigos)
  - Gráficas Nassi-Shneiderman
  - Diagramas Warnier-Orr
  - Gráficas de estructura de datos
  - Gráficas de configuraciones de red
  - Gráficas de configuración de sistemas distribuidos
  - Gráficas de Configuraciones de equipos mayores
- Modelos de simulación de diagramas administrativos
  - Organigramas
  - Diagramas de métodos y procedimientos
  - Gráficas de tiempos y movimientos

  - Estudios ergonómicos
  - Planos de distribución de la planta
  - Planos de instalaciones
  - Planos de rutas de evacuación
  - Planos de configuración de centros de cómputo
- Modelos de simulación por medio de gráficas financieras y estadísticas
  - Curvas de tendencias
  - Gráficas de Pie, horizontales, verticales, de área, circulares y semicirculares
  - Gráficas de punto de equilibrio
- Otros modelos de simulación
  - Gráficas de pantalla
  - Planes de contingencia informática
  - Digitalización de imágenes
  - Procesamiento de datos ficticios

Evidentemente existen muchos más modelos que se pueden utilizar para simular el comportamiento de los sistemas en evaluación, pero la intención es destacar la importancia de utilizar los modelos de simulación en una auditoria de sistemas computacionales.

Para finalizar este punto, a continuación veremos las siguientes definiciones.

Modelo

"La duplicación de la realidad empírica o de una teoría científica con la cual guarda igualdad de formas (isomorfía), sus fines son diagnósticos explicativos y preventivos."[19]

"Representación simplificada o esquemática de un fenómeno o proyecto en el cual incluye sus variables más significativas. También puede significar una imitación o patrón de comportamiento que simula casos reales."[20]

"La construcción de un modelo es una técnica común para el estudio de las características o aspectos de la conducta de los objetos o sistemas bajo condiciones variables. En sí mismo, el modelo es generalmente una representación de objetos, eventos, procesos o sistemas y su uso es para la predicción y el control."
"Es la imitación matemática o física de un sistema real."[21]

11.4 Evaluación

La evaluación es una de las técnicas más comunes en cualquier tipo de auditoría y es considerada como la herramienta típica para auditar cualquier actividad, ya que permite determinar, mediante pruebas concretas, si lo cuantificado (o cualificado) es lo que se esperaba obtener de lo que se está evaluando; así se determina si se está cumpliendo con la actividad revisada, conforme a lo que se esperaba de ella. En esta téc-

nica se aplica el principio fundamental del control: establecer parámetros de medición, recopilación de información y comparación de lo realmente alcanzado con lo planeado, y con el resultado obtenido se hace una retroalimentación de los resultados de esta evaluación.

Esta técnica se aplica fácilmente mediante los siguientes pasos y requiere de poco trabajo:

- *El establecimiento anticipado de ciertos parámetros o relaciones de carácter cualitativo, a los cuales se les asigna un cierto valor numérico, matemático, estadístico, contable o de cualquier otro tipo (casi siempre en forma porcentual). Supuestamente, el valor más alto será el nivel óptimo de la operación y el menor el más deficiente.*
- *Mediante distintas pruebas y herramientas de auditoría se procede a recopilar la información y se asigna un puntaje, el cual será el que alcance el aspecto de sistemas computacionales en evaluación, según sus resultados.*
- *El valor obtenido en el paso anterior se compara con el valor esperado (otro cierto valor ideal), el que supuestamente deberá cumplir la actividad que en evaluación.*
- *Después de hacer la comparación se sacan conclusiones para valorar el grado de cumplimiento del sistema que está siendo auditado.*
- *Finalmente se procede a elaborar el informe sobre los resultados obtenidos.*

Esto mismo se realizará cuando se trate de una evaluación cualitativa, en donde los valores serán de carácter subjetivo, tales como excelente, bueno, deficiente, sí cumple, cumple parcialmente o cualquier otro valor cualitativo, siempre que sea útil para comparar lo realmente alcanzado con lo que se esperaba alcanzar.

En ambos casos, evaluación de carácter cuantitativo o cualitativo, el resultado será determinado por la posible diferencia que se encuentre entre el valor esperado y el valor obtenido mediante las pruebas de auditoría que se hayan utilizado. Después se continua con la retroalimentación, a través de la elaboración y presentación del informe para su valoración y solución.

Como es costumbre, a continuación presentaremos las definiciones más características de esta evaluación, a fin de conceptualizar mejor su aplicación.

Evaluación

"Proceso de comparación entre valores observados y valores esperados establecidos previamente desde un punto de vista."[22]

"Análisis crítico para determinar la eficiencia de una persona o la efectividad de una actividad específica, en base a parámetros establecidos, con el propósito de detectar las causas de las variaciones y definir las posibles medidas correctivas."[23]

Evaluar

*"Del latín derivado **valere**: Valer. Tasar, justipreciar."*[24]

"Señalar el valor de una cosa. Calcular el valor que debe tener."[25]

"Parte del proceso de control, que consiste en el análisis crítico de los resultados obtenidos, con respecto a las metas o normas establecidas, con el fin de determinar las causas de las variaciones y definir las posibles medidas correctivas."[26]

Valorar

"Señalar precio a una cosa. Atribuir determinado valor o estima a persona y cosas. Hacer que aumente de valor una cosa [...]"[27]

Valor

"Grado de calidad, mérito, utilidad, virtud o precio que tienen personas o cosas. Significación y alcance de algo [...] Precio equivalente de una cosa [...]"[28]

Valorización del desempeño

"Métodos de observación y disposición de carácter uniforme y general, a través de los cuales se estima el trabajo de cada empleado."[29]

Después de ver las definiciones anteriores, entenderemos como evaluación lo siguiente:

> *Acción mediante la cual el auditor de sistemas computacionales obtiene los resultados del desempeño alcanzado de una función, actividad, tarea u operación y los compara con los resultados esperados, con el propósito de valorar su grado de cumplimiento y poder así retroalimentar dichos resultados a través de un informe, para incrementar la eficiencia del desempeño alcanzado.*

Podemos decir que la evaluación es una de las herramientas de mayor utilidad para el auditor de sistemas computacionales, debido a que ayuda a comparar el funcionamiento actual de un sistema computacional con su funcionamiento esperado, a fin de valorar el grado de cumplimiento de sus funciones, actividades y operación; con esos resultados, el auditor estará en posibilidades de retroalimentar al responsable del sistema, para coadyuvar a que sus acciones sean efectivas. Lo mismo se realiza con las funciones del área de sistemas, de un directivo, de los empleados o de los usuarios; es decir, se compara su cumplimiento actual con lo esperado de ellos. Lo más importante es, mediante alguna de las técnicas de recopilación, obtener los resultados de su desempeño actual (o pasado) y examinarlos con lo que deberían realizar; con esas observaciones se aprecia el desempeño logrado en comparación con lo esperado y se elabora el informe correspondiente.

A continuación presentaremos los principales tipos de auditoría en donde se aplica la evaluación.

11.4.1 Evaluación de la gestión administrativa del área de sistemas

En estas evaluaciones, el auditor debe apreciar cómo se realizan las acciones de carácter administrativo para cumplir con las funciones encomendadas al área de sistemas de la empresa; el auditor debe procurar contemplar todos los aspectos relacionados con la gestión informática y administrativa de dicho centro para valorar la eficacia y eficiencia de la actividad administrativa de sus directivos, empleados y funcionarios.*

Entre las formas de evaluación de la gestión informática encontramos las siguientes:

11.4.1.1 Evaluación de la actividad administrativa

En esta parte se evalúan los aspectos administrativos del área de sistemas, a través de la comparación de lo esperado en el aspecto puramente administrativo con lo realmente alcanzado en este renglón.

- *Evaluar la existencia y cumplimiento de los planes, programas y presupuestos que afectan al área de sistemas computacionales.*
- *Evaluar la existencia, difusión y cumplimiento de los objetivos institucionales y que los objetivos del área de sistemas computacionales sean acordes a esos objetivos.*
- *Evaluar la existencia, congruencia y apego a la estructura de organización del centro de cómputo, incluyendo la asignación de funciones, la congruencia de los puestos, los niveles y líneas de autoridad, responsabilidad y comunicación formal.*
- *Evaluar la existencia y aplicación del perfil de puestos para la selección y promoción del personal del área de sistemas computacionales, así como la ocupación actual de dicho personal.*
- *Evaluar la división adecuada de trabajo y departamentalización de las funciones y actividades del personal, así como la distribución correcta de cargas de trabajo y que no haya duplicidad de funciones, actividades o puestos.*
- *Evaluar la administración de los recursos humanos asignados al área de sistemas, en cuanto a capacitación, adiestramiento, índices de rotación y ausentismo.*

* El área de sistemas computacionales se ha caracterizado por su aparente desapego al cumplimiento de las funciones administrativas tradicionales de una empresa, ya que muy frecuentemente se da el caso de que se privilegian las acciones técnicas y de cómputo; la mayoría de los responsables de estas áreas omite o posterga las actividades de la gestión administrativa. Por esta razón, el auditor de sistemas encontrará muchas deficiencias en el manejo netamente administrativo; como ejemplo de lo anterior podemos citar la carencia, deficiencia o inexistencia de la planeación y control de actividades, de la elaboración y ejercicio de presupuestos, de la elaboración y seguimiento de planes y programas de capacitación, de las medidas preventivas o correctivas de la rotación de personal o de los planes contra contingencias informáticas, entre muchos otros aspectos administrativos de los cuales carece la mayoría de centros informáticos, salvo muy honrosas excepciones en las que sí se contemplan estos aspectos.

- *Evaluar la existencia y aplicación de la gestión financiera y contable en el manejo de los recursos informáticos del centro de cómputo.*
- *Evaluar la forma en que funcionarios, empleados y usuarios del sistema ejercen la gestión directiva y cumplen con sus funciones y actividades, respectivamente.*
- *Evaluar la forma en que los directivos y jefes del centro de cómputo ejercen su autoridad, sus estilos de mando, su liderazgo y la supervisión.*
- *Evaluar las relaciones personales y de trabajo entre directivos, empleados y usuarios del centro de cómputo y personas ajenas a éste.*
- *Evaluar la suficiencia o carencia de recursos informáticos y de personal para cumplir con las actividades del centro de cómputo.*
- *Evaluar la forma administrativa en que se manejan las requisiciones de hardware, software, mobiliario y equipos de oficina, consumibles y demás implementos del área de sistemas computacionales, e inclusive la forma de realizar la planeación y control de dichas requisiciones.*
- *Evaluar la forma en que se planea, organiza, dirige y controla el desarrollo de proyectos informáticos en el área de sistemas, así como el cumplimiento de la metodología, estándares y lineamientos institucionales para el desarrollo de sistemas.*
- *Evaluar la administración de seguros sobre los sistemas computacionales, la información, el personal y usuarios de sistemas, así como la suficiencia, actualización y vigencia de dichos seguros. Si es el caso, la forma en que se hicieron las posibles reclamaciones para éstos.*
- *Evaluar el estado general de la gestión administrativa del área de sistemas, así como su cumplimiento adecuado para las actividades informáticas en la empresa.*

11.4.1.2 Evaluación en cuanto a la gestión de los sistemas computacionales

En esta parte se evalúa la administración de los proyectos informáticos del área de sistemas; ya sea que se desarrollen en esta área, se adquieran de terceros o se compren ya realizados. Lo importante es evaluar la forma en que se realiza esta función, desde el punto de vista de la administración informática. Entre algunos de los aspectos que tienen que ser evaluados respecto a este punto tenemos los siguientes:

- *Evaluar la administración y el control de proyectos informáticos y si éstos se apegan a los requerimientos, lineamientos, políticas y necesidades de cómputo de la empresa, y evaluar que se cumpla con los estándares para la adquisición del software, hardware, periféricos, redes y codificación de los sistemas, así como con las metodologías institucionales de análisis y desarrollo de sistemas informáticos.*
- *Evaluar la administración de las funciones, actividades y operaciones del centro de cómputo, de los sistemas computacionales, del software, así como la asignación del hardware, periféricos, mobiliario, equipos e instalaciones.*

- *Evaluar la existencia, difusión y aplicación de las medidas y métodos de seguridad y prevención informática, así como de los planes contra contingencias para el área de sistemas.*
- *Evaluar la existencia y cumplimiento de programas para la evaluación y adquisición del hardware, equipos, periféricos, consumibles e instalaciones físicas del sistema.*
- *Evaluar la existencia y cumplimiento de programas para la evaluación y adquisición del software, sistemas operativos, lenguajes, programas y paqueterías de uso institucional, así como su explotación y aplicación en las unidades administrativas y en el propio centro de cómputo.*
- *Evaluar la forma en que se administra y atiende la seguridad en el acceso a las instalaciones, a los sistemas computacionales, a las bases de datos y a la información institucional.*
- *Evaluar la forma en que se proporciona la asistencia y asesoría a los usuarios de los sistemas de la empresa.*

11.4.2 Evaluación del equipo de cómputo

La evaluación del equipo de cómputo es una de las partes fundamentales de la auditoría de sistemas; por esta razón se debe evaluar la forma en que se administra y controla la asignación de funciones y actividades de los sistemas computacionales de la empresa; sean éstos centralizados en un área de sistemas o asignados a cada área de la empresa. También se debe evaluar la manera en que se da el mantenimiento a estos sistemas. Lo anterior se puede realizar llevando a cabo las siguientes evaluaciones.

11.4.2.1 Evaluación del diseño lógico del sistema

Es la evaluación del funcionamiento interno del sistema computacional, en cuanto al manejo de su software, arquitectura y configuración, conforme a las necesidades informáticas de la empresa y de la propia área:

- *Evaluar la forma en que se lleva a cabo la configuración del sistema, equipos, bases de datos y de los archivos de información institucional, así como la documentación de cambios y alteraciones de su funcionamiento original y de las actualizaciones y cambios de equipos, configuraciones y plataformas.*
- *Evaluar si los componentes lógicos corresponden a las características de funcionamiento de los sistemas computacionales de la empresa, así como evaluar la arquitectura, configuración y funcionamiento de dichos sistemas.*
- *Evaluar las características, protocolos y componentes lógicos de las comunicaciones y programas de enlace entre los equipos de cómputo de la empresa, sean éstos internos o externos.*

- *Evaluar que en la empresa existan y se apliquen las metodologías para el desarrollo y adquisición de sistemas computacionales.*
- *Evaluar la administración de los métodos de accesos, seguridad y operación del sistema.*
- *Evaluar la administración de las características lógicas del hardware, software, periféricos, instalaciones y componentes asociados al sistema.*
- *Evaluar la administración de la arquitectura y configuración de redes de cómputo, equipos mayores y monousuarios de la empresa.*
- *Evaluar los componentes, características y construcción de las bases de datos y archivos de información institucional, a fin de verificar que funcionen de acuerdo con las características, costumbres y necesidades de la empresa.*

11.4.2.2 Evaluación del diseño físico del sistema

Así como es importante evaluar el aspecto lógico de los sistemas, también lo es evaluar la administración y control de los componentes físicos de los equipos de cómputo, de acuerdo con las siguientes evaluaciones:

- *Evaluar la forma en que se lleva a cabo la configuración del sistemas, y de sus equipos e instalaciones físicas, así como la documentación de cambios y alteraciones de su funcionamiento original y de las actualizaciones y cambios de equipos, configuraciones y plataformas.*
- *Evaluar si los componentes físicos, periféricos, mobiliario y equipos del sistema se apegan a los estándares y lineamientos establecidos para la función informática de la empresa.*
- *Evaluar las características y peculiaridades de los sistemas, periféricos e instalaciones del centro de cómputo y si éstos se apegan a los estándares y lineamientos establecidos para la función informática de la empresa.*
- *Evaluar la forma en que se realizaron las instalaciones eléctricas, de comunicación y de datos en el área de sistemas computacionales, así como la existencia y periodicidad de mantenimiento de dichas instalaciones.*
- *Evaluar la administración de los métodos de acceso, seguridad y protección físicas del área de sistemas, la seguridad del personal y los usuarios de sistemas, así como la existencia de medidas preventivas y correctivas en casos de desastre.*
- *Evaluar la distribución del mobiliario y equipos en el área de sistemas y en las áreas que tengan equipos de cómputo; asimismo, evaluar si dicha distribución satisface las necesidades de protección, seguridad y bienestar de los usuarios de los sistemas.*
- *Evaluar el aspecto ergonómico de las instalaciones, mobiliario y equipos de cómputo de las áreas de sistemas, así como sus repercusiones en la salud y bienestar de los usuarios de sistemas de la empresa.*

11.4.2.3 Evaluación del control de accesos y salidas de datos

El activo más importante de cualquier área de sistemas es la información; por esta razón, el auditor de sistemas computacionales debe evaluar la forma en que se controla y protege el acceso a la información y a los propios sistemas computacionales de la empresa.

- *Evaluar los estándares, medidas de seguridad y métodos establecidos para la consulta de datos y salida de información del área de sistemas.*
- *Evaluar la existencia y cumplimiento de las especificaciones, estándares, medidas de seguridad y métodos de acceso, consulta, uso, manipulación y modificación de la información y datos contenidos en las bases de datos del sistema, así como los procesos y operación del mismo.*
- *Evaluar la existencia y aplicación de las normas, políticas y procedimientos para el control del acceso de datos, para su procesamiento y salida del sistema computacional.*
- *Evaluar la administración y el control de los niveles de accesos de administradores, operadores y usuarios del sistema, así como el uso y explotación de dichos niveles.*
- *Evaluar las medidas de seguridad y protección establecidas para el manejo adecuado de la información institucional, así como los planes contra contingencias y resguardos de bases de datos y archivos de información.*
- *Evaluar la administración adecuada de la seguridad de las bases de datos e información institucional, así como la existencia y periodicidad de respaldos de información.*
- *Evaluar la existencia, difusión y funcionamiento de un plan contra contingencias informáticas para salvaguardar la información institucional, así como la realización de simulacros.*
- *Evaluar la forma de resolver problemas relacionados con el manejo de la información de las bases de datos, causados por impericia, descuido, negligencia, alteración dolosa, piratería, sabotajes o cualquier otra alteración que haya sufrido la información institucional; asimismo, evaluar las medidas correctivas y preventivas adoptadas para solucionar estos problemas.*
- *Evaluar la administración de los niveles de accesos, contraseñas, privilegios de manejo de información y demás medidas de seguridad para proteger las bases de datos de los sistemas de la empresa.*

11.4.2.4 Evaluación del control de procesamiento de datos

La actividad preponderante del área de sistemas es el procesamiento de información, ya sea en un área concentrada, en equipos independientes o en sistemas de red interconectados en todas las áreas; por ello es de suma importancia que el auditor de sis-

temas computacionales sepa valorar la administración y control de estos sistemas; con ello emitirá una opinión bien fundamentada sobre el aprovechamiento de los recursos informáticos de la empresa.

- *Evaluar la existencia y aplicación de los estándares para el procesamiento de datos de los sistemas de la empresa.*
- *Evaluar la existencia y aplicación de controles específicos para el procesamiento de datos de los sistemas de la empresa.*
- *Evaluar la existencia y aplicación de los procesos lógicos y procedimientos adecuados para la captura de datos, el procesamiento de la información y la elaboración de informes, así como su funcionamiento adecuado.*
- *Evaluar el tiempo dedicado específicamente al funcionamiento de los sistemas computacionales de la empresa, en cuanto al tiempo dedicado al procesamiento de información, a la compilación y pruebas de nuevos programas, a la captura de datos, al mantenimiento del sistema operativo, al tiempo de fallas de los sistemas, al uso de Internet, al uso de impresoras, a las actividades ajenas al área de sistemas, a la ejecución de programas, al tiempo ocioso y en sí a las actividades específicas del área de sistemas.*
- *Evaluar el aprovechamiento de los sistemas computacionales de la empresa, en relación con los usos específicos a los cuales están destinados; de preferencia a través de los promedios de uso real, promedios de equipo encendido al día y los tiempos muertos de los mismos.*
- *Evaluar la utilidad y aprovechamiento de los sistemas computacionales de acuerdo con sus características, tecnología, configuraciones y software, a fin de apreciar si estos sistemas son suficientes para cubrir las necesidades de cómputo de los usuarios y las áreas de la empresa.*
- *Evaluar la existencia y aplicación de las rutinas de identificación, claves de accesos, formas de almacenamiento, periodicidad y resguardo de información de las bases de datos, archivos y programas institucionales.*
- *Evaluar la administración y control de los equipos de cómputo monousuarios, de sus planes de mantenimiento, de la frecuencia con que se lleva a cabo dicho mantenimiento, así como la respuesta a las demandas de los usuarios.*
- *Evaluar la administración de las redes de sistemas de la empresa, en cuanto a su funcionamiento, forma de compartir los recursos informáticos e información, la distribución de terminales, así como el manejo de privilegios, contraseñas y software.*
- *Evaluar si están identificadas y si se aplican las formas de procesamiento de datos (en línea, lote o cualquier otra forma) y la forma en que se manejan sus justificaciones.*
- *Evaluar la administración y control de la frecuencia y volumen de la operación y funcionamiento del sistema.*

11.4.2.5 Evaluación de controles de almacenamiento

El resguardo de la información también es uno de los aspectos fundamentales que el auditor de sistemas debe evaluar, debido a la importancia que tiene la información en todas las áreas de una empresa. Recordemos que éste es el activo más valioso de los sistemas computacionales y, por lo tanto, se debe valorar específicamente la forma de resguardar la información, la periodicidad con que se lleva a cabo, así como la forma de archivarla.

- *Evaluar el diseño adecuado de los archivos, bases de datos y la forma en que se almacena la información en los sistemas computacionales de la empresa.*
- *Evaluar la administración y control de archivos, programas e información de los sistemas computacionales de la empresa.*
- *Evaluar las formas y tipos de almacenamiento de información establecidos para los sistemas computacionales de la empresa, en cuanto al uso de disquetes, cintas, CD-Rs grabables, sistemas DVD o cualquier otro dispositivo de almacenamiento, y si éstos son acordes con las necesidades informáticas de la misma.*
- *Evaluar la existencia y seguimiento de programas de respaldos de información (backups), así como su realización adecuada, custodia y vigencia, de acuerdo con los periodos establecidos y con las características específicas para cada archivo.*
- *Evaluar la custodia de los respaldos de información, y verificar que éstos se encuentren fuera de la empresa.*
- *Evaluar la existencia y aplicación de los planes y programas de prevención contra contingencias informáticas.*
- *Evaluar la administración y control de los respaldos de información y programas institucionales, así como el manejo de los archivos del centro de cómputo.*

11.4.2.6 Evaluación de controles de seguridad

La seguridad es uno de los aspectos fundamentales para el buen funcionamiento de los sistemas computacionales; por esa razón, el auditor debe evaluar la existencia de controles de seguridad, así como su uso adecuado en las áreas de sistemas de la empresa.

- *Evaluar la existencia y aplicación de las medidas de seguridad y protección del sistema, programas, información, instalaciones, empleados, usuarios, equipos y mobiliario del sistema computacional de la empresa.*
- *Evaluar la administración y control de accesos lógicos al sistema, contraseñas, privilegios en el manejo de información, software y demás componentes del sistema, así como las medidas de seguridad en las bases de datos de la empresa para su funcionamiento adecuado.*
- *Evaluar la existencia y funcionamiento de los sistemas de control de accesos físicos, así como la seguridad de las áreas del centro de cómputo.*

- *Evaluar la existencia de salidas de emergencia, señalamientos de evacuación y demás carteles que ayuden a la actuación inmediata en caso de siniestros.*
- *Evaluar si existen y se aplican procedimientos de acceso a los sistemas computacionales, al procesador, terminales, programas e información, así como su actualización.*
- *Evaluar la existencia y aplicación de medidas de seguridad relacionadas con la comunicación de datos, acceso a redes de comunicación e Internet, para evitar el manejo doloso y la piratería de la información o infiltración de virus informáticos que afecten a los sistemas.*
- *Evaluar la administración y control de la seguridad y protección de las bases de datos e información de los sistemas de la empresa, así como su adecuado funcionamiento.*
- *Evaluar las medidas de seguridad, protección y erradicación de virus informáticos de los sistemas computacionales de la empresa, así como la difusión de las medidas preventivas y correctivas para evitar la propagación de dichos virus.*
- *Evaluar las medidas de seguridad y protección establecidas para el manejo adecuado de la información institucional, así como los planes contra contingencias y los resguardos de bases de datos y archivos de información.*
- *Evaluar la existencia de funcionarios responsables de la seguridad y protección de los bienes informáticos, información, personal y usuarios del área de sistemas, así como su capacitación para cumplir con las funciones requeridas.*
- *Evaluar las medidas de seguridad y protección de los bienes informáticos de la empresa, en cuanto al hardware, software, instalaciones, mobiliario y equipo, así como el uso y funcionamiento adecuados de estos bienes.*
- *Evaluar la existencia, difusión y actualización de los planes contra contingencias informáticas, así como su elaboración y aplicación adecuadas en las áreas de sistemas.*
- *Evaluar la existencia y aplicación periódica de simulacros de contingencias informáticas, así como las medidas preventivas y correctivas tomadas después de su aplicación.*
- *Evaluar la existencia de seguros que amparen al personal, usuarios, bienes informáticos, la información, el mobiliario y equipo del área de sistemas de la empresa, así como las formas en que se hacen las posibles reclamaciones.*
- *Evaluar todos los aspectos relacionados con la seguridad implantada en las áreas informáticas de la empresa, en cuanto a la seguridad física, seguridad lógica, seguridad de los sistemas, de las bases de datos, de la información, del personal, de los bienes muebles e inmuebles, de los sistemas operativos, del software y paqueterías institucionales y demás clasificaciones de sistemas adoptadas en la empresa.*

11.4.2.7 Evaluación de controles adicionales para la operación del sistema

El auditor de sistemas computacionales también debe evaluar todos los demás aspectos relacionados con la operación de los sistemas computacionales, a través de diversos controles sobre la actividad informática, tales como la documentación de sistemas, la estandarización de metodologías, programas, protocolos de comunicación y demás cuestiones informáticas tendientes a mejorar la operación del sistema.

- *Evaluar la existencia, uso y actualización de todos los manuales e instructivos de operación, del sistema, de usuarios y de procedimientos del área de sistemas.*
- *Evaluar la existencia, uso y actualización de las metodologías y estándares institucionales para el desarrollo de los sistemas de la empresa.*
- *Evaluar la existencia, uso y actualización de los estándares de programación y documentación de sistemas, conforme a las normas, políticas y lineamientos establecidos en la empresa en materia de informática.*
- *Evaluar la existencia, uso y actualización de la estandarización de lenguajes, programas y paqueterías de uso institucional, así como su uso adecuado en el desarrollo de sistemas en la empresa.*
- *Evaluar el uso y actualización de bitácoras para el registro de las incidencias y reportes que se presentan en el área de sistemas, a fin de llevar un registro y control de los cambios, errores, mantenimiento, operaciones y demás aspectos que repercutan en la operación del área de sistemas.*
- *Evaluar el uso de programas, paquetes de auditoría y seguimiento de actividades en las redes de sistemas computacionales de la empresa, para valorar el aprovechamiento de sus recursos y la administración y control de las operaciones de los sistemas.*
- *Evaluar la existencia de diagramas para el desarrollo de sistemas, de acuerdo con las normas y estándares establecidos en la empresa, y verificar que la codificación de sistemas se haga conforme a estos documentos.*

11.4.2.8 Evaluación de aspectos técnicos del sistema

Al revisar las actividades técnicas de los sistemas computacionales, el auditor debe evaluar todo lo relacionado con la configuración, lógica, procedimientos internos, sistemas operativos, protocolos de comunicación y todos los demás aspectos técnicos que intervienen de alguna manera en la operación normal del sistema, sean sistemas de redes, compartidos o individuales.

- *Evaluar la administración y control del sistema operativo del equipo de cómputo y que éste cumpla con las necesidades de operabilidad del propio sistema.*
- *Evaluar la administración y control de los lenguajes de operación, desarrollo y programación de los sistemas de la empresa.*

- *Evaluar la administración y control de sistemas de redes, multiusuarios y microcómputo que están instalados en la empresa, así como su funcionamiento adecuado para satisfacer las necesidades informáticas de la empresa.*
- *Evaluar la administración y control de los sistemas de telecomunicación y teleprocesamiento de los sistemas de la empresa, así como las redes de comunicación, Internet y cualquier otro medio de recepción y transmisión de información entre los equipos de la empresa y entre sistemas externos.*
- *Evaluar el uso y aprovechamiento compartido de los recursos informáticos, así como su manejo adecuado para satisfacer las necesidades informáticas de la empresa.*
- *Evaluar la existencia y aplicación de las medidas de prevención, correctivas y de control para evitar la contaminación informática de los sistemas de la empresa.*
- *Evaluar los procesos internos del sistema en relación con las entradas de datos, procesamiento y emisión de la información y almacenamiento en sus medios.*
- *Evaluar la actualización permanente y pertinente de acuerdo con los cambios tecnológicos que afectan a los sistemas computacionales de la empresa, en cuanto a la adquisición y uso del software, del hardware, de nuevos equipos de cómputo, periféricos, tarjetas adicionales del sistema, telecomunicaciones y todos los demás cambios de tecnología computacional.*
- *Evaluar la actualización continua y permanente en el diseño e implantación de estándares de operación, en la adquisición de tecnología, capacitación del personal y usuarios, desarrollo de sistemas, seguridad y protección del sistema, el procesamiento de datos y en los demás aspectos relacionados con la administración y control de sistemas computacionales de la empresa.*

11.4.3 Evaluación integral de sistemas

La manera más completa e importante de realizar una auditoría de sistemas computacionales es evaluar, de manera integral, todas las funciones, actividades, acciones, operaciones y tareas de los sistemas del área de cómputo de la empresa; esto sólo se logrará mediante la revisión integral de todas las áreas que contribuyen de alguna manera al procesamiento de información de la institución, y mediante la participación de un grupo interdisciplinario de profesionales de la auditoría que sean capaces de evaluar, en su especialidad, todos los aspectos relacionados con las necesidades informáticas del área. Para entender mejor esto, a continuación citaremos sólo algunas de las muchas formas de evaluación que se pueden dar en estos casos.

11.4.3.1 Evaluación externa o interna integral de sistemas

Debido a que la auditoría integral puede ser realizada lo mismo por auditores externos (ajenos a la empresa) o por auditores internos (que laboran en la empresa), a conti-

nuación presentamos un grupo de evaluaciones que pueden ser aplicadas mediante cualquiera de las dos formas de evaluación.

Además, sólo mencionamos de manera general algunos de los muchos aspectos que se tienen que evaluar en forma integral, enfatizando que tales aspectos aquí presentados sólo servirán para la mejor comprensión de este tipo de evaluación; es más, conviene aclarar que la auditoría integral debería contener casi todos los aspectos de evaluación antes señalados y los que citaremos a continuación:

- *Evaluar integralmente la forma en que se realiza la gestión del sistema computacional de la empresa, así como la actividad administrativa del área de sistemas, a fin de valorar la forma en que se satisfacen las necesidades informáticas de la empresa.*
- *Evaluar integralmente la existencia y apego a la estructura de organización del centro de cómputo, así como la asignación de funciones, la congruencia de los puestos, los niveles y líneas de autoridad y comunicación formal.*
- *Evaluar integralmente la administración y control de proyectos de desarrollo de sistemas en el área de informática, así como su aprovechamiento óptimo para satisfacer las necesidades de cómputo de la empresa.*
- *Evaluar globalmente la administración y control de la operación del sistema de captura y almacenamiento de datos, procesamiento de información y emisión de los informes de la empresa.*
- *Evaluar integralmente la administración, adquisición, aplicación, aprovechamiento y control de los sistemas, lenguajes operativos, programas y paqueterías de aplicación y desarrollo de sistemas en el área de informática de la empresa.*
- *Evaluar integralmente los sistemas computacionales de la empresa, así como sus procesadores, características, periféricos, tarjetas, medios de almacenamiento, equipos adicionales e instalaciones del área de sistemas.*
- *Evaluar integralmente y exclusiva el funcionamiento del sistema computacional de la empresa, en cuanto a su arquitectura, componentes internos, protocolos, procesadores, memoria, configuración, intercomunicaciones, tarjetas adicionales y todos los demás aspectos técnicos relacionados con el propio sistema.*
- *Evaluar integralmente los sistemas y medidas de seguridad, prevención, solución y capacitación para evitar contingencias en el área de sistemas de la empresa.*
- *Evaluar integralmente todos los aspectos relacionados con los virus informáticos en la empresa, las medidas preventivas, correctivas y de control para evitar contraerlos, su propagación, así como para erradicarlos de las áreas de sistemas de la empresa.*
- *Evaluar globalmente el comportamiento y operación del sistema computacional de la empresa, así como su aprovechamiento adecuado por parte de los usuarios.*
- *Evaluar integralmente la oportunidad, veracidad, suficiencia y confiabilidad de la información contenida en las bases de datos, así como su almacenamiento, conservación y protección.*

- *Evaluar integralmente todos los controles de acceso a las instalaciones del centro de cómputo.*
- *Evaluar integralmente la administración del acceso al sistema computacional, del software, paqueterías y bases de datos institucionales, así como las medidas de seguridad y de control para el acceso, consulta, alteración y modificación de los mismos por parte del personal del área y los usuarios del sistema.*
- *Evaluar integralmente la administración y control del acceso, consulta, manipulación y modificación de las bases de datos del sistema, el almacenamiento, seguridad y custodia de la información, así como la periodicidad de la actualización de respaldos, su custodia y duración.*

11.4.4 Evaluaciones con el apoyo de la computadora

En estos casos las evaluaciones se hacen para auditar todas las demás áreas de la empresa, pero utilizando la computadora como un apoyo fundamental. A continuación presentamos algunos ejemplos de esas evaluaciones:

11.4.4.1 Evaluaciones exclusivamente al sistema computacional con apoyo de la computadora y aplicaciones

En estas evaluaciones se utiliza la computadora como un apoyo para realizar las operaciones, estadísticas y graficación requeridas para apreciar el comportamiento de cada uno de los aspectos no informáticos que están siendo evaluados, debido a la facilidad para procesar información y presentar resultados; sin embargo, estas mismas evaluaciones se pueden realizar sin el apoyo de estos equipos.

- *Evaluar el aprovechamiento y utilidad del hardware institucional, con el apoyo de los sistemas computacionales, a través del análisis estadístico del tiempo que se utiliza el sistema para el procesamientos de información, la compilación de programas y pruebas de nuevos sistemas, la captura de datos, el uso de Internet, el uso de impresoras y equipos periféricos, la ejecución de actividades ajenas al área de sistemas, así como el tiempo que permanece el sistema sin ser utilizado.*
- *Evaluar la utilidad, rendimiento y explotación del software institucional, con el apoyo de una computadora, a través del análisis estadístico del tiempo que se utiliza dicho software para la elaboración de nuevos proyectos informáticos, el uso del sistema operativo, paqueterías para procesamientos de información, la compilación de programas y pruebas de nuevos sistemas, la captura de datos, el uso de Internet y la ejecución de actividades ajenas al área de sistemas, así como el tiempo que permanece dicho software sin ser utilizado.*
- *Evaluar estadísticamente, y con el apoyo de los sistemas computacionales, los reportes de incidencias, alteraciones y las repercusiones que tienen éstas en los sistemas de seguridad de las áreas de cómputo de la empresa, así como los mé-*

todos preventivos y correctivos que se aplican para la protección de los bienes y del personal informático.

- *Evaluar el rendimiento y aprovechamiento del sistema de red o sistema multiusuario, con el apoyo de la computadora, a través del análisis estadístico del tiempo que se utiliza dicho sistema para la elaboración de nuevos proyectos informáticos, el uso compartido del sistema operativo y la operación de programas, bases de datos y recursos del sistema, el uso conjunto del software y paqueterías para el procesamiento de información, la compilación de programas y pruebas de nuevos sistemas, la captura de datos, al uso de Internet y la ejecución de actividades ajenas al área de sistemas, así como el tiempo que permanece dicho sistema sin ser utilizado.*
- *Evaluar estadísticamente, y con el apoyo de los sistemas computacionales, el rendimiento, utilidad y aprovechamiento de los microsistemas de las áreas de la empresa, en cuanto al uso del sistema monousuario para procesamientos de información, la compilación de programas y pruebas de nuevos sistemas, la captura de datos, el uso de Internet, el uso de impresoras y equipos periféricos, la ejecución de actividades ajenas al área de sistemas, así como el tiempo que permanece dicho sistema sin ser utilizado.*
- *Evaluar estadísticamente, y con el apoyo de una computadora, el acceso, uso y aprovechamiento de las telecomunicaciones de la empresa, el uso de redes locales, redes regionales y redes mundiales, así como el uso y aprovechamiento de Internet.*
- *Evaluar estadísticamente, y con el apoyo de una computadora, la productividad integral del procesamiento de la información en los sistemas computacionales de la empresa.*

11.4.4.2 Evaluaciones en auditorías tradicionales con el apoyo de la computadora y aplicaciones

En estas evaluaciones se utiliza la computadora como apoyo para realizar las auditorías tradicionales, con el fin de apreciar mejor cada uno de los aspectos de todas las áreas de una empresa que están siendo evaluados; esto debe a la facilidad para procesar información y presentar resultados. Sin embargo, muchas de estas mismas evaluaciones se realizan actualmente sin el apoyo de estos equipos, entre algunos casos tenemos los siguientes:

- *Evaluar, con el apoyo de paqueterías de aplicación administrativa, todos los aspectos de la gestión administrativa de las áreas de la empresa.*
- *Evaluar, con el apoyo de hojas electrónicas de trabajo, todas las actividades contables, estadísticas, administrativas y financieras de las áreas administrativas de la empresa.*

- *Evaluar, con el apoyo de los paquetes contables de la empresa, las operaciones y registros contables, estados financieros y, en general, todos los reportes financieros y contables de la empresa.*
- *Evaluar, con el apoyo de diversas paqueterías, todas las actividades y operaciones no computarizadas de la empresa.*
- *Evaluar el desarrollo de programas de cómputo específicos para auditoría, con el fin de evaluar todas las áreas institucionales, así como el propio sistema.*
- *Evaluar, con el apoyo de los sistemas computacionales, las técnicas y métodos tradicionales de auditoría que se aplican en las evaluaciones de las demás áreas de la empresa.*
- *Evaluar el uso de las aplicaciones mixtas de programas de cómputo y los métodos tradicionales de auditoría, en la evaluación de todas las actividades de la empresa.*

11.4.5 Evaluaciones sin el uso de la computadora

En este tipo de evaluaciones, el auditor evalúa la aplicación utilización de la auditoría pero sin contar con el apoyo de los sistemas computacionales; este caso es muy similar a los casos señalados en la evaluación de carácter administrativo y evaluaciones integrales; por esta razón, solamente indicaremos algunos ejemplos de estas evaluaciones:

- *Evaluar el cumplimiento de las funciones y actividades administrativas del centro de cómputo.*
- *Evaluar la gestión financiera del centro de cómputo.*
- *Evaluar la operación de los sistemas computacionales de la empresa.*
- *Evaluar la administración y control de la realización de sistemas computacionales.*
- *Evaluar la documentación de los sistemas computacionales de la empresa.*
- *Evaluar administración y control de las técnicas y sistemas de procesamiento de información de la empresa.*
- *Evaluar la administración y control de los sistemas de seguridad y prevención de contingencias del área de sistemas.*
- *Evaluar la administración y control de las instalaciones y equipos para el funcionamiento de los sistemas de la empresa.*
- *Evaluar el uso y acceso a los sistemas, bases de datos y programas de cómputo de la empresa.*

11.4.6 Evaluaciones de los controles en sistemas computacionales

El fundamento de cualquier tipo de auditoría es el manejo adecuado del control interno de la empresa evaluada, debido a que la aplicación de dicho control es esencial para el manejo correcto de todas las actividades de dicha empresa; por esta razón, en el capítulo 4 estudiamos estas actividades bajo el carácter contable del control interno. Sin

embargo, en el aspecto informático también tienen que ser analizadas bajo el concepto y aplicación del control interno informático, mismo que analizamos en el capítulo 5.

Basándonos en esas consideraciones para realizar la evaluación a todas las actividades informáticas, a continuación únicamente mencionaremos los principales controles internos informáticos que pueden ser evaluados durante una auditoría:

11.4.6.1 Evaluación del control interno estudiado en este libro

En esta parte sólo mencionamos las evaluaciones de los controles internos señalados en el capítulo 5 de este libro, sin profundizar en ellas.

- Evaluación del control interno sobre la organización del área de sistemas, en relación con los siguientes aspectos:
  - *Dirección*
  - *División del trabajo*
  - *Separación de funciones*
  - *Asignación de responsabilidades*
  - *Perfiles de puesto*
- Evaluación del control interno sobre el análisis y desarrollo de sistemas, en relación con los siguientes aspectos:
  - *La estandarización de metodologías para el desarrollo de proyectos*
  - *Asegurar que el beneficio de sistemas sea el óptimo*
  - *Elaborar estudios de factibilidad del sistema*
  - *Garantizar la eficiencia y eficacia en el análisis y diseño de sistemas*
  - *Vigilar la efectividad y eficiencia en la implantación y mantenimiento del sistema*
  - *Hacer más eficiente el uso del sistema con su documentación*
- Evaluación del control interno sobre la operación del sistema, en relación con los siguientes aspectos:
  - *La prevención y corrección de los errores de operación*
  - *Prevenir y evitar la manipulación fraudulenta de la información*
  - *Implantar y mantener la seguridad en la operación*
  - *Mantener la confiabilidad, oportunidad, veracidad y suficiencia en la operación y procesamiento de la información*
- Evaluación del control interno sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados.
  - *Verificar la existencia y funcionamiento de procedimientos de captura de datos*
  - *Controlar el procesamiento adecuado de todos los datos*
  - *Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos*
  - *Comprobar la suficiencia de la emisión de información*

- Evaluación del control interno sobre la seguridad en el área de sistemas.
  - — *Controles para prevenir y evitar las amenazas, riesgos y contingencias que inciden sobre las áreas de sistemas*
  - — *Controles sobre la seguridad física del área de sistemas*
  - — *Controles sobre la seguridad lógica de los sistemas*
  - — *Controles sobre la seguridad de las bases de datos*
  - — *Controles sobre la seguridad en la operación de los sistemas computacionales*
  - — *Controles sobre la seguridad del personal del área de sistemas*
  - — *Controles sobre la seguridad en la telecomunicación de datos*
  - — *Controles sobre la seguridad en sistemas de redes y multiusuarios*

11.4.6.2 Evaluación del control interno propuesto por Jerry Fitzgerald[30]

Debido a la importancia de este autor en lo referente a los sistemas computacionales, así como al magnífico estudio que hace de los controles internos aplicables al área de sistemas, en esta parte sólo se propone la evaluación de los controles internos que nos cita dicho autor, con la única intención de que el lector los conozca y adopte los que más le convengan para hacer su evaluación de sistemas:

- *Evaluación del control general organizativo*
- *Evaluación del control de entradas*
- *Evaluación del control de comunicaciones de datos*
- *Evaluación del control de salidas*
- *Evaluación del control de sistemas distribuidos o terminales en líneas*
- *Evaluación del control de la seguridad física*
- *Evaluación del control de las bases de datos*
- *Evaluación del control del software institucional*

11.4.7 Evaluaciones de otros aspectos de sistemas computacionales

En el capítulo 1 de este libro propusimos una clasificación de las clases de auditorías que existen y, más concretamente, hicimos la agrupación de los tipos de auditorías que se pueden realizar en los sistemas computacionales. Tomando como base esta clasificación, a continuación veremos los siguientes tipos de auditoría de sistemas que no señalamos en los puntos anteriores.

11.4.7.1 Evaluación de los sistemas de redes

Es la evaluación de todos los recursos informáticos de los sistemas de redes, los cuales son compartidos y existe un servidor central en el que se concentran todos los recursos importantes del sistema, procesadores, memorias, discos duros de almacenamiento, sis-

temas operativos, programas, paqueterías y todo el software dedicado al manejo de la red, además de sus terminales distribuidas de acuerdo con una configuración y características específicas que satisfacen las necesidades de cómputo de la empresa. El auditor de sistemas computacionales debe evaluar todos los aspectos relacionados con la red.

- Aspectos de la administración de los sistemas de redes que deben ser evaluados:
  - *Evaluación de los sistemas de seguridad y protección del sistema de redes, de sus programas, información, instalaciones, empleados y usuarios.*
  - *Evaluación de la administración y control de sistemas de red, multiusuarios y microcómputo.*
  - *Evaluación de la administración y control de sistemas de telecomunicación, Internet, correo electrónico, teleconferencia y teleprocesamiento.*
  - *Evaluación de la administración y control de los sistemas de redes locales (LANs), metropolitanas (MANs), mundiales (WANs), Internet y multiusuarios.*
  - *Evaluación de la administración de los recursos informáticos, personal e información de sistemas multiusuarios, compartidos y de redes.*
  - *Evaluación de los sistemas de control de niveles de accesos, privilegios y restricciones al sistema, software y a las bases de datos compartidas.*
  - *Evaluación de la administración de los procedimientos para el acceso al procesador, terminales, programas, bases de datos e información institucional.*
  - *Evaluación de la administración y control de los niveles de accesos, privilegios, contraseñas y usos específicos de los usuarios de acuerdo con su función en las actividades informáticas de los sistemas.*
  - *Evaluación de los estudios de viabilidad y factibilidad para el diseño, adquisición e instalación de los sistemas de redes de la empresa, así como de los estudios técnicos, de costo-beneficios, de necesidades informáticas, de actualización y funcionamiento de dichas redes.*
  - *Evaluación del diseño, configuración e instalación de los sistemas de redes, de sus topologías y protocolos de comunicación, así como de los servidores y terminales que satisfagan las necesidades de la empresa.*
  - *Evaluación de la administración y control de las adquisiciones de servidores, procesadores, memorias, instalaciones, software y hardware para la instalación de redes, terminales y comunicaciones dentro de la empresa.*
  - *Evaluación del diseño, configuración, arquitectura, protocolos e instalación de las redes de cómputo de la empresa.*
  - *Evaluación de la administración y control de protocolos, configuraciones, topologías y cableados de los sistemas de redes.*
  - *Evaluación de las necesidades de sistemas operativos, programas integrales, paqueterías, programas de desarrollo y demás software que satisfaga las necesidades informáticas de la empresa.*

11.4.7.2 Evaluación del servicio OUTSOURCING

En la actualidad es muy común encontrar empresas que contratan los servicios informáticos de otras empresas especializadas en sistemas, ya que les resulta más rentable y económico que esas empresas les hagan el trabajo que realizarlo ellas mismas.

Estos servicios abarcan casi todas las especialidades informáticas, desde la captura de datos y procesamiento de información, el desarrollo de nuevos proyectos de sistemas, la administración y mantenimiento de los servicios informáticos, el mantenimiento de los sistemas operativos, del software, de programas, de paqueterías y lenguajes, hasta el mantenimiento y actualización de sistemas (hardware), periféricos, instalaciones y demás componentes físicos de los sistemas, así como la impresión de documentos y muchas actividades más del área de sistemas.

De entre las muchas aplicaciones de este servicio, el auditor debe tomar en cuenta los siguientes aspectos:

- *Evaluar que exista un contrato de servicios, en el cual se especifiquen claramente las condiciones del servicio, coberturas de servicios que se amparan, los costos, los límites de responsabilidad, los alcances y todo lo relacionado con la prestación de estos servicios computacionales. Si es posible, también debe evaluar los beneficios y las desventajas de dichos contratos.*
- *Evaluar la calidad de los proveedores de servicios de cómputo que atenderán a la empresa, en cuanto a capacidad instalada, sus equipos disponibles, personal de apoyo y servicio, tiempo de respuesta, software, programas, lenguajes y paqueterías disponibles para el servicio, así como la calidad del respaldo de proveedores, fabricantes y servicios de apoyo.*
- *Evaluar las instalaciones del prestador de servicios, en relación con la infraestructura física de sus equipos, capacidad de sus funcionarios y personal de sistemas, seriedad en el cumplimiento de su trabajo, oportunidad, confiabilidad y eficiencia en el proceso de información, así como todos aquellos aspectos que impliquen un valor agregado.*
- *Evaluar la administración y control de las aplicaciones y desarrollo de programas informáticos para atender las necesidades de cómputo de la empresa.*
- *Comparar los costos-beneficios, gastos-rendimiento, ahorros en tiempo, operabilidad y trabajo que implica el servicio de outsourcing con los mismos costos-beneficios, gastos-rendimiento, y ahorros en tiempo, operabilidad, trabajo y rendimiento informático que implica realizar el trabajo de cómputo en la empresa.*
- *Evaluar la seguridad y confiabilidad que representa la contratación de servicios de cómputo, así como las medidas preventivas y correctivas adoptadas para evitar un manejo inadecuado de la información institucional.*
- *Evaluar en cuáles áreas de la empresa son aplicables los servicios externos de cómputo y en cuáles no son aplicables, valorando sus coberturas actuales.*

11.4.7.3 Evaluación de la función ergonómica de los sistemas de cómputo

La ergonomía, de *ergon*: trabajo y *nomos*: leyes, es la ciencia que estudia el bienestar, confort y seguridad de los trabajadores dentro de su medio ambiente laboral, considerando su entorno profesional y el impacto que tienen las herramientas y los instrumentos de trabajo en el desempeño de sus actividades y en su salud física y emocional, a fin de proponer medidas preventivas y correctivas que permitan desarrollar el trabajo en las mejores condiciones posibles. Esta ciencia se define de la siguiente manera:

"La ergonomía, la ciencia de trabajo, es un campo de tecnología que considera limitaciones y capacidades humanas en el diseño de máquinas y objetos [...] los procesos de trabajo que ellos deben seguir y los ambientes en que ellos operan."[31]

La ergonomía es una ciencia moderna que, aplicada en el ámbito de las computadoras, se encarga de estudiar el confort, bienestar y seguridad con que los usuarios de los sistemas computacionales realizan su trabajo, la influencia del medio ambiente y las repercusiones del uso de estos sistemas en la salud física y emocional de los usuarios y su consecuencia en la productividad de su trabajo.

El auditor de sistemas computacionales debe evaluar estas repercusiones y consecuencias en la salud de los usuarios, en cuanto a los siguientes aspectos:

- *Evaluar los estudios ergonómicos sobre el impacto del uso de las pantallas de los sistemas, la iluminación y demás reflejos que afectan la salud visual de los usuarios.*
- *Evaluar los estudios ergonómicos sobre las distintas posiciones y posturas que se adoptan frente a la computadora, así como su posible repercusión en la columna vertebral, tórax, cuello, nuca y demás afectaciones ortopédicas para la salud, el rendimiento, el descanso y bienestar de estos usuarios.*
- *Evaluar los estudios ergonómicos sobre la repercusión del uso del teclado y ratón en los brazos, muñecas y dedos de los usuarios de sistemas computacionales.*
- *Evaluar los estudios ergonómicos sobre el impacto del medio ambiente laboral en la salud física y bienestar de los usuarios de sistemas computacionales.*
- *Evaluar los estudios ergonómicos sobre las cargas de estrés, condiciones ambientales, estilos de dirección y condiciones generales de bienestar para el desarrollo adecuado de las actividades computacionales en la empresa, así como su impacto en la salud emocional de los usuarios.*
- *Evaluar los índices de ausentismo, rotación de personal, cambios de actitud y demás aspectos que repercuten en el buen desempeño de las actividades de sistemas de cómputo, a fin de evaluar su impacto en la salud física y emocional de los usuarios.*
- *Evaluar los estudios ergonómicos sobre las demás afectaciones físicas causadas por el medio ambiente, iluminación, sistemas de aire acondicionado, instalaciones, mobiliarios etcétera.*

El auditor también debe evaluar el impacto de los sistemas en el desempeño y productividad del personal que está en contacto con las computadoras, y en sí debe evaluar todo lo relacionado con el bienestar, confort y medio ambiente que rodea a los sistemas computacionales, su repercusión en la salud física y emocional de los trabajadores, así como las medidas preventivas, correctivas y diseños de espacios adecuados para el desarrollo óptimo del trabajo.

A continuación presentamos algunos de estos aspectos que el auditor tiene que evaluar:

- *Evaluación de la existencia y aplicación de los estudios ergonómicos relacionados con el bienestar y seguridad en el desempeño de los directivos, empleados y usuario de sistemas de la empresa.*
- *Evaluación del estudio del impacto en la salud física de los directivos, empleados y usuarios de sistemas de la empresa, en cuanto a sus repercusiones en la vista, el tórax, cuello, nuca, columna vertebral, brazos, manos, dedos y demás impacto en su salud física.*
- *Evaluación de la existencia y seguimiento de las medidas para prevenir repercusiones en la salud de los directivos, empleados y usuarios de sistemas de la empresa, así como de las medidas correctivas para mejorar esas situaciones.*
- *Evaluación de los estudios, propuestas y diseños del mobiliario y equipos que permitan a los directivos, empleados y usuarios de sistemas computacionales, y a todos los empleados de la empresa en general, desarrollar su trabajo con seguridad, confort y bienestar.*
- *Evaluación de la existencia, aplicación y seguimiento a los estudios ergonómicos realizados en las áreas de sistemas de la empresa, así como de las medidas correctivas y preventivas derivadas de los mismos, a fin de mantener la seguridad, confort y bienestar de los usuarios de sistemas de la empresa.*

11.4.7.4 Evaluación de la calidad ISO-9000 aplicable a los sistemas computacionales

Actualmente se ha popularizado el sistema de administración y aseguramiento de calidad a través de la certificación ISO-9000, cuyo principal objetivo es evaluar que los productos o servicios que proporcionan las empresas a sus clientes cumplan con los estándares de calidad establecidos en las normas ISO.*

Para el área de sistemas se puede aplicar la norma ISO-9004 que marca la guía para sistemas de aseguramiento de calidad. "[...] Esta norma se define como implementar un sistema de calidad, basado en una filosofía de calidad y documentado en un manual de calidad. Este sistema debe incluir todas las políticas, procesos y procedimientos necesarios para asegurar la calidad [...]"[32]

Respecto a la auditoría ISO-9000 que se realiza en las áreas de sistemas, ésta se puede realizar en dos sentidos:

* ISO: International Standards Organization (Organización Internacional de Estándares). Del griego *isos*: igual. Op-cit. Diccionario Etimológico, pág. 256.

- Para evaluar la manera en que se obtiene la certificación de Calidad ISO-9000 en los sistemas, productos y servicios de cómputo de la empresa, a través de la propia auditoría de calidad de sistemas de esta certificación, y con los requisitos, características y modalidades de esta auditoría.
- Para evaluar la aplicación de las normas ISO 9001[33] a través de la evaluación de los siguientes aspectos:
  - *Evaluación de la administración y control de los procesos relacionados con "La norma que exige [...] identificar y planear [...] procesos [...] para que se lleven a cabo condiciones controladas."*[34]
  - Evaluación de las inspecciones y pruebas relacionadas con el procedimiento para saber si el producto o los resultados del proceso se realizaron correctamente, conforme a las características y especificaciones del diseño del sistema.
- Para evaluar la aplicación y seguimiento de la norma ISO 9000, como guía para las normas ISO 9001, ISO 9002, ISO 9003, conforme a lo que indica el autor de referencia, lo cual se considera aplicable en todos sus párrafos:[35]
  - *4.1 Responsabilidad administrativa*
  - *4.2 Sistemas de calidad*
  - *4.3 Revisión del contrato*
  - *4.4 Control de proyectos*
  - *4.5 Control de documentos e información*
  - *4.6 Compras (adquisiciones)*
  - *4.7 Control de productos proporcionados al cliente*
  - *4.8 Identificación del producto y posibilidad de seguimiento*
  - *4.9 Control de procesos*
  - *4.10 Inspecciones y pruebas*
  - *4.11 Control de inspecciones, equipos de mediciones y prueba*
  - *4.12 Estado de inspección y prueba*
  - *4.13 Control de productos que no llenan requisitos*
  - *4.14 Acciones correctivas y preventivas*
  - *4.15 Manejo, almacenamiento, embalaje, preservación y envío*
  - *4.16 Control de registros de calidad*
  - *4.17 Auditorías internas de calidad*
  - *4.18 Capacitación*
  - *4.19 Servicio*
  - *4.20 Técnicas estadísticas*
- Para evaluar los fundamentos de la calidad ISO 9000-3 y todos los relativos a la aplicación de los servicios computacionales, en cuanto a la documentación de los procedimientos, la realización de lo documentado y la evaluación a la realización de productos o servicios de sistemas computacionales.

- Para evaluar la aplicación de la norma ISO 9002 para los sistemas de calidad del modelo de aseguramiento de la calidad en la producción, instalaciones y servicios. Con todas las secciones de esta norma aplicables a los sistemas computacionales.
- Para evaluar la aplicación de la norma ISO 9003 para los sistemas de calidad del modelo de aseguramiento de la calidad en la inspección y pruebas finales. Con todas las secciones de esta norma aplicables a los sistemas computacionales.
- Para evaluar la aplicación de la norma ISO 9000-1 para los sistemas de calidad del modelo de aseguramiento de la calidad, que señalan las normas de aseguramiento y administración de la calidad. Lineamientos para la selección y uso. Con todas las secciones de esta norma aplicables a los sistemas computacionales.
- Para evaluar la aplicación de la norma ISO 9004-1 para los sistemas de calidad del modelo de aseguramiento de la calidad, que señalan los elementos de administración y sistemas de calidad. Lineamientos. Con todas las secciones de esta norma aplicables a los sistemas computacionales.
- Para evaluar la aplicación de las demás normas de calidad ISO 9000 aplicables en la evaluación de la calidad de los sistemas computacionales de la empresa, así como las NOM-MEX, las recientes Quality System o cualquier otra norma similar para la calidad de los sistemas.

11.4.7.5 Evaluación de los proveedores y distribuidores de sistemas

Actualmente, los permanentes cambios tecnológicos hacen necesario evaluar constantemente las adquisiciones de nuevos sistemas, no sólo en cuanto al software del sistema, sino en lo relativo al hardware, los equipos periféricos y todos los componentes de sistemas de una empresa, incluso en la capacitación de los usuarios, a fin de verificar que los cambios de la tecnología computacional se hagan conforme a las necesidades reales de las áreas de sistemas computacionales de las empresas.

Es por ello que el auditor de sistemas computacionales debe evaluar los aspectos relacionados con la adquisición de nuevos productos informáticos, así como a los proveedores y distribuidores que los proporcionan, a fin de garantizar las adquisiciones más adecuadas, al menor costo y con la más alta calidad y servicio para las necesidades de cómputo de la empresa; por esa razón debe tomar en cuenta los siguientes puntos:

- *Evaluación de la existencia y de la aplicación correcta de los procedimientos adoptados en la empresa para la adquisición de sistemas computacionales.*
- *Evaluación de la existencia y aplicación de los procedimientos para identificar y establecer las mejoras de los sistemas computacionales, de acuerdo con las normas y políticas de la empresa.*
- *Evaluación de las convocatorias y concursos de adquisición de activos informáticos, a fin de verificar la elección correcta de proveedores y que las adjudicaciones se hayan realizado con transparencia y conforme a los costos y procedimientos autorizados por la empresa.*

- *Evaluación de la calidad de los productos, así como de la oportunidad, confiabilidad y calidad de los proveedores y distribuidores de sistemas para proporcionar los servicios y mantenimiento de activos informáticos.*
- *Evaluación del seguimiento y control de los proveedores, distribuidores, asesores y desarrolladores de sistemas, así como de la utilidad e importancia que éstos tienen para la empresa.*
- *Evaluación de los últimos cambios de sistemas computacionales de la empresa, valorando que éstos cumplan con las necesidades específicas de actualización del área de sistemas.*

11.4.8 Importancia de las evaluaciones de sistemas computacionales

Finalizaremos este apartado de la evaluación señalando la importancia que ésta tiene para la auditoría de sistemas computacionales, en razón de las siguientes consideraciones:

- La evaluación por sí misma no tiene ningún sentido si no se concibe como un apoyo para el desempeño óptimo del trabajo, debido a que permite identificar la problemática de sistemas computacionales, para proponer mejoras a su desempeño.
- La evaluación es parte integral de las actividades administrativas del área de sistemas, debido a que por medio de esta herramienta se puede saber cuál es el desempeño real de los sistemas computacionales, en comparación con su desempeño esperado, y con los resultados de esa comparación se retroalimenta a los directivos para la toma de decisiones.
- La evaluación debe ser un proceso permanente que permita valorar el cumplimiento de las funciones, actividades, operaciones y tareas de los sistemas de cómputo, sus obstáculos y limitaciones, sus avances permanentes y la mejora en el servicio que proporciona a la empresa.
- La credibilidad de la evaluación se fundamenta en los siguientes aspectos:
  - *La calidad en la interpretación del análisis de los resultados esperados contra los realmente alcanzados.*
  - *La oportunidad, confiabilidad, veracidad, claridad y suficiencia de los resultados de la misma evaluación.*
  - *La confidencialidad de los procesos de evaluación, en cuanto a la información que se recopila, los responsables involucrados y el uso de los resultados.*
  - *La calidad en la aplicación de herramientas, métodos y procedimientos para la recopilación de información, análisis y resultados que se emiten.*
  - *La utilidad que tiene para evaluar todos los aspectos relacionados con el área de sistemas, los sistemas computacionales y las funciones, actividades, operaciones y tareas que desempeñan los directivos, empleados y usuarios de sistemas de la empresa.*
- La evaluación proporciona información muy valiosa sobre el aspecto de sistemas que se está evaluando, ya que permite analizar a fondo su comportamiento, funcionalidad, aplicación y utilidad para la empresa.

- Al aplicar una evaluación, el auditor puede identificar claramente a los responsables de utilizar, aplicar y resguardar los bienes informáticos del sistema.
- Los resultados de la evaluación permiten proponer opciones para corregir, mejorar o mantener el uso y aprovechamiento de los recursos informáticos de los sistemas, así como del desempeño de las funciones, actividades y operaciones de los directivos, empleados y usuarios de los sistemas de la empresa.
- Al emitir un dictamen sobre el resultado de las evaluaciones al área de sistemas computacionales, se ayuda a los responsables de dicha área a tomar mejores decisiones respecto a las problemáticas en el desempeño de las actividades de sistemas y con ello se optimiza el servicio de sistemas de la empresa.

11.5 Diagrama del círculo de evaluación

Con esta herramienta de apoyo para la evaluación de los sistemas computacionales se puede valorar, visualmente, el comportamiento de los aspectos de los sistemas que están siendo auditados, así como su cumplimiento y limitaciones (ver figura 11.7).

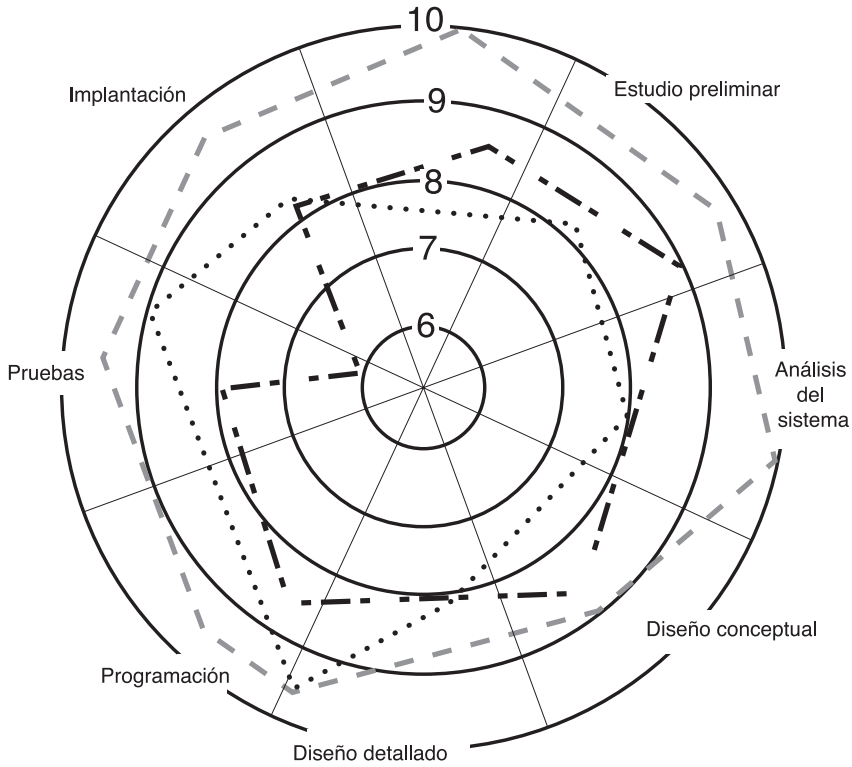


Figura 11.7 *Diagrama del círculo de evaluación*

Esta gráfica está integrada por círculos concéntricos y líneas, los cuales tienen una función específica:

- ***Círculos:*** *a estos círculos se les asignan valores arbitrarios ascendentes, de preferencia los interiores más bajos (6) y exteriores más altos (10), o puede ser cualquier otro criterio de calificación.*
- ***Líneas o puntos de segmentos:*** *estas líneas señalan los segmentos o sectores en que se divide cada uno de los aspectos de sistemas que serán evaluados. En este ejemplo se eligieron, como segmentos, las fases del análisis y diseño de sistemas.*
- ***Líneas de cumplimiento máximo exigido:*** *estas líneas representan el entorno de la calificación más alta que se exige a cada uno de los aspectos que serán evaluados (en este caso se utilizó* línea punteada*).*
- ***Líneas de cumplimiento mínimo exigido:*** *estas líneas representan el entorno de la calificación más baja que se puede aceptar para cada uno de los aspectos que están siendo evaluados (en este ejemplo,* línea punteada*).*
- ***Líneas o cruz de evaluación:*** *estas líneas representan la calificación alcanzada en la parte o segmento del trabajo que está siendo auditado; para obtener esta calificación, el auditor le asigna un valor a esa parte del trabajo, de acuerdo con los resultados obtenidos, según su criterio (en este ejemplo,* línea larga y punto*).*

El análisis que se desprende de la evaluación del círculo de ejemplo, es que en casi todas las fase del análisis y diseño del sistema, sí cumplen con la calidad en el desarrollo de los sistemas: porque están dentro del rango máximo (área enmarcada por líneas gruesas) y el rango mínimo (área delimitada por líneas punteadas). De ahí mismo se desprende que las fases de análisis preliminar y la fase de pruebas no cumplen con el mínimo deseado. El uso de esta herramienta de evaluación permite analizar, de un solo vistazo, toda la problemática que incide en determinados aspectos; el auditor puede evaluar todo el desarrollo de los sistemas de la empresa y valorar, según su criterio, el grado de cumplimiento global e individual de cada una de esas fases.

Esta técnica de evaluación también se puede utilizar para analizar cualquier otro aspecto relacionado con los sistemas computacionales de la empresa, pero se deben hacer las siguientes modificaciones:

- *Modificar los círculos de valores de evaluación, ya sea su número o los valores numéricos asignados a cada uno; también se pueden establecer rangos cualitativos, en escalas desde excelente para el máximo hacia deficiente para el mínimo o alguna otra escala similar.*
- *También se puede variar el número de segmentos que serán utilizados, agregando o eliminando estas líneas de división de acuerdo con las necesidades concretas de evaluación.*

En algunos casos convendría eliminar tantos círculos y señalar sólo el área de cumplimiento máximo y el área de cumplimiento mínimo, e indicar los puntos de evaluación, como se indica en el siguiente ejemplo:

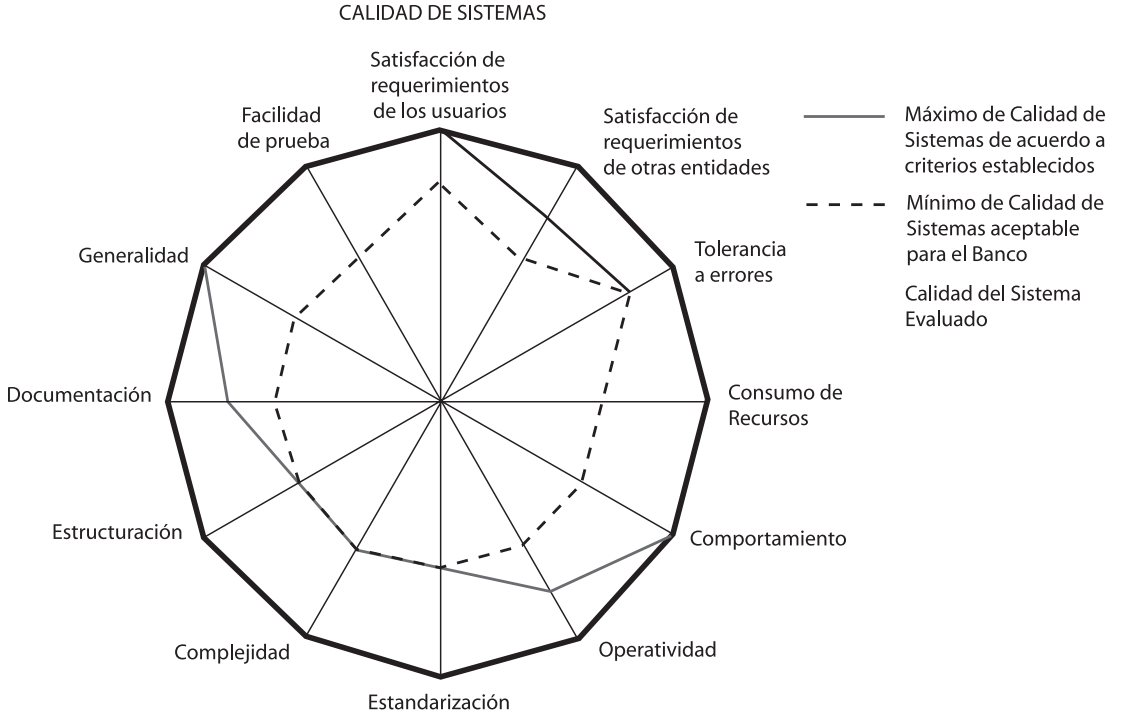


Figura 11.8 *Calidad de Sistemas*

En el ejemplo (ver la figura 11.8) utilizamos el círculo de evaluación para analizar los rangos de calidad dentro de los cuales se proporcionaba el servicio de computación en las áreas administrativas de una empresa cualquiera. El área de cumplimiento máximo es la línea gruesa exterior (toda la figura) y el área de cumplimiento mínimo son las líneas punteadas. La evaluación es la línea continua menos gruesa.

En este caso, el resultado es que se cumple con la calidad más o menos satisfactoriamente.

Es aconsejable que antes de aplicar este diagrama circular de evaluación, el auditor de sistemas determine en grandes grupos los aspectos de informática que serán evaluados, con el propósito de hacer una de concentración de los tópicos afines o relacionados entre sí, para realizar un examen más global de los puntos que debe analizar.

Este diagrama también se puede utilizar para hacer la presentación gráfica de los principales problemas encontrados en aspectos específicos de computación en la empresa, ya que con dicha presentación es más fácil comprender las desviaciones que se reportan.

A continuación se indican algunos ejemplos de aspectos comunes que pueden ser evaluados mediante esta herramienta:

- Para evaluar la seguridad en el área de sistemas computacionales (en este caso siete sectores):
  - *Seguridad en el acceso físico al área de sistemas*
  - *Seguridad en el acceso y uso de las bases de datos*
  - *Seguridad en el mantenimiento y resguardo de las bases de datos e información*
  - *Seguridad del personal informático*
  - *Seguridad de las instalaciones del área de sistemas*
  - *Plan contra contingencias del área de sistemas*
  - *Seguridad lógica del sistema*
- Para la evaluación administrativa del área de sistemas (en este caso 11 sectores)
  - *Evaluación de la misión, visión y objetivos del área de sistemas*
  - *Evaluación de las estrategias, planes y programas del área de sistemas*
  - *Evaluación de la estructura de organización del área de sistemas, en lo relacionado con las funciones, actividades y tareas, líneas de autoridad y responsabilidad*
  - *Perfil de puestos del área de sistemas*
  - *Documentación de sistemas*
  - *Seguridad y protección de los activos informáticos*
  - *Instalaciones del área de sistemas*
  - *Capacitación, adiestramiento y promoción del personal del área de sistemas computacionales*
  - *Desarrollo de proyectos informáticos*
  - *Estandarización de metodologías, programas, equipos y sistemas*
  - *Mobiliario, equipos y componentes del sistema*
- Para la evaluación de los sistemas computacionales (en este caso ocho sectores):
  - *Diseño lógico del sistema computacional*
  - *Diseño físico del sistema computacional*
  - *Controles de acceso y salida de datos*
  - *Controles de procesamiento de información*
  - *Controles de almacenamiento de datos*
  - *Controles de seguridad*
  - *Controles para la operación del sistema*
  - *Aspectos técnicos del sistema*

Estos casos sirven para ejemplificar el uso de los círculos (sectores) de evaluación de sistemas computacionales, pero debemos tomar en cuenta que el diseño de estos aspectos se debe hacer de acuerdo con las características y necesidades de evaluación del área de sistemas, así como a las escalas de valoración.

11.6 Lista de verificación (o lista de chequeo)

Éste es uno de los métodos de recopilación y evaluación de auditoría más sencillos, más cómodos y más fáciles de utilizar, debido a la simplicidad de su elaboración, la comodidad en su aplicación y por la facilidad para encontrar desviaciones, lo cual la hace una de las herramientas más confiables y utilizables para cualquier revisión de sistemas computacionales; asimismo, se aplica tanto para el área de sistemas, para la gestión administrativa o para cualquier otra función informática.

Esta herramienta consiste en la elaboración de una lista ordenada, en la cual se anotan todos los aspectos que se tienen que revisar del funcionamiento de un sistema, de sus componentes, del desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación del área de sistemas; esta lista se complementa con una o varias columnas en las que se califica el cumplimiento del aspecto evaluado. Por lo general se palomea el cumplimiento (✓), se tacha el incumplimiento (**X**) o se deja en blanco. Con esto se identifica a simple vista el cumplimiento o incumplimiento del aspecto evaluado.

La lista de verificación (o lista de chequeo; a partir de aquí se tratarán indistintamente ambos conceptos) puede ser diseñada en **dos columnas**: el concepto y el cumplimiento o incumplimiento, o en **varias columnas**: una para el concepto y las otras para elegir una calificación representada en cada columna, según el grado de cumplimiento del concepto.

Ejemplo de dos columnas

En este ejemplo se muestra una lista de chequeo sencilla, en la cual verificaremos que una red de cómputo cuente con todos sus componentes, aplicaciones y que sea confiable:

Verificar el funcionamiento y cumplimiento adecuado de la red de cómputo, así como la inclusión de sus componentes, su aplicación y su uso.	
Descripción del concepto	**Cumple**
La instalación de la red es flexible y adaptable a las necesidades de la empresa.	
La lista de componentes de la red contiene todo el hardware requerido para su funcionamiento adecuado.	
La lista de componentes de la red contiene todo el software requerido para su funcionamiento adecuado.	
La red de cómputo es aprovechada al máximo en la empresa.	

Continúa

Continuación

Los recursos de la red se comparten de acuerdo con las necesidades de la empresa.	
La configuración de recursos de la red es la mejor para el uso correcto de los sistemas computacionales de la empresa.	
Se acepta la transferencia frecuente de grandes volúmenes de información.	
Existen niveles de acceso y seguridad en la red.	

Ejemplo de lista de chequeo de varias columnas

En el siguiente ejemplo se muestra una lista de chequeo con grados de calificación de cumplimiento; en este caso revisaremos la seguridad del centro de cómputo.

Verificar la seguridad en el centro de cómputo, y calificar sólo una de las columnas de cada concepto según su grado de cumplimiento.				
Descripción del concepto	**100% Excelente**	**80% Cumple**	**60% Mínimo**	**40% Deficiente**
1. Evaluación de la seguridad en el acceso al sistema				
• *Evaluar los atributos de acceso al sistema.*				
• *Evaluar los niveles de acceso al sistema.*				
• *Evaluar la administración de contraseñas del sistema.*				
• *Evaluar la administración de la bitácora de acceso al sistema.*				
• *Evaluar el monitoreo en el acceso al sistema.*				
• *Evaluar las funciones del administrador del acceso al sistema.*				
• *Evaluar las medidas preventivas o correctivas en caso de siniestros en el sistema.*				
2. Evaluación de la seguridad en el acceso al área física				
• *Evaluar el acceso del personal al centro de cómputo.*				
• *Evaluar el acceso de los usuarios y terceros al centro de cómputo.*				
• *Evaluar la administración de la bitácora de acceso físico al área de sistemas.*				
• *Evaluar el control de entradas y salidas de bienes informáticos del centro de cómputo.*				

Continúa

Continuación

• *Evaluar la vigilancia del centro de cómputo.*				
• *Evaluar las medidas preventivas o correctivas en caso de siniestros en el centro de cómputo.*				

En este ejemplo se supone que el auditor o la persona que realice el chequeo, calificará el cumplimiento, según su criterio, señalando la columna que satisface el nivel de cumplimiento del aspecto de seguridad informático que está evaluando.

11.7 Análisis de la diagramación de sistemas

Ésta es una de las principales herramientas de apoyo para el análisis y diseño de los sistemas computacionales, y es de las que más utilizan los desarrolladores de sistemas, debido a que por medio de estos diagramas el analista puede representar los flujos de información, actividades, operaciones, procesos y los demás aspectos que intervendrán en el desarrollo de los propios sistemas; además, por medio de los diagramas el programador puede visualizar el panorama específico del sistema, para elaborar de manera más precisa la codificación de instrucciones para el programa.

El auditor de sistemas computacionales también puede aprovechar esto para evaluar el desarrollo correcto los proyectos de sistemas que se realizan en la empresa, ya que le permite evaluar si el flujo de información es acorde con las necesidades del programa y si las operaciones y actividades que se realizan satisfacen los requerimientos del mismo. Además, también le ayudan a valorar el desempeño correcto de las actividades de los líderes de proyectos, de los analistas de sistemas, de los programadores y de todas las personas que intervienen en el desarrollo del proyecto.

El auditor puede utilizar esta herramienta para el diseño de sistemas de diferentes formas en una auditoría de sistemas, de acuerdo con su experiencia, conocimientos y habilidades, mismas que debe canalizar en los siguientes sentidos:

- *Solicitar los diagramas del sistema para analizar su lógica de desarrollo, contenido y congruencia con lo que el usuario espera del sistema, a fin de valorar estos aspectos en el funcionamiento actual de dicho sistema y con ello verificar que su operación sea correcta.*
- *Analizar el diagrama del sistema, a fin de evaluar si la codificación de instrucciones (programación) se hizo de acuerdo con el diseño de dicho sistema, si el programa cumple con los procedimientos previamente diseñados, conforme a las necesidades de los usuarios plasmadas en este diagrama, tanto de operación como de procedimientos.*
- *Elaborar un diagrama del sistema que va a evaluar, a fin de identificar los procedimientos, actividades y operación, según su punto de vista, y compararlos*

con el desarrollo actual del sistema, con los propios diagramas del sistema y con las instrucciones diseñadas para el mismo. Con ello puede corroborar el funcionamiento adecuado de dicho programa.

- *Verificar la documentación de los sistemas a través de sus diagramas, evaluando que las instrucciones plasmadas en la documentación sean acordes a las actividades que se desarrollan con dichos sistemas.*
- *Evaluar el desarrollo correcto de las actividades, procedimientos y operaciones del sistema, tomando los diagramas de sistemas como base de análisis, y verificar la forma en que los usuarios operan dicho programa, y si con ello se satisfacen las necesidades informáticas del mismo.*

El uso de esta herramienta de análisis y diseño de sistemas puede ser de gran ayuda para auditar el desarrollo de proyectos informáticos de la empresa, las acciones de cómputo que se satisfacen con dichos proyectos y la forma en que los usuarios operan el sistema.

11.7.1 Modelos de sistemas

Los modelos de sistemas se utilizan para tratar de interpretar una realidad acerca de las necesidades informáticas del usuario, identificando el comportamiento que tendrá el sistema a través de sus distintos procesos, actividades y componentes, mismos que el auditor puede evaluar de manera gráfica y sencilla (ver figura 11.9).

Modelos

Son representaciones abstractas de la realidad

Análisis	Procesos	De flujo de datos Gráficas de transformación
	Datos	Entidad-Relación Modelado de datos Estructura de datos Estructura lógica
	Estado-Evento	Estado-Transición Historia de la vida de la entidad
Diseño	Diseño	Gráficas de estructura
Las demás no son soportadas		

Figura 11.9

En el modelo del diagrama 11.1 se observan, de manera general, las etapas del desarrollo de un proyecto informático por medio de sus procesos y sus datos, así como de los estados y eventos que lo compondrán. El diseño del sistema también se puede comentar por medio de las gráficas de estructura.

Las Gráficas de los diagramas de modelo están compuestas por etapas generales en las cuales se determina, en forma específica, cada uno de sus componentes.

El auditor de sistemas debe estar pendiente de analizar todos los modelos de sistemas diseñados para el desarrollo de los proyectos, ya que puede existir un sinnúmero de ellos para un solo proyecto; también debe evaluar su congruencia, aplicación correcta y utilidad para el diseño del propio sistema.

Presentamos este ejemplo sólo para identificar el tipo de modelos de sistemas a que se refiere esta sección, pero debemos señalar que estos modelos pueden variar en contenido, contexto y forma de representación, de acuerdo con las necesidades específicas de los desarrolladores de sistemas, de los usuarios y del propio auditor que los aplique para valorar el desarrollo de los proyectos informáticos de una empresa.

11.7.2 Diccionario de datos

El diccionario de datos se aplica principalmente en el desarrollo de las bases de datos de un sistema, para determinar cada uno de los campos de datos, el tipo, tamaño y descripción de los datos que contendrán dichas bases de datos, como se indica en el siguiente ejemplo:

Mediante este diccionario de datos se presentan los contenidos de una base de datos, de una manera visual, sencilla y clara. En este documento se detalla específicamente el total de los campos que componen esta base de datos, y se presenta el contenido de cada uno dichos campos (ver la figura 11.10).

Diccionario de Datos

Campo	Tipo	Tamaño	Descripción
Cmater	Carácter	5	Clave del material *
Cusuario	Carácter	5	Clave del usuario *
Fprestam	Numérico	6	Fecha del préstamo *
Flímite	Numérico	6	Fecha límite de entrega *
Fentrega	Numérico	6	Fecha de devolución del préstamo
Xedopres	Carácter	9	Estado del préstamo: PRESTADO, PERDIDO O DEVUELTO *
Crespons	Carácter	3	Iniciales de la persona que modificó el registro por última vez. *

Los asteriscos indican aquellos campos que no pueden estar vacíos, debido a la funcionalidad necesitada del sistema

Figura 11.10

En el ejemplo se presentan los siguientes aspectos:

- *El **total de datos** que integrarán la base de datos.*

- *El **nombre o sinónimo del dato** (generalmente mnemotécnico); es el nombre que se le da al campo, según el vocablo particular utilizado por el programador o software utilizado.*
- *El **tipo de información;** es la determinación del tipo de datos que aceptará ese campo: carácter, numérico, alfanumérico, de texto o de fecha.*
- *El **tamaño del campo;** (rangos permitidos por el campo) es el número de dígitos que aceptará cada campo.*
- *La **descripción del campo;** si es necesario se presenta una breve descripción del contenido, características o cualquier otro comentario del campo.*

En este tipo de diagramas de sistemas, los diccionarios de bases de datos, también se puede incluir otro tipo de información, de acuerdo con las necesidades específicas del desarrollador del sistema, como campos indexados, privilegios, condiciones especiales y demás características necesarias para cada campo.

La función del auditor en la evaluación de bases de datos es revisar todos los aspectos relacionados con el diseño, elaboración y aplicación de las bases de datos; sin embargo, para el caso del ejemplo, consiste en verificar que exista un diccionario de bases de datos, con este modelo o con cualquier otro, así como verificar la designación correcta de cada uno de los campos, el tipo de datos utilizados y la cantidad de dígitos que acepta la base de datos, además de otros aspectos especiales del diseño de esta base de datos y su diagramación.

11.7.3 Diagrama Nassi-Schneiderman

Al igual que los diagramas de sistemas anteriores, los desarrolladores de sistemas computacionales también utilizan este diagrama gráfico para el análisis y diseño del software estructurado de un nuevo sistema. En este diagrama gráfico se definen, lo más objetiva y claramente posible, los procesos, decisiones e iteraciones del sistema, a fin de señalar gráficamente todas las acciones que seguirá el programa para su funcionamiento adecuado (ver la figura 11.11).

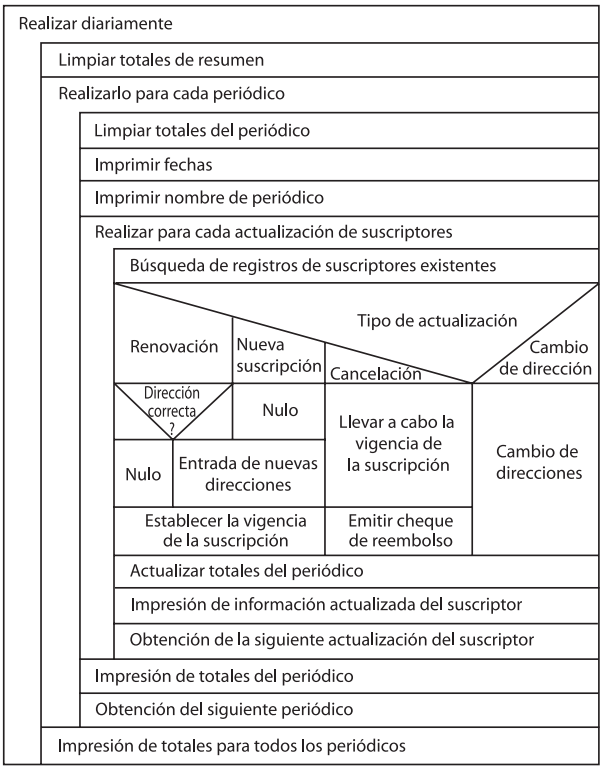


Figura 11.11 *El uso de un diagrama Nassi-Schneiderman para ilustrar el servicio de actualización de suscripciones diarias de un periódico*

Concretamente, este diagrama utiliza tres grandes apartados: los procesos, decisiones e iteraciones.

- ***Procesos*** *(representados por rectángulos); son la definición de variables, actividades, entradas, salidas y todos aquellos procesos que se deberán ejecutar en el programa.*
- ***Decisiones o condiciones alternativas*** *(representadas por los triángulos invertidos y su siguiente línea de alternativa) que muestran las diferentes alternativas o decisiones que se pueden tomar durante el procesamiento, mismas que debe cubrir el programa.*
- ***Iteraciones*** *(representadas por los ciclos y repeticiones) son las operaciones del contenido total de este diagrama, las cuales indican el funcionamiento total del sistema.*

El diagrama de ejemplo[36] (figura 11.11) por sí mismo representa la forma en que se estructura un software.

11.7.4 Diagrama de estado–transición

En este diagrama se representan los flujos de información que se siguen en una relación de programación estructurada, a fin de visualizar el proceso que se sigue para el desarrollo de las actividades del programa. Por lo general, las entidades se expresan con el nombre del responsable del proceso y las flechas señalan el proceso que se ha de seguir en el programa; además, los rectángulos señalan el estado que guardan en relación con la actividad del proceso que se está ejecutando.

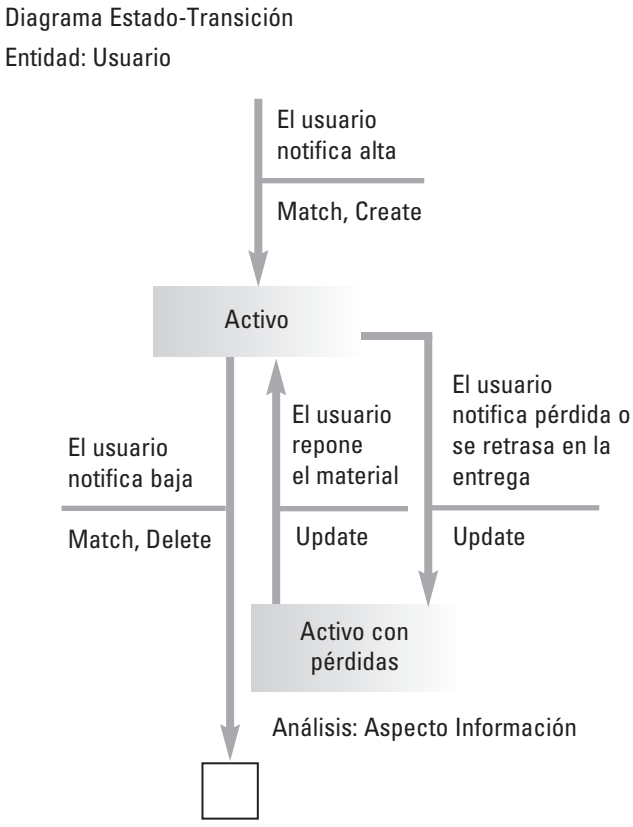


Figura 11.12 *Diagrama Estado-Transición*

En este ejemplo (figura 11.12) se indica la acción que sigue una entidad (el usuario) para dar de alta un dato o para darlo de baja.

Las flechas nos indican el procedimiento que se sigue para cada una de las acciones del dato que va a ser utilizado.

Está claro que este diagrama nos permite seguir, de manera gráfica, el proceso de la información, en este caso de una sola actividad. Este diagrama es sólo una parte de

una serie de diagramas que, en conjunto, representan la forma estructurada que seguirá un proceso total de un sistema.

Mediante este tipo de diagramas, el auditor de sistemas puede evaluar si el procedimiento que utilizó el diseñador del sistema es acorde con las necesidades de los usuarios, la forma en que interpretó las necesidades de éstos, así como la lógica del sistema. También puede evaluar la programación que realizó el codificador, según el lenguaje utilizado.

11.7.5 Diagrama de contexto

Este diagrama muestra de una manera casi global todas las entidades o los procesos que alimentan el objeto principal del sistema, a través de rectángulos que representan la entidad o proceso en particular y la interacción de éstos con el proceso fundamental, indicado por flechas que señalan el flujo que se sigue para la interacción de ambos.

En este ejemplo se presenta el sistema para el control de una biblioteca, que es el procesamiento central del programa.

Figura 11.13 *Diagrama de Contexto*

Además, en la figura 11.13, se presenta cada una de las entidades o procesamientos auxiliares que se intercalarán con el proceso central (rectángulos), el cual indica los nombres de cada una de las entidades, así como la acción concreta que realizan para el procesamiento central de este programa. Tal sería el caso de un usuario, quien en una acción devuelve material al control de la biblioteca; después del procesamiento en el control de la biblioteca, al mismo usuario se le regresa o entrega el recibo correspondiente.

En este caso concreto sólo se presentan entidades, usuarios, recursos humanos, departamento de redes, etcétera, pero se podría dar el caso de que fueran otros procesamientos los que interactuaran con este proceso central, según las necesidades del diseñador del sistema.

Este diagrama es muy útil para el auditor de sistemas computacionales, debido a que le permite identificar el sistema desde todo su contexto y con todas las posibles interacciones que se dan en sus procesos y programación; esto le permitirá identificar cada uno de los componentes, entidades y procesos que integran el sistema, así como las interacciones entre ellos y los flujos de información que se siguen con el funcionamiento de dicho sistema. Además, analizar a fondo este tipo de diagramas le ayuda al auditor a comprender el funcionamiento total del sistema y le permite identificar, por separado, el funcionamiento de cada uno de sus componentes; con todo esto, el auditor puede evaluar a fondo el funcionamiento del sistema, su aplicación, así como su diseño y programación, entre muchos otros aspectos.

11.7.6 Diagrama de flujo de datos

Éste es el más común de los diagramas de sistemas y tiene un sinnúmero de representaciones, en las cuales se usan simbologías clásicas como la IBM, HIPO o una simbología particular establecida por el diseñador del sistema. Lo importante del diagrama es que permite identificar las operaciones, actividades, participantes, el flujo de información y las alternativas que se siguen durante el proceso, contemplando visualmente todas las características, procedimientos y flujos que llevan los datos, desde su inicio hasta su terminación, así como los cambios de direccionamiento por medio de decisiones.

A continuación se muestran tres tipos de diagramación de sistemas considerados dentro de esta categoría de diagramas de flujo. En ninguno de estos casos se hacen comentarios, pues sería necesario establecer parámetros de diagramación, lo cual no es la intención de este autor, sino únicamente presentar este tipo de diagramas para su conocimiento.

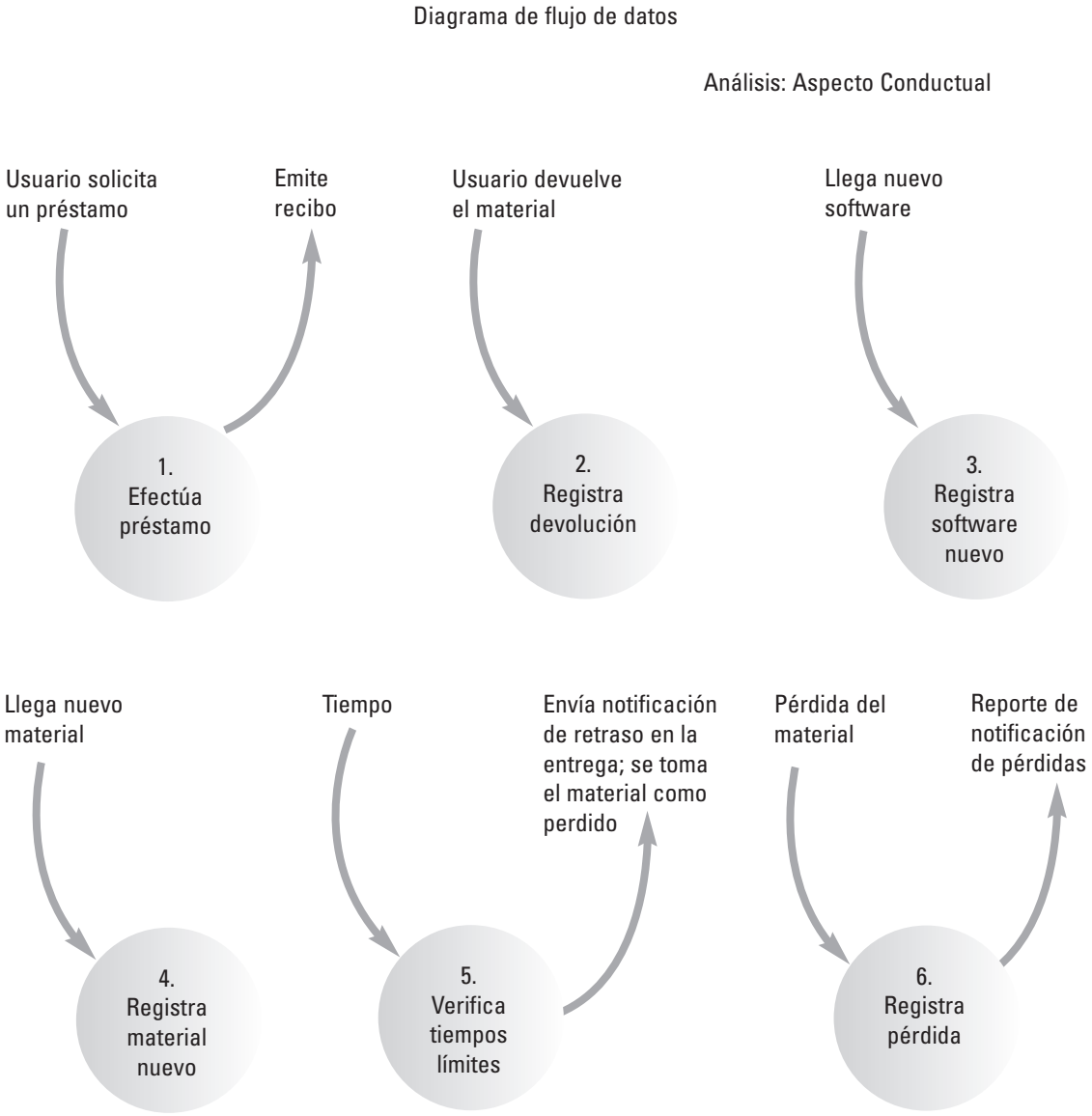


Figura 11.14 *Diagrama de flujo de datos*

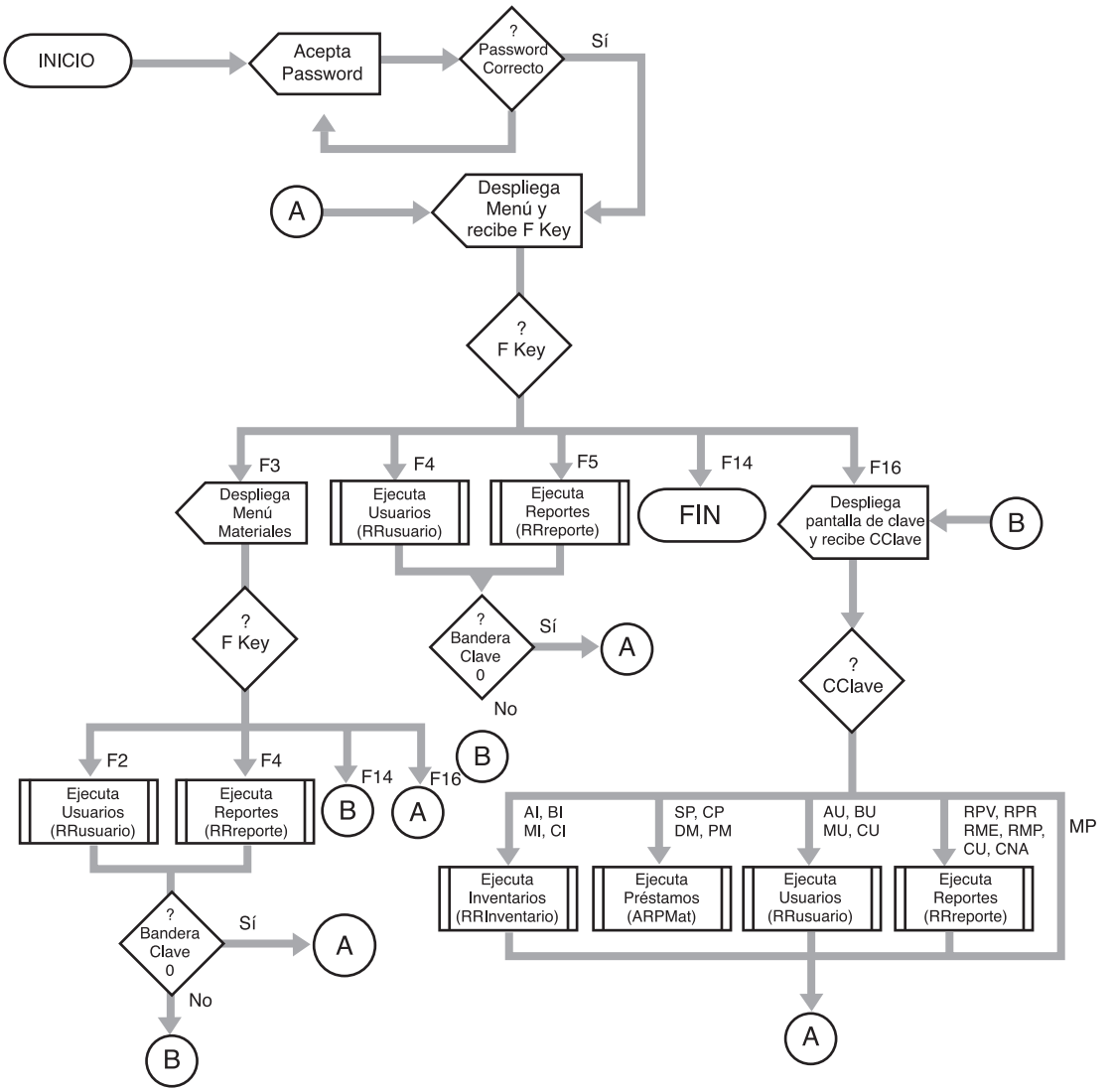


Figura 11.15 *Diagrama de flujo de datos*

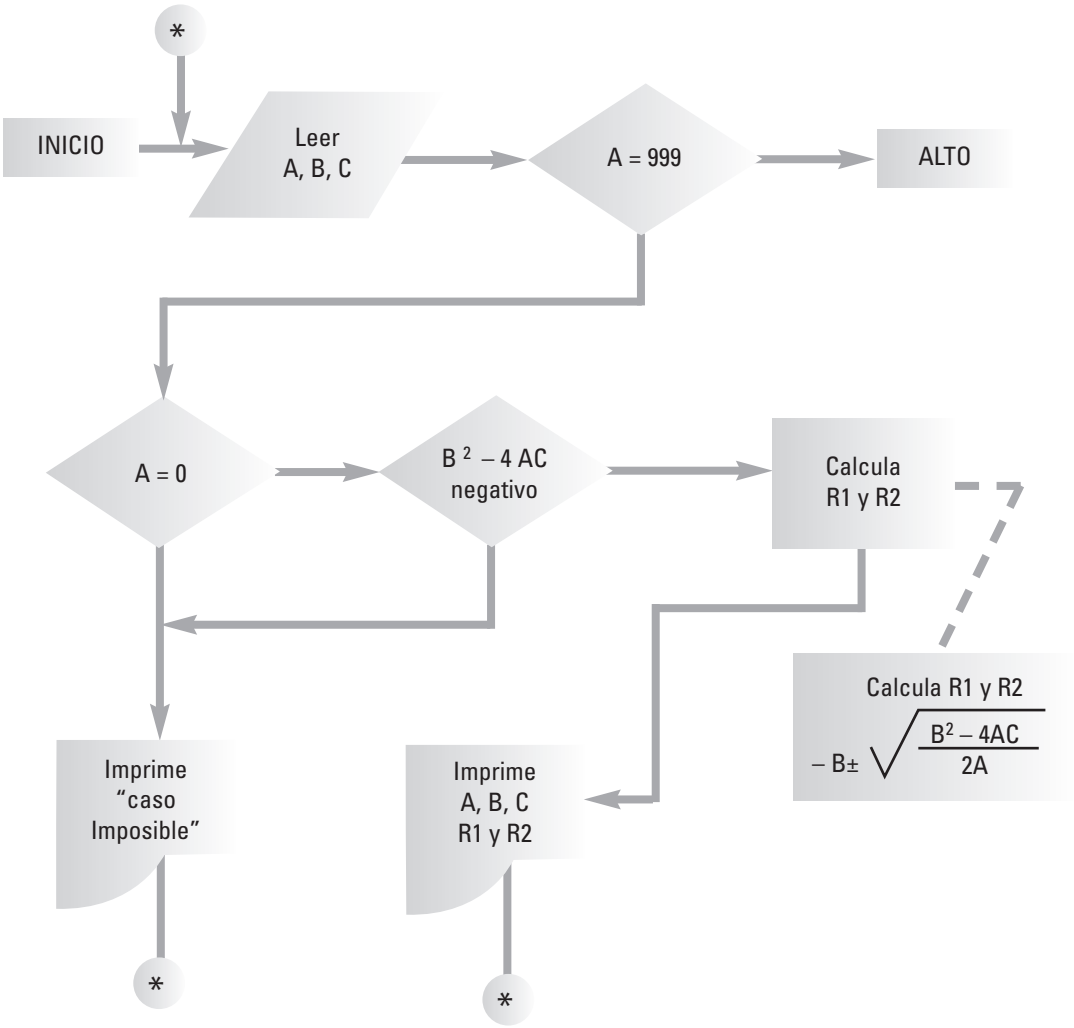


Figura 11.16 *Diagrama de flujo de datos*

11.7.7 Diagrama modular

Los diagramas modulares de sistemas son muy similares a los anteriores, sólo que en éstos se muestra el flujo de la información en módulos representados por organigramas de actividades, operaciones o entidades que participan en el proceso del sistema; en estos diagramas cada módulo tiene acciones concretas y sólo se muestra en forma general para que se entienda su participación en el proceso; sin embargo, cada módulo puede tener un diseño modular por sí mismo.

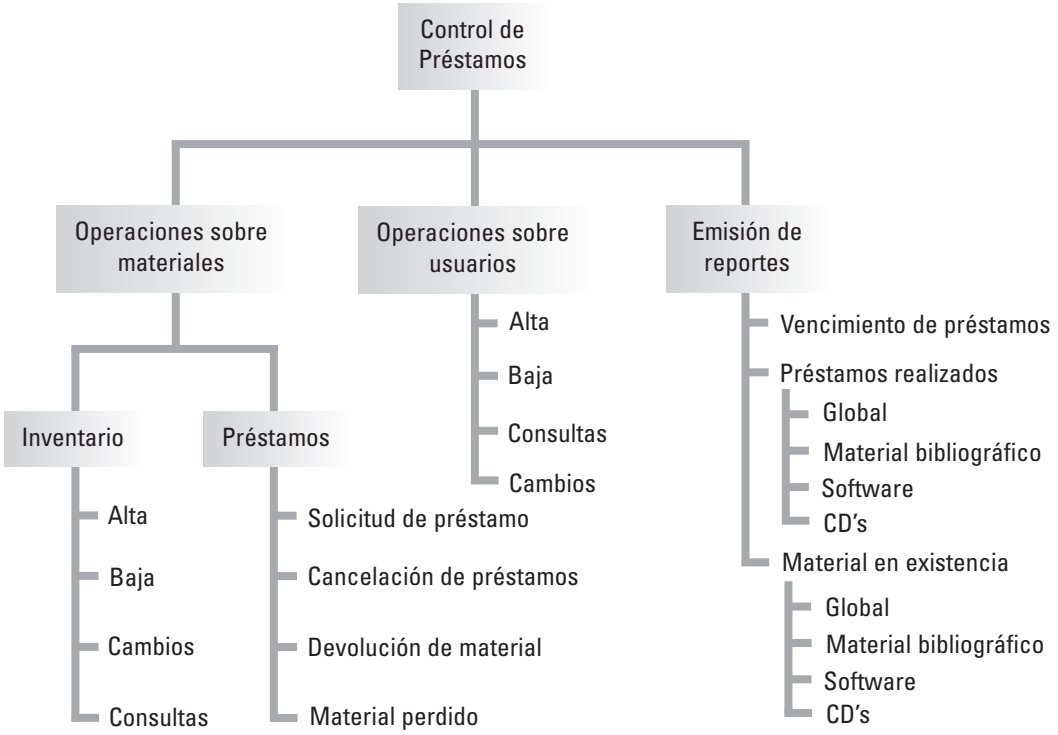


Figura 11.17 *Diagrama modular principal*

En el ejemplo (figura 11.17) se presenta un diagrama modular del procedimiento que se sigue para el control de prestamos, considerando todas las actividades modulares que intervienen en este proceso. En cada módulo concreto, como en el caso del módulo inventario, se deben dar otros procesos para las altas, bajas, cambios y consultas.

La ventaja de utilizar este diagrama modular es que se puede presentar todo el procesamiento del sistema en una sola gráfica, o en cada módulo, según sea el caso.

Al aplicar este diagrama de módulos, el auditor puede identificar el contexto general del sistema, tanto en su totalidad como en cada uno de los módulos que lo integran, lo cual le permitirá realizar una evaluación integral del funcionamiento del sistema, de su programación y de su aplicación.

Conviene finalizar este apartado señalando que existen muchos tipos de diagramas en el ambiente informático y que por la variedad de aplicaciones que tienen sería imposible citarlos todos en esta obra; sin embargo, nada impide al auditor de sistemas computacionales utilizar en la práctica de su trabajo los diagramas de flujo que requiera, siempre y cuando éstos le sean útiles para identificar el funcionamiento de los sistemas. Esto último es lo más recomendable.

11.8 Diagrama de seguimiento de una auditoría de sistemas computacionales

El uso de esta técnica, también conocida como mapa conceptual de evaluación, es de mucha utilidad en una auditoría de sistemas computacionales, ya que permite hacer un mapa conceptual de todos los aspectos de los sistemas en evaluación. Al utilizar esta técnica se hace un seguimiento concreto de todas y cada una de las partes que componen el sistema, lo cual permite que el auditor tenga un panorama completo de todo el sistema, a fin de evaluar integralmente todos sus aspectos. Los diagramas de seguimiento se usan tanto para la gestión informática, para la seguridad del sistema, para los componentes del sistema o para cualquier otro aspecto informático en evaluación.

Esta herramienta informática se aplica mediante un diagrama descriptivo del sistema, de tipo secuencial descendente, con sangrías significativas de izquierda a derecha, las cuales van señalando cada una de las partes que integran el aspecto de sistemas auditado, de tal manera que el auditor pueda identificarlas. Con ello logra tener un panorama general de lo que está auditando y puede señalar las principales observaciones que encuentra, así como las partes que se ven afectadas por esas desviaciones. Si esta herramienta se aplica correctamente, permite contemplar todos los aspectos de sistemas involucrados, así como sus posibles desviaciones.

Este diagrama está compuesto por grandes apartados, los cuales corresponden a los aspectos medulares del sistema evaluado. Dentro de cada uno de estos apartados se van confeccionando las principales partes, componentes y actividades concretas que integrarán cada módulo. Asimismo, dentro de cada módulo se pueden identificar las partes concretas que lo integran y así sucesivamente. Este diagrama se complementa con líneas que cubren todos los componentes señalados en cada apartado.

A continuación presentaremos un diagrama de seguimiento de auditoría o mapa conceptual, con el fin de entender mejor la aplicación de esta herramienta:

Aspecto principal en evaluación

(I) Primer aspecto de evaluación

(I-1) Componente uno del primer aspecto de evaluación
- (I-1-A) Integrante A del componente uno
- (I-1-B) Integrante B del componente uno

(I-2) Componente dos del primer aspecto de evaluación
- (I-2-A) Integrante A del componente dos
- (I-2-B) Integrante B del componente uno

(I-3) Componente tres del primer aspecto de evaluación
- (I-3-A) Integrante A del componente dos
- (I-3-B) Integrante B del componente uno

(II) Segundo aspecto de evaluación

(II-1) Componente uno del segundo aspecto de evaluación
(II-1-A) Integrante A del componente uno
(II-1-A-1) Parte 1 del integrante A
(II-1-A-2) Parte 2 del integrante A
(II-1-A-3) Parte 3 del integrante A
(II-1-B) Integrante B del componente uno
(II-1-B-1) Parte 1 del integrante B
(II-1-B-2) Parte 2 del integrante B

(II-2) Componente dos del segundo aspecto de evaluación
(II-2-A) Integrante A del componente tres
(II-2-B) Integrante B del componente tres

(II-3) Componente tres del segundo aspecto de evaluación
(II-3-A) Integrante A del componente tres
(II-3-B) Integrante B del componente tres
(II-3-C) Integrante C del componente tres

(III) Tercer aspecto de evaluación

(III-1) Componente uno del tercer aspecto de evaluación
(III-1-A) Integrante A del componente uno
(III-1-A-1) Parte 1 del integrante A
(III-1-A-1-a) Parte menor del integrante A
(III-1-A-1-b) Parte menor del integrante A
(III-1-A-2) Parte 2 del integrante A
(III-1-A-3) Parte 3 del integrante A
(III-1-B) Integrante B del componente uno
(III-1-B-1) Parte 1 del integrante B
(III-1-B-2) Parte 2 del integrante B

(III-2) Componente dos del tercer aspecto de evaluación
(III-2-A) Integrante A del componente tres
(III-2-B) Integrante B del componente tres

(III-3) Componente tres del tercer aspecto de evaluación
(III-3-A) Integrante A del componente tres
(III-3-A) Integrante B del componente tres

En este diseño conceptual se utilizaron los siguientes elementos:

- Para los aspectos fundamentales de la evaluación:
  Color negro y letra negrita, sin líneas
- Para cada uno de los componentes:
  Color rojo y letra cursiva, líneas del mismo color

- Para los integrantes de cada componente:
  Color azul y letra normal, líneas del mismo color
- Para las partes de cada integrante:
  Color verde y letra normal, líneas del mismo color
- Para la parte menor:
  Color negro y letra normal, sin línea

Como podemos observar en el diseño propuesto, los colores, el tipo de letra y las demás características fueron elegidos a voluntad; el auditor puede hacer lo mismo para elaborar su propio mapa conceptual del aspecto de sistemas que esté auditando. Lo que importa es que designe perfectamente cada una de las partes que compondrán el diagrama, de acuerdo con las características de los aspectos que evalúe.

Los colores pueden sustituirse por tipos de letras y formatos de negrillas, cursiva o subrayado, y las líneas por grosor y tipo de línea.

A continuación presentaremos un mapa conceptual para evaluar el diseño de una área de sistemas cualquiera.

Mapa conceptual para evaluar el diseño de una Red del área de sistemas

- **Planeación**
  - *Misión del área de sistemas*
  - *Visión del área de sistemas*
  - *Objetivos del área de sistemas*
  - *Diseño físico de la red del área de sistemas*
    - Configuración de la red
    - Servidor
    - Terminales
    - Sistemas de almacenamiento de información
      - *Discos duros*
      - *Cintas*
      - *CD-ROMs (quemadores)*
      - *DVDs*
      - *Otros sistemas de almacenamiento de datos*
    - Instalaciones
      - *Instalaciones eléctricas*
      - *Instalaciones de datos*
      - *Instalaciones de comunicación*
    - Protocolos de comunicación
  - *Diseño lógico de la red del área de sistemas*
    - Sistema operativo

  - Lenguajes de desarrollo de sistemas
  - Paqueterías
  - Programas de aplicación
  - Protocolos de comunicación
  - Diseño de accesos al sistema
- *Estrategias para el área de sistemas*
- *Políticas del área de sistemas*
- *Normas del área de sistemas*
- *Programa de trabajo*
- *Procedimientos de operación*

- **Estructura de organización del área de sistemas**
  - *Estructura de puestos del área de sistemas*
  - *Establecimiento de funciones para los puestos del área de sistemas*
  - *Asignación de jerarquías en el área de sistemas*
  - *Establecimiento de responsabilidad de los puestos del área de sistemas*
  - *Designación de canales de comunicación en el área de sistemas*
  - *Organigrama del área de sistemas*
  - *Perfiles de puestos*

- **Requerimientos de recursos para el área de sistemas**
  - *Personal informático para el área de sistemas*
    - Personal del área de sistemas
    - Usuarios del área de sistemas
    - Asesores y consultores para el área de sistemas
    - Proveedores y distribuidores para el área de sistemas
  - *Requerimientos del sistema (hardware)*
    - Computadoras
    - Servidores
    - Impresoras
    - Procesadores
  - *Requerimientos de software*
    - Sistema operativo
    - Lenguajes de desarrollo de sistemas
    - Paqueterías
    - Programas de aplicación
    - Protocolos de comunicación
    - Diseño de accesos al sistema
    - Licencias
  - *Requerimientos de mobiliario y equipos*
  - *Requerimientos de instalación en el área de sistemas*

— *Estudio de localización de planta para el área de sistemas*
— *Requerimientos de materiales y consumibles en el área de sistemas*

- **Servicio que proporcionará el área de sistemas**
  — *Captura de datos, procesamiento y emisión de información*
  — *Diseño de sistemas*
    - Diseño de proyectos de sistemas institucionales
    - Diseño de bases de datos
    - Programas de aplicación
    - Instalación de paqueterías
    - Instalación de programas específicos de aplicación

  — *Seguridad del área de sistemas*
    - Seguridad de acceso a los sistemas institucionales
    - Seguridad de aceso y uso de las bases de datos
    - Seguridad de acceso al área de sistemas
    - Seguridad del personal informáticos y usuarios
    - Programas contra contingencias informáticas

  — *Mantenimiento de sistemas*
    - Mantenimiento preventivo
    - Mantenimiento correctivo

  — Auditoría de sistemas
  — Asesoría y capacitación a usuarios
  — Administración de la base de datos

11.9 Programas para revisión por computadora

Esta técnica es de las de más utilizadas en cualquier auditoría de sistemas computacionales, debido a que permite revisar, desde la misma computadora y mediante un programa específico, el funcionamiento del sistema, de una base de datos, de un programa en especial o de alguna aplicación de interés; ya sean sus procesamientos, su funcionamiento interno, el aprovechamiento de las aplicaciones informáticas, el consumo de recursos, los resultados del procesamiento de información o el comportamiento específico de alguna actividad administrativa, entre otros aspectos.

Esta herramienta tiene dos vertientes importantes; por un lado, el uso de programas específicos, previamente diseñados por desarrolladores de sistemas, con el propósito de evaluar aspectos específicos de sistemas, de contabilidad, nóminas o cualquier otro aspecto especial de la gestión administrativa de la empresa o de los propios sistemas computacionales. Por otro lado, el diseño de programas concretos que el auditor desarrolla le permiten evaluar aspectos concretos que desea auditar, los cuales pueden ser desde aspectos netamente de sistemas, casos concretos de gestión informática, el funcionamiento interno del sistema, su arquitectura o su procesamiento

de datos. Algunas veces hasta la revisión interna del sistema, en cuanto al hardware, software, componentes, instalaciones y aspectos técnicos del sistema.

En ambos casos el auditor de sistemas determina, de acuerdo con su experiencia, conocimientos y necesidades específicas de evaluación, el programa que va a utilizar, ya sea alguno de los programas existentes en la empresa o el mercado si cumplen con sus necesidades concretas de evaluación, o bien algún programa que él mismo diseñará para evaluar el aspecto de sistemas o de gestión administrativa que le interese. Este programa lo puede diseñar y programar el propio auditor o solicitar su elaboración al área de sistemas, siempre que se cumpla correctamente con sus especificaciones.

A continuación presentaremos algunos ejemplos de estos programas.

11.9.1 Programas de revisión elaborados por desarrolladores

Este tipo de programas ya se han desarrollado previamente por distribuidores y fabricantes de software, de acuerdo con una necesidad específica del mercado o para propósitos específicos; aunque también son realizados por desarrolladores de la misma empresa. Con ellos se busca evaluar alguna orientación sustantiva de los sistemas computacionales, en cuanto al hardware, software, instalaciones, conexiones del sistema, rendimientos de equipo o cualquier otro aspecto especial que el auditor pueda aprovechar para evaluar el sistema.

En estos casos, el auditor de sistemas identifica sus necesidades concretas de evaluación y, de acuerdo con ellas, busca los programas ya desarrollados que le permitan auditar los aspectos de sistemas que le interesan. Con estos programas también revisa los asuntos del sistema o de la gestión administrativa del sistema o de la empresa que desea auditar.

No se requiere una amplia experiencia para el uso de estos programas, ya que la mayoría de las veces son muy sencillos de manejar; sin embargo, en caso de que el auditor no los conozca lo suficiente, el personal informático será quien le ayude a utilizar este software.

Un ejemplo de este tipo de programas es la evaluación del software y hardware de los sistemas, en relación con la problemática del año 2000, en donde se tuvieron que revisar los siguientes aspectos, entre muchas otras cosas:

- *El BIOS del sistema*
- *El reloj del sistema*
- *Los procesadores y componentes de la tarjeta madre*
- *Los sistemas de aplicación para evaluar su funcionamiento en el año 2000*
- *Las conexiones internas o externas del sistema*
- *Las fechas de los datos en las bases de datos*
- *La confiabilidad de las operaciones de cálculo de fechas*
- *La interconectividad interna y externa de sistemas anteriores a 1995*
- *Los periféricos y componentes asociados al sistema*

El anterior es sólo uno de los muchos ejemplos de programas ya desarrollados que están a disposición del auditor para evaluar los aspectos de sistemas que son de su interés. Entre los programas más comunes se encuentran los programas de contabilidad, nómina, aplicaciones estadísticas, de evaluación de hardware, evaluación de componentes internos y arquitectura del sistema, de monitoreo de estaciones de trabajo y de rutinas de auditoría del sistema.

11.9.2 Programas de revisión elaborados por el auditor

Para utilizar esta opción, el auditor identifica los aspectos de los sistemas, de la gestión administrativa o de las bases de datos que debe revisar en el área de sistemas y establece, en forma anticipada, uno a uno los asuntos concretos que va a revisar mediante el apoyo de un sistema computacional; para ello diseña un programa de revisión que contemple sus intereses de evaluación, determinando, lo más preciso posible, las rutinas de revisión que necesita, las bases de datos, el lenguaje o programas especiales de desarrollo que va a utilizar, y en sí diseña, y si es posible programa, el sistema de evaluación que requiere para realizar su revisión.

Es muy frecuente que el auditor de sistemas desconozca el uso del lenguaje o programas de desarrollo que se actualizan en el sistema computacional de la empresa, por lo que tendrá que recurrir a los servicios de un programador; éste, de acuerdo con las características y estándares de programación de la empresa, seguirá las instrucciones determinadas por el auditor, y siguiendo el diseño del programa del auditor, realizará la codificación de instrucciones, elaborará las pruebas correspondientes y liberará el programa de cómputo para que el auditor lo aplique en su revisión.

El auditor de sistemas recurre frecuentemente a los analistas de sistemas, con la intención de que éstos interpreten sus necesidades de cómputo; bajo esta circunstancia adopta el papel de usuario de sistemas, con un doble propósito: por un lado, que el área de sistemas realice el análisis de sus necesidades concretas y determine los pasos necesarios para que, tanto analista de sistemas como programador, elaboren en conjunto el programa de revisión que requiere el auditor, a fin de que, una vez terminado el sistema, el auditor lo pueda aplicar libremente a lo que desea auditar. Por otro lado, con la interpretación de esa postura de usuario, también procura analizar cómo se atienden, interpretan y desarrollan en el área de sistemas las necesidades de cómputo de los usuarios, y evalúa la atención que reciben éstos.

Ejemplificar este caso nos tomaría mucho tiempo; por esta razón sólo mencionamos el punto, ya que tendríamos que describir un programa específico para poder ejemplificar esta aplicación. Pero debemos señalar que es potestad del auditor diseñar, programar o solicitar la realización de un programa de cómputo que cubra sus necesidades de auditoría.

12

Propuesta de puntos que se deben evaluar en una auditoría de sistemas computacionales

Estructura del capítulo

Objetivos del capítulo

Considerando los tipos de auditoría de sistemas computacionales expuestos en este libro, sugerir los puntos específicos que el auditor debe tomar en cuenta para aplicarlos de acuerdo con la actividad de sistemas que tenga que auditar. Estos puntos se presentan en forma general y como un apoyo para el auditor.

Introducción del capítulo

En el capítulo 1 definimos los tipos de auditoría de sistemas computacionales que permiten evaluar la actividad informática de una empresa; asimismo, en los siguientes capítulos también señalamos los principales elementos de sistemas que se deben tomar en cuenta en cada uno de los tipos de auditoría ahí propuestos. Tomando esto en cuenta, a continuación haremos un análisis más profundo sobre la manera de aplicar cada uno de los tipos de auditoría sugeridos, a fin de que el lector conozca los puntos que debe considerar al planear su auditoría de sistemas computacionales; claro está, de acuerdo con las necesidades específicas de evaluación de sistemas de la empresa que vaya a auditar.

Cabe señalar que para exponer las siguientes sugerencias de puntos específicos adoptaremos la misma estructura propuesta en la clasificación de auditorías presentada en el capítulo I, y aunque a primera vista los puntos que vamos a estudiar en esta parte pueden parecer repetitivos, comparándolos con lo expuesto a lo largo de los capítulos anteriores, esta aparente repetición de conceptos no es tal, ya que presentaremos todo un panorama concreto de métodos, técnicas, herramientas y procedimientos específicos de auditoría de sistemas computacionales, los cuales se deben aplicar según las necesidades específicas de auditoría de la empresa. También presentamos los principales aspectos que el auditor debe tomar en cuenta para diseñar su propia evaluación de sistemas, de acuerdo con sus requerimientos específicos de evaluación y de acuerdo con su experiencia, conocimientos y habilidades.

El esquema de presentación de las auditorías de sistemas que seguiremos será el siguiente:

- *Auditoría con la computadora*
- *Auditoría sin la computadora*
- *Auditoría a la gestión informática del área de sistemas*
- *Auditoría al sistema computacional*
- *Auditoría alrededor de la computadora*

- *Auditoría de la seguridad de los sistemas computacionales*
- *Auditoría a los sistemas de redes*
- *Auditoría outsourcing a los sistemas computacionales*
- *Auditoría ISO-9000 en los sistemas computacionales*
- *Auditoría ergonómica de los centros de cómputo*
- *Auditoría integral a los centros de cómputo*

En aras de un mejor entendimiento, presentaremos nuevamente la definición de cada auditoría, así como algunos puntos que se podrían utilizar para cada tipo de auditoría, si el asunto informático así lo permite. El propósito es que el lector identifique todos los aspectos que le permitan adoptar, adaptar o modificar las sugerencias de evaluación informática que se pueden utilizar en esa auditoría, o que al analizar lo que ahí se propone pueda identificar aspectos similares que le ayuden a satisfacer sus necesidades específicas de evaluación de sistemas computacionales.

12.1 Auditoría con la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la auditoría que se realiza con el apoyo de los equipos de cómputo y sus programas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas pero sí susceptibles de ser automatizadas; dicha auditoría se realiza también a las actividades del propio centro de sistemas y a sus componentes. La principal característica de este tipo de auditoría es que, sea en un caso o en otro, o en ambos, se aprovecha la computadora y sus programas para la evaluación de las actividades que se revisarán, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoría.*

Esta auditoría se caracteriza porque al realizarla se cuenta con el apoyo de los equipos de cómputo y de sus programas de revisión específica para evaluar la propia área de sistemas, utilizando los servicios informáticos como si fueran elementos de soporte para auditar cualquier otra área de la empresa, no necesariamente computarizada pero sí susceptible de ser automatizada.

En esta auditoría se utilizan los sistemas computacionales de acuerdo con las necesidades específicas de las áreas a revisar, aprovechando las técnicas especiales de computación que ofrecen estos sistemas, mismas que se adaptan a las técnicas tradicionales de auditoría para realizar con ambos una revisión, evaluación y dictamen de las áreas de sistemas que serán auditadas. Esta auditoría también es aplicable a las propias actividades administrativas e informáticas del área de sistemas de la empresa.

Este tipo de revisiones de auditoría se puede clasificar de acuerdo con las siguientes aplicaciones específicas:

- Uso de la computadora y aplicaciones exclusivamente en auditorías de los sistemas computacionales de la empresa.
- Uso de la computadora y aplicaciones exclusivamente en auditorías de las demás áreas de la empresa.
- Auditorías con la computadora y aplicaciones, en combinación con las herramientas tradicionales, para evaluar los sistemas computacionales.

A continuación analizaremos cada una de estas aplicaciones.

12.1.1 Uso de la computadora y aplicaciones exclusivamente en auditorías de los sistemas computacionales de la empresa

En este tipo de auditorías se recurre al uso de los recursos informáticos con los cuales cuenta la empresa: sistemas computacionales, personal del área de sistemas, métodos, técnicas y procedimientos informáticos, desarrollo de programas especiales de software, programas especiales de evaluación informática y todos los demás elementos del sistema computacional, con el propósito de evaluar las funciones, operaciones y actividades informáticas que se realizan, tanto en los propios sistemas computacionales del centro de informática como en las demás áreas de la empresa que estén sistematizadas.

El auditor, no necesariamente de sistemas, puede utilizar la computadora como un auxiliar valioso en la recopilación, procesamiento y emisión de datos procesados en el sistema, mismos que le permitirán evaluar los aspectos que está auditando, a fin de emitir su dictamen sobre el uso de los sistemas, el cumplimiento de sus funciones y el desarrollo de las actividades y operaciones que se llevan a cabo dentro del centro de cómputo.

En un plano puramente práctico, el auditor de sistemas, o de cualquier otra disciplina de la auditoría, puede utilizar la computadora para evaluar muchos aspectos relacionados con las actividades del área de sistemas, o de las demás áreas de la empresa que cuenten con estos recursos informáticos, de la misma manera como utilizaría la computadora para obtener información del sistema, para procesarla en el mismo de ser necesario y emitir su opinión sobre el cumplimiento alcanzado, en comparación con lo esperado de esas áreas.

A continuación presentaremos una serie de posibles actividades del área de sistemas que pueden ser evaluadas mediante el apoyo de estos recursos informáticos, aclarando que con la presentación de esta lista sólo pretendemos ejemplificar el uso de la computadora como soporte de la actividad del auditor.

12.1.1.1 Auditoría del rendimiento y aprovechamiento del hardware y del software en las áreas de sistemas

En esta auditoría se aprovecha la computadora para evaluar, dentro del propio sistema, el uso y explotación de todos los componentes y recursos del sistema, ya sea por medio de programas internos o de programas diseñados ex profeso para ello; así encontramos que se pueden auditar por medio de los siguientes programas:

- ***Los programas específicos de revisión interna del sistema.*** *Son programas y utilerías diseñados por proveedores o desarrolladores para revisar el hardware, el software y los demás componentes del sistema, a fin de emitir un diagnóstico sobre el funcionamiento interno de dicho sistema. A continuación presentamos algunos ejemplos de estos programas:*

  COMIT.* *Es un programa que permite revisar el funcionamiento interno del sistema, desde el procesador hasta la memoria, pantallas, métodos de acceso de información, dentro otros aspectos. Este programa emite un listado del sistema revisado.*

  TO AUDIT. *Programa de revisión interna del sistema, similar al anterior.*
- *Los propios programas de auditoría que incluyen sistemas. Éstos son programas de aplicación específica que se utilizan para evaluar (y corregir) el funcionamiento de los componentes del sistema. Tenemos como ejemplos de estos programas las propias utilerías de los sistemas computacionales, sean PCs, redes o sistemas mayores, de las cuales no citamos ejemplos concretos.*
- *Los programas elaborados por personal del área de sistemas o desarrolladores externos. Estos programas son elaborados, interna o externamente, para evaluar aspectos específicos del software, ya sea el funcionamiento, aplicación o cualquier otro aspecto relacionado con el sistema operativo, con los lenguajes de programación, programas de desarrollo, programas de aplicación, utilerías o cualesquier programas que utilicen los sistemas computacionales. A continuación citaremos algunas de las muchas aplicaciones de estos programas:*

  Guard Dog Deluxe.[1] *Paquete que protege en Internet de la transferencia de controles ActiveX, pequeñas aplicaciones Java, Cookies y virus.*

  McAfee VirusScan Security. *Son programas elaborados con el propósito de evitar la entrada de virus informáticos en los sistemas computacionales, así como para erradicarlos de esos sistemas; existen muchas aplicaciones de estos programas: en archivos, paqueterías, sistemas operativos, memoria o en Internet.*

La computadora también se utiliza en algunos casos para valorar estadísticamente el rendimiento y aprovechamiento de los sistemas computacionales, en lo referente

* Tanto COMIT como TO AUDIT son programas aplicados por este autor para evaluar el funcionamiento de la arquitectura y componentes de las PCs.

al hardware, al software y a las bases de datos, entre muchas otras aplicaciones del sistema. De esto no presentamos ejemplos de aplicación, ya que obedecerían a usos concretos del auditor.

12.1.1.2 Auditoría a los métodos y sistemas de seguridad establecidos en el centro de cómputo

En esta auditoría la computadora se utiliza para evaluar los sistemas de seguridad de acceso al sistema, a las bases de datos, a los programas y a las aplicaciones específicas del sistema. Aquí el auditor utiliza la computadora, o una red, para valorar la manera en que están diseñadas, establecidas y protegidas las formas de acceso al sistema, los privilegios de uso, las contraseñas y las demás protecciones de los sistemas computacionales de la empresa.

En la parte que corresponde a la evaluación de la seguridad de los sistemas computacionales, en este mismo capítulo, ampliamos las opciones, características y aplicaciones concretas de auditoría para esta evaluación de la seguridad; aquí sólo mencionamos su existencia como una parte de la auditoría con la computadora.

12.1.1.3 Auditoría al rendimiento y aprovechamiento de los sistemas computacionales

Para estos casos, los sistemas informáticos se emplean para valorar el aprovechamiento de los sistemas de información de la empresa, ya sean *sistemas individuales (PCs), sistemas de redes locales (LANs), redes de área metropolitana (MANs), redes de área mundial (WANs), servidores de sistemas o sistemas mayores*; asimismo, se recurre al apoyo de los recursos de los sistemas computacionales para hacer la evaluación del rendimiento de los propios sistemas, de sus componentes, del manejo de la información, administración de las bases de datos, operación y configuración de los sistemas y de sus componentes, de las telecomunicaciones y de las instalaciones de los sistemas.

Cuando el auditor de sistemas o de cualquier otra disciplina de auditoría utiliza los recursos del sistema para auditar cada uno de los integrantes del propio sistema, su información y la administración de todos sus recursos, utiliza el hardware, software, información, capacidad de procesamiento y sus programas de cómputo, a fin de evaluar el aprovechamiento real del sistema computacional de la empresa; para ello compara, en el mismo sistema, el aprovechamiento y rendimiento obtenidos dentro de algún período, proceso o circunstancia específica con el comportamiento esperado en ese mismo lapso, proceso o situación; con esto obtiene el comportamiento real del sistema informático de la empresa, el cual le es de gran ayuda para hacer su evaluación e informe correspondientes.

Al utilizar la computadora como soporte para su evaluación de auditoría, el auditor también utiliza los siguientes programas:

- *Programas de evaluación del sistema que él mismo haya diseñado.*
- *Programas elaborados por desarrolladores de software, paqueterías de aplicación y evaluación de sistemas.*
- *Programas desarrollados por fabricantes, desarrolladores y distribuidores de hardware, software y componentes del sistema.*
- *Programas asociados al sistema operativo del propio sistema informático.*
- *Programas que desarrolla el personal informático del área, para evaluaciones específicas de los aspectos concretos que deben ser auditados.*

Debido a que estas aplicaciones de programas de evaluación por medio de los sistemas de la empresa son muy similares (diríamos iguales) a las expuestas en la sección anterior, solamente las mencionamos para conocimiento del lector, ya que en los siguientes tipos de auditorías las trataremos con mayor detalle.

12.1.1.4 Auditoría a la productividad del procesamiento de información

Otro aspecto que también puede ser evaluado con el apoyo de la computadora es la productividad de los sistemas computacionales de la empresa en cuanto al procesamiento de la información, lo cual se realiza a través del análisis de los resultados de los procedimientos de captura y procesamiento de datos, así como de emisión de resultados, cualesquiera que sean los sistemas computacionales utilizados en la empresa.

Lo realmente importante de la evaluación con el apoyo de la computadora es que el auditor puede evaluar la cantidad, calidad, oportunidad, confiabilidad, suficiencia, veracidad y congruencia de la información que se procesa en los sistemas de la empresa, comparando la productividad del procesamiento del sistema mediante el uso de datos ficticios, datos reales o un híbrido de ambos, esto mediante el diseño y aplicación de pruebas simuladas en el mismo sistema o con pruebas de aplicación a la actividad informática real de los sistemas y sus datos ya sea con operaciones, reales o simuladas de esos sistemas o por medio de cualquier otro método de evaluación y prueba. Lo importante para el auditor es evaluar el funcionamiento del sistema en cuanto a su productividad real, en comparación con su productividad esperada.

El auditor recurre a los siguientes puntos para hacer este tipo de evaluaciones:

- *Los programas de evaluación y prueba de la productividad del sistema diseñados por él mismo; por ejemplo:*
  - *— Programas de simulación de pruebas y de datos.*
  - *— Programas de pruebas con aplicación y datos reales.*
  - *— Programas híbridos de aplicaciones reales y datos ficticios o de aplicaciones simuladas y datos reales.*
- *Los programas elaborados por desarrolladores y diseñadores de software, paqueterías de aplicación y evaluación de sistemas, así como de diseño de bases de datos.*

- Los programas desarrollados por fabricantes, desarrolladores y distribuidores de hardware, software y componentes del sistema.
- Los programas asociados al sistema operativo, los cuales evalúan el procesamiento de la información que se procesa en el sistema.
- Los programas que desarrolla el personal informático del área, para evaluar pruebas y datos específicos de la información que debe ser auditada.

Debido a que estas aplicaciones de programas y pruebas para la evaluación de la productividad de los sistemas computacionales de la empresa son similares (diríamos casi iguales) a los expuestos en las secciones anteriores, sólo que especificados para los procesos de captura, procesamiento de datos y emisión de resultados sobre esa información, únicamente los mencionamos para conocimiento del lector, ya que en posteriores exposiciones los trataremos con mayor detalle.

12.1.2 Auditoría con la computadora a las áreas tradicionales

En este tipo de auditorías el auditor utiliza los servicios del sistema computacional, así como sus procedimientos y programas especiales de revisión específica, para realizar la evaluación de las demás áreas de la empresa, e incluso del área de sistemas como una entidad ajena a los sistemas que se manejan en dicha empresa.

El auditor realiza esta evaluación combinando la técnica tradicional de auditoría con los recursos del sistema computacional y aplicando algún software de auditoría o programas de evaluación que él mismo diseña de acuerdo con sus necesidades, con el fin de evaluar más objetivamente todas las áreas de una empresa, no sólo las sistematizadas, sino también las que tengan características especiales que le permitan sistematizar sus operaciones.

El propósito global de este tipo de auditorías es revisar las áreas, operaciones y sistemas de una organización, utilizando las técnicas y métodos tradicionales de auditoría, así como los sistemas computacionales de la empresa. De esta manera, el auditor de sistemas, o de cualquier otra disciplina de auditoría, obtiene una mejor aplicación de las técnicas, métodos y procedimientos tradicionales de la auditoría, y complementa dicha aplicación con la confiabilidad, oportunidad y veracidad que le proporciona el apoyo de los sistemas computacionales. Consecuentemente, realiza una mejor evaluación de las actividades, operaciones y funciones de esas áreas de la empresa, lo cual le ayuda a emitir un mejor diagnóstico y un dictamen más acertado.

En la práctica, este tipo de auditoría requiere de un amplio conocimiento de las técnicas, métodos y procedimientos de auditoría, así como de un profundo conocimiento del manejo, uso y aprovechamiento de los paquetes y programas de cómputo aplicables a la auditoría; en muchos casos es necesario hacer diseños especiales de programas de revisión, ya que son pocos los desarrolladores de software que se han enfocado a satisfacer las necesidades de los auditores no informáticos. Actualmente se encuentran en el mercado pocos programas y aplicaciones específicas de auditoría que cuenten las he-

rramientas, técnicas y procedimientos de la auditoría tradicional, que le permitan al auditor que no tiene experiencia en sistemas, evaluar los tópicos que no son informáticos de todas las áreas de una organización por medio de la computadora.

Para ampliar este punto, a continuación presentamos las siguientes subclasificaciones para este tipo de auditorías, atendiendo al ambiente en donde se aplicarán los programas de revisión.

12.1.2.1 Auditoría con el apoyo de paquetería de aplicación específica para auditorías tradicionales

En este caso, el auditor, de cualquier especialidad, utiliza la computadora para evaluar cualquier área de la empresa, incluso el área de sistemas computacionales; para ello se apoya en paquetería de aplicación específica para el tipo de auditoría que desea realizar; ya sea que esta paquetería exista, o mediante el diseño de aplicaciones especiales, de acuerdo con sus necesidades de evaluación.

La característica de esta auditoría es que se utilizan las herramientas tradicionales de la auditoría para auditar las diferentes áreas de la empresa, y se utiliza la computadora únicamente como apoyo para obtener la información que se requiere de esas áreas, para hacer el procesamiento de datos, e incluso para llevar a cabo simulaciones de las actividades normales de las áreas evaluadas, si así se requiere. Esto le permite al auditor hacer una evaluación más profunda, ahorrar tiempo y obtener resultados más confiables.

En la actualidad, con el concurso de los nuevos sistemas de redes de cómputo, en los cuales se comparten los recursos y se aprovecha mutuamente la información de la empresa, el auditor puede llevar a cabo su auditoría desde una terminal del mismo sistema de red; incluso, si la evaluación así lo requiere, puede monitorear las actividades, operaciones y manejo de la información de las áreas que audita, sin que el usuario lo note. Esto le permite evaluar con mayor profundidad esas áreas y le ayuda a realizar el seguimiento de la información y del manejo adecuado de los datos que está evaluando, así como el uso, confiabilidad y seguridad de la información de las áreas que evalúa. Si el auditor utilizara únicamente las herramientas tradicionales de auditoría, difícilmente alcanzaría tal profundidad.

Sin embargo, el principal problema en estas evaluaciones es la carencia de programas específicos de evaluación para una auditoría, lo cual obliga al auditor a realizar programas de revisión concreta de acuerdo con las características de las áreas que esté evaluando y con las necesidades de la propia revisión. No obstante, para los auditores que no están muy familiarizados con el uso de los sistemas es muy difícil elaborar estos programas, lo cual les obliga a recurrir al área de sistemas computacionales para que les elaboren dichos programas.

Debido a la diversidad de aplicaciones de este tipo de auditorías, no hemos presentado ejemplos, ya que éstos estarían en función de las necesidades específicas de

evaluación del auditor; solamente citamos la gran ayuda que proporciona la computadora para realizar estas auditorías.

12.1.2.2 Auditoría con el apoyo de paquetería de aplicación administrativa

Es la evaluación que se realiza utilizando los paquetes de software específicos, cuya aplicación es de carácter administrativo, financiero, contable o estadístico, los cuales han sido diseñados para que puedan ser utilizados en cualquier sistema computacional; es decir, en macrocomputadoras, minicomputadoras, microcomputadoras, laptops o sistemas de redes.

Con estos paquetes se facilitan las actividades de un auditor, debido a que, al aprovechar las facilidades que obtiene con el uso de dichos sistemas y programas, puede realizar una evaluación tradicional de los registros, operaciones, funciones y actividades de una empresa o una de sus áreas específicas, utilizando las técnicas, métodos y procedimientos típicos de la auditoría, pero apoyándose en los sistemas y programas para la captura y el procesamiento de datos; con la combinación de ambos obtiene los resultados que le facilitan hacer la interpretación, evaluación y dictamen de los aspectos resultantes de la evaluación administrativa de las actividades y operaciones de la empresa o de sus áreas.

En el mercado hay múltiples ejemplos de lo anterior, así que sólo presentaremos el nombre de algunos de estos programas:

- ***Diagnôstik.***[2] *Programa para el análisis y diagnóstico financieros que permite la evaluación del origen y aplicación de recursos, índices financieros, flujo de efectivo y rentabilidad de la empresa.*
- **Admiplus.*** Programa de administración empresarial que se utiliza para llevar a cabo la administración de la empresa, así como para auditar dicha administración.
- **COI.** Programa de contabilidad que se puede utilizar para realizar la contabilidad de la empresa y para la auditoría de la misma.
- **NOI.** Programa administrativo de nóminas que se utiliza para realizar la nómina del personal, el registro de sus ingresos, egresos y registros de impuestos en la computadora. También se puede utilizar para realizar la auditoría del área de personal.

12.1.2.3 Auditoría con el apoyo de hojas electrónicas de trabajo

Es la evaluación que se hace aplicando los métodos, técnicas y procedimientos de la auditoría tradicional, pero apoyándose para procesar sus resultados en los cálculos, estadísticas y gráficas que se obtienen con la aplicación de programas de hoja de cálculo.

* ADMIPLUS es una marca registrada por Grupo SP de México, S.A. de C.V.

Con estas hojas de cálculo, el auditor captura, procesa y emite los resultados derivados de los levantamientos de información que realiza con la aplicación de las herramientas tradicionales de auditoría, sólo que, en su tabulación y procesamiento se apoya en hojas de cálculo, con el fin de obtener resultados más confiables, acertados y oportunos, lo cual le permite hacer una mejor evaluación y elaborar un dictamen más eficiente.

Tradicionalmente, las hojas de cálculo se han utilizado en las aplicaciones contables, administrativas y estadísticas, facilitando la captura y el procesamiento de los datos obtenidos con las herramientas tradicionales; por esta razón se han popularizado entre los auditores para realizar el procesamiento de información en las auditorías de cualquier área o tópico de una empresa.

En el mercado hay múltiples ejemplos de estas hojas de cálculo, así que sólo presentaremos algunos nombres de estos programas:

- ***Hojas electrónicas de datos.*** *Son los programas de aplicación específica de programas integrados para realizar cálculos estadísticos, matemáticos y financieros en la computadora; entre estos programas, los más populares son* ***Excel*** *de Microsoft,* ***Lotus*** *de Lotus Develoment y Quatro, entre otros.*

12.1.2.4 Auditoría con el apoyo de programas de bases de datos

Es la evaluación de los datos y sistemas de procesamiento y archivo de bases de datos de una área o de toda la empresa; para realizar esta revisión se utilizan los métodos, técnicas y procedimientos de la auditoría tradicional, apoyándose en los datos que se obtienen de los sistemas computacionales y de los programas de manejo, procesamiento y almacenamiento de archivos y bases de datos. El auditor utiliza los datos y resultados arrojados por esos sistemas y, aplicando las herramientas tradicionales de auditoría, puede evaluar el comportamiento de la información y hacer su dictamen sobre la actuación de dicha información en áreas específicas o en toda la organización.

La auditoría tradicional se apoya en los programas de bases de datos para obtener los datos de un área en especial o de toda la empresa, y con ellos realiza pruebas y simulaciones del comportamiento de esos datos, lo que le permite verificar cómo se realiza el manejo de la información en las diferentes áreas de la empresa. Aquí se evalúan la administración y manejo de los aspectos específicos de la información, así como también que su procesamiento y almacenamiento sean adecuados. Con estas evaluaciones, apoyadas en equipos de cómputo, se obtienen auditorías más completas, confiables, acertadas y oportunas.

En este mismo capítulo trataremos más a fondo el manejo de las bases de datos que pueden ser aplicables a este punto; por esta razón no presentamos ejemplos al respecto.

12.1.2.5 Auditoría con el apoyo de paquetes contables

La auditoría más popular y que más utilizan las empresas y las autoridades hacendarias es la auditoría de carácter contable; en ésta, el auditor financiero realiza todas las actividades y procedimientos de la técnica contable, pero apoyándose en el equipo de cómputo para realizar la recopilación de los registros y operaciones contables de la organización, y privilegiando el uso de las técnicas, procedimientos y herramientas de la auditoría contable para evaluar el registro adecuado y la elaboración correcta de los estados financieros de la empresa. A veces se apoya en estos sistemas para realizar el procesamiento de información y los cálculos financieros de esta auditoría.

Las autoridades fiscales, por lo menos en muchos países, ya aceptan los registros de operaciones contables en sistemas de registro electromagnéticos (discos, CD-ROMs o cintas), en los que se asientan los resultados de las operaciones y los estados financieros de la empresa. Pero los equipos de cómputo sólo se utilizan para registrar y procesar las actividades contables, bajo las técnicas específicas de la auditoría financiera.

Como ejemplos, podemos ver los casos citados en el apartado correspondiente al apoyo de las paqueterías administrativas. Incluso, también se acepta el uso de las hojas de trabajo para el ejercicio de los registros contables de la organización.

12.1.2.6 Auditoría con el apoyo de diversas paqueterías

En esta evaluación, el auditor, de cualquier especialidad, utiliza las técnicas, métodos y procedimientos tradicionales de la auditoría, pero se apoya en los sistemas computacionales, programas, paqueterías y lenguajes específicos, con los cuales puede realizar adecuadamente la revisión de las áreas que debe evaluar.

Lo fundamental en este tipo de auditorías es que el auditor puede manejar libremente los sistemas, lenguajes, paquetes y programas que existen en el mercado, y en caso de que no existan programas que satisfagan sus necesidades, se apoya en el desarrollo de las aplicaciones informáticas que sí lo hacen, para así obtener los resultados deseados para su revisión. El propósito es procesar adecuadamente la información con las herramientas tradicionales de auditoría y emitir los resultados de esas aplicaciones especiales. Con estos resultados, el auditor puede hacer una evaluación adecuada de los resultados finales de las áreas auditadas y emitir un dictamen correcto sobre los aspectos evaluados.

A continuación presentamos algunos ejemplos de estas aplicaciones:

- *Los paquetes estadísticos y de aplicación financiera.*
- *Los programas de telecomunicación y teleprocesos de información.*
- *Los paquetes de contabilidad.*
- *Los sistemas para la emulación de sistemas y realización de pruebas.*

Los anteriores son sólo algunos de los muchos tipos de aplicaciones de sistemas concretos, las cuales se deben realizar de acuerdo con las necesidades específicas de

evaluación de las áreas, funciones y aplicaciones de una organización, así como con los conocimientos, experiencia y habilidades del auditor.

12.1.3 Auditoría con la computadora y aplicaciones combinadas en los sistemas de computo y herramientas tradicionales

Éste es un enfoque especial, en el que se combinan los dos tipos de auditorías que analizamos anteriormente; con la conjugación de ambas herramientas, la computación y la auditoría tradicional, se busca hacer una evaluación integral de los sistemas de información de la empresa, así como de sus demás áreas, funciones, operaciones y actividades. Esto se realiza mediante la aplicación de las técnicas, métodos y procedimientos tradicionales de la auditoría y con el apoyo de los sistemas computacionales, incluyendo su hardware, software y equipos periféricos para el procesamiento de datos y la emisión de resultados.

También se busca realizar una revisión integral de los propios sistemas computacionales de la empresa, sean del área de sistemas o de las demás áreas, contando con las herramientas tradicionales y con el apoyo de los sistemas computacionales para hacer las evaluaciones de los resultados obtenidos con ambas herramientas y poder elaborar el dictamen de sus propios sistemas y de las áreas, operaciones, funciones y procedimientos de toda la empresa.

Esta auditoría es una combinación natural de las dos que analizamos anteriormente y se desarrolla mediante el uso de los programas elaborados deliberadamente para hacer una auditoría de sistemas computacionales y de sus componentes, así como de las áreas, funciones, actividades y operaciones manuales, mecánicas y electrónicas de una empresa o de sus áreas funcionales.

Ejemplos clásicos de este tipo de auditoría son las revisiones integrales a la gestión administrativa y a los sistemas de procesamiento, centralizados o compartidos, ya que en ambos se pueden utilizar las herramientas típicas de auditoría con el apoyo de los sistemas computacionales para evaluar tanto los propios sistemas computacionales como las funciones, actividades y operaciones que se realizan en el centro de información, así como en las demás áreas de una empresa.

12.2 Auditoría sin la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de cómputo, y en sí de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos, pero dicha evaluación se realiza sin el uso de los sistemas computacionales. Es también la evaluación tanto a la estructura*

de organización, funciones y actividades de funcionarios y personal de un centro de cómputo, así como a los perfiles de sus puestos, a los reportes, informes y bitácoras de los sistemas, a la existencia y aplicación de planes, programas y presupuestos en dicho centro, así como del uso y aprovechamiento de los recursos informáticos para la realización de actividades, operaciones y tareas. Asimismo, es la evaluación de los sistemas de seguridad y prevención de contingencias, de la adquisición y uso del hardware, software y personal informático, y en sí de todo lo relacionado con el centro de cómputo, pero sin el uso directo de los sistemas computacionales.

En este tipo de auditorías, el auditor utiliza las técnicas, métodos y procedimientos tradicionales de revisión, con el propósito de hacer una evaluación manual del área de sistemas computacionales de la empresa, abarcando en ello todos los aspectos administrativos, contables, financieros, estadísticos, de personal y de las demás especialidades de las gestiones de carácter administrativo que intervienen en la operación de un centro de cómputo de una empresa, a fin de emitir un dictamen sobre la actuación de sus directivos y empleados, sobre el aprovechamiento y uso de todos los recursos asignados a esa área, en cuanto a sus equipos de computación, sus instalaciones y la administración de sus consumibles, así como sobre los planes, presupuestos y programas que afectan el comportamiento financiero de dicha área.

Esta revisión manual también se hace para evaluar la estructura de organización, las líneas de autoridad, las funciones y el perfil de puestos de los directivos y empleados del área de sistemas, la capacitación y adiestramiento de su personal y usuarios, la existencia y aplicación de los sistemas de seguridad y prevención de contingencias que puedan afectar el funcionamiento de la función informática de la empresa, así como los métodos de evaluación y adquisición del hardware, software y consumibles que se requieren en los sistemas computacionales de las distintas áreas de la empresa. Todas estas evaluaciones se realizan sin el uso de los sistemas computacionales.

Concretamente, podemos decir que este tipo de auditorías tiene como principal característica la realización de una evaluación del centro de cómputo, de su gestión administrativa y sus operaciones, realizando dicha evaluación, tabulación y emisión de resultados en forma manual, sin el apoyo de los sistemas computacionales, sino únicamente con las herramientas clásicas del auditor: calculadoras, recopilación documental, observación directa, comparación y los otros elementos tradicionales que se utilizan en este tipo de auditoría.

A continuación presentamos algunas gestiones concretas de carácter administrativo que pueden ser evaluadas de forma tradicional:

- *Auditoría a la actividad administrativa del centro de cómputo.*
- *Auditoría a la gestión financiera del centro de cómputo.*
- *Auditoría a la operación de los sistemas.*
- *Auditoría al desarrollo de los proyectos de sistemas computacionales.*

- *Auditoría a las técnicas y sistemas de procesamiento.*
- *Auditoría a los sistemas de seguridad y prevención de contingencias.*
- *Auditoría de los consumibles para el funcionamiento de los sistemas.*
- *Auditoría del uso y acceso a los sistemas y programas computacionales.*

Existen, desde luego, otros tipos de evaluaciones específicas para auditar las actividades y operaciones del centro de sistemas mayores, intermedios, compartidos o de aplicación personal de cualquier empresa, según las necesidades concretas de la auditoría y las actividades que se realizan en la gestión administrativa de dicho centro.

A continuación presentamos el uso de cada una de las auditorías especificadas anteriormente, con el único propósito de que el lector entienda su importancia.

12.2.1 Auditoría a la actividad administrativa del centro de cómputo

Es la revisión de las actividades administrativas de cualquier área de sistemas, la cual se realiza con las herramientas tradicionales de auditoría; esta revisión se practica a los siguientes aspectos: a la planeación, organización, dirección y control de las diferentes actividades del área de sistemas, al cumplimiento de las funciones, tareas y actividades encomendadas a los funcionarios, personal y usuarios del área de sistemas, al control financiero y contable de sus bienes informáticos, a los ejercicios del presupuesto asignado a dicha área, a la capacitación, adiestramiento y promoción del personal del área, al funcionamiento de los sistemas de procesamiento y al uso del equipo de cómputo, entre muchas otras acciones administrativas del área de sistemas que pueden ser evaluadas.

A continuación presentamos algunos aspectos que se evalúan en este tipo de auditorías:

- *Auditoría a los planes, programas y presupuestos que afectan al centro de información de la empresa.*
- *Auditoría a la estructura de organización, puestos, funciones, niveles de autoridad y canales de comunicación del centro de cómputo, según el tamaño, características y sistemas de procesamiento de la institución.*
- *Auditoría a la selección, capacitación, adiestramiento y promoción del personal del área y de los usuarios del sistema informático de la empresa.*
- *Auditoría a la administración, uso y métodos de control para el acceso y protección de los sistemas computacionales, de los programas institucionales y de la información de la empresa.*
- *Auditoría a la aplicación de las técnicas y métodos de dirección, supervisión, toma de decisiones, coordinación y de motivación del personal y de los usuarios del centro de cómputo.*

En el siguiente punto, *Auditoría a la gestión financiera de un centro de cómputo,* trataremos más ampliamente éstas y otras aplicaciones de este tipo de auditoría; esto obedece a que la auditoría administrativa es uno de los aspectos básicos que se utili-

zan para evaluar el centro de cómputo de cualquier empresa, dependiendo de las necesidades de revisión y de las características de los sistemas computacionales, de su tamaño, así como de las aplicaciones y servicios informáticos que éstos proporcionan a las demás áreas de la organización.

12.2.2 Auditoría a la gestión financiera del centro de cómputo

Ésta es prácticamente una auditoría de carácter financiero, en la cual se utilizan las técnicas, métodos y procedimientos de la auditoría contable para revisar la contabilidad y el manejo financiero del área de sistemas; esta revisión puede ser realizada por el área de contabilidad de la empresa o por el área de sistemas, si ésta lleva su propia contabilidad. Asimismo, con este tipo de evaluación se puede realizar el seguimiento de las operaciones y registros financieros que repercuten en el funcionamiento del centro de cómputo, así como de las aplicaciones de los programas financieros, la asignación de los presupuestos y el control de ingresos y egresos del área de sistemas, el ejercicio correcto y oportuno de los bienes informáticos de esta área y en sí se puede hacer el seguimiento de todos los aspectos financieros que repercuten en el funcionamiento del área de sistemas de la organización.

Además, en este tipo de auditoría, el auditor se apoya en los criterios determinados por el control interno contable y en los registros que afectan la protección de los bienes y activos del área de sistemas, así como sus actividades y operación, para evaluar las operaciones financieras de esta área y la protección de sus bienes y activos.

Este tipo de evaluación puede y debe ser realizada por un auditor especializado en la rama de la contabilidad y en la aplicación de las herramientas, métodos y procedimientos propios de esta clase de auditoría, debido a lo especializado de este tipo de evaluación. En razón de que la aplicación de esta auditoría contable es muy difundida y popular, no tiene caso citar ejemplos; sólo insistiremos en que esta auditoría debe tratar de cubrir todos los aspectos financieros y contables del centro de cómputo, lo cual omite auditar muchas veces el auditor especializado en el área de sistemas.

12.2.3 Auditoría a la operación de los sistemas

Es la evaluación del desempeño y cumplimiento correctos de las actividades, funciones, tareas y operaciones encomendadas a las áreas y unidades administrativas del área de sistemas de una empresa, utilizando las técnicas, métodos y procedimientos típicos de una auditoría operacional.

Con esta auditoría se busca verificar el cumplimiento adecuado de las operaciones y actividades encomendadas al área de sistemas, a fin de prevenir, o corregir, las posibles deficiencias en el manejo y operación del sistema de procesamiento de datos de la empresa, con todo lo que esta evaluación implica. También se busca evaluar las medidas preventivas y correctivas de seguridad de las áreas, sistemas y actividades de di-

cho sistema, así como los programas de contingencias informáticas para el mejor funcionamiento de las actividades y operaciones informáticas de la empresa.

Igual que en los casos anteriores, tampoco presentamos ejemplos de la aplicación de esta auditoría operacional en el área de sistemas, debido a que existe un sinnúmero de autores de administración y de ingeniería que abarcan las formas de evaluación a los aspectos operacionales de tiempos y movimientos, organización, métodos y procedimientos de operación, actividades fabriles y todas las demás herramientas de una evaluación operativa, sólo que en este caso éstas deberán estar enfocadas al área de sistemas.

12.2.4 Auditoría al desarrollo de los proyectos de sistemas computacionales

Es la revisión que se hace utilizando las técnicas, métodos y procedimientos tradicionales de auditoría, con el fin de evaluar, entre muchas otras cosas, el desarrollo correcto de los sistemas de aplicación que se perfeccionan en el área de sistemas de la empresa, analizando la forma en que se llevan a cabo los proyectos de sistemas, la interpretación adecuada de las necesidades de los usuarios, la forma en que se implantan estos sistemas en las áreas involucradas, la posible repercusión de su implementación en los actuales sistemas de información institucionales, así como la posible influencia en el funcionamiento de las actividades informáticas en las áreas de la empresa que utilizan estos sistemas.

Esta auditoría sin la computadora también se utiliza para evaluar la actualización en el diseño de los sistemas de procesamiento de datos y la operación de los equipos, periféricos y procesadores, de acuerdo con las necesidades de información de la empresa y con los avances tecnológicos de la informática, así como la capacitación necesaria para el personal y usuarios, derivada de la puesta en práctica de nuevos sistemas computacionales en el área de sistemas de la empresa.

En estas auditorías se utilizan las herramientas tradicionales de la auditoría, mismas que pueden ser aplicadas por cualquier auditor, debido a que el propósito es evaluar el uso de las metodologías y estándares institucionales para el análisis, diseño e implementación de los sistemas computacionales, así como los estándares, políticas y procedimientos para la programación, documentación, liberación y mantenimiento de un sistema que se desarrolla en el área de sistemas o de uno que se adquiere de proveedores y desarrolladores. También se evalúa todo lo relacionado con la administración y control de los proyectos de sistemas de esta área, en cuanto a la planeación, ejecución y liberación del sistema, incluyendo el manejo del personal y las herramientas de administración y control de su desarrollo.

A continuación presentamos algunos aspectos que se evalúan en este tipo de auditorías:

- *Evaluación de la existencia, seguimiento y cumplimiento de los planes, programas y presupuestos de elaboración de los proyectos de sistemas de la empresa.*

- *Evaluación de la existencia, difusión y cumplimiento de los estándares de análisis, diseño, codificación, implementación y mantenimiento de los nuevos sistemas computacionales en el área de sistemas.*
- *Evaluación de la existencia, uso y seguimiento de las metodologías institucionales para el desarrollo de los nuevos proyectos de sistemas de la empresa.*
- *Evaluación del desempeño, integración y cumplimiento de las funciones, actividades y tareas encomendadas al líder de proyectos, al personal asignado al área de sistemas y a los usuarios que intervienen en el proyecto de sistemas de la empresa, así como de los desarrolladores externos y proveedores de sistemas computacionales.*
- *Evaluación de la existencia, aplicación y cumplimiento de la planeación y control de los programas de actividades, tareas, eventos y tiempos para el desarrollo de los proyectos de sistemas de la empresa.*
- *Evaluación de la existencia, estandarización y uso de las herramientas, técnicas, métodos y procedimientos institucionales para el desarrollo de los proyectos de sistemas de la empresa, así como de la constante actualización e innovación tecnológica de dichos sistemas.*
- *Evaluación de las actividades de implementación, liberación y mantenimiento de los proyectos de sistemas elaborados en la empresa.*
- *Evaluación de las necesidades en cuanto a sistemas computacionales, así como del seguimiento de las soluciones de los problemas de dichos sistemas, de acuerdo con los estándares de desarrollo de proyectos en el área de sistemas.*

12.2.5 Auditoría a las técnicas y sistemas de procesamiento

Esta auditoría se realiza con el apoyo de las herramientas, métodos y procedimientos tradicionales de la auditoría, a fin de evaluar la manera en que se aplican, actualizan y aprovechan las técnicas específicas de la función informática, en cuanto al funcionamiento, explotación y aprovechamiento de los sistemas computacionales de la empresa, así como las técnicas, métodos y procedimientos utilizados para la captura procesamiento y almacenamiento de datos, la emisión de la información, la operación de los sistemas de seguridad, resguardo y custodia de la información procesada en el sistema del centro de cómputo, los programas institucionales y los propios sistemas de operación en beneficio de la función informática de la empresa.

Para practicar esta evaluación, es necesario que el auditor sea especialista en auditorías de sistemas, en ingeniería informática o disciplinas similares, puesto que el ejercicio de esta revisión exige un alto grado de conocimientos en informática, ya que está enfocada a evaluar los siguientes aspectos:

- *La problemática relacionada con el funcionamiento técnico del sistema computacional.*

- *Las causas, incidencias y repercusiones de las "caídas del sistema" y las medidas preventivas y correctivas del caso.*
- *La falta de aprovechamiento de los sistemas a causa de fallas de los componentes internos, externos, de las instalaciones, del personal informático o de los usuarios del sistema.*
- *La frecuencia del mantenimiento correctivo o la ausencia del mantenimiento preventivo para asegurar el funcionamiento correcto de los sistemas.*
- *La detección y frecuencia de errores en el procesamiento de la información.*

Éstos son sólo algunos de los casos de carácter técnico que el auditor de sistemas debe estar preparado para evaluar.

En estas auditorías se debe realizar una profunda evaluación de las técnicas y sistemas utilizados para el procesamiento de información del propio sistema, del funcionamiento de su arquitectura interna, de sus componentes y demás equipos asociados, a fin de revisar el aprovechamiento adecuado de los siguientes aspectos:

- *La configuración y arquitectura del sistema computacional, a fin de valorar que cumplan con las necesidades informáticas de la organización.*
- *Las actividades y operaciones técnicas del sistema, a fin de valorar la capacidad de procesamiento, velocidad, memoria y aprovechamiento de las configuraciones interna y externa del sistema, ya sea PC, red, cliente-servidor o sistemas mayores.*
- *Los tiempos productivos y no productivos del procesador, a fin de valorar su repercusión en la actividad informática de la empresa, en relación con los siguientes aspectos:*
  - *— La operación normal del sistema computacional.*
  - *— La captura, actualización y consulta de datos.*
  - *— El procesamiento de datos y la emisión de resultados.*
  - *— El desarrollo, codificación, compilación e instalación de los programas desarrollados en el área de sistemas.*
  - *— Los lapsos improductivos y no aprovechados en los que no se utilizan los periféricos, equipos asociados y demás componentes del sistema computacional del área de sistemas de la empresa.*
  - *— Los tiempos productivos e improductivos del personal del área y usuarios del sistema.*
  - *— Los tiempos productivos e improductivos en todas las actividades del área de sistemas, así como en las actividades del personal del área y usuarios del sistema.*
- *Las técnicas y actividades informáticas para evaluar el aprovechamiento y la producción del sistema, en cuanto a la operación de sus componentes internos (procesador, memorias, velocidad de procesamiento, etcétera) y de sus componentes externos (disco duro, tarjetas, impresoras, drives, módems, etcétera).*

En sí, aquí se revisan todas las actividades que repercuten de alguna manera en la operación correcta y en el funcionamiento adecuado de los sistemas de procesamiento del centro de informática de la empresa, así como todos los aspectos técnicos, administrativos e informáticos que influyen en las actualizaciones tecnológicas de los sistemas computacionales.

En los siguientes puntos analizaremos con mayor profundidad esta evaluación al equipo de cómputo, anticipando que en estos casos se hace la evaluación únicamente con las técnicas tradicionales de auditoría y sin el uso de los sistemas computacionales, mientras que, en lo que se analiza para esos puntos, se evalúan contando con los sistemas de cómputo en forma completa.

12.2.6 Auditoría a los sistemas de seguridad y prevención de contingencias

Es la evaluación, con las herramientas tradicionales de auditoría, de la existencia, aplicación y operación de los sistemas y métodos de seguridad establecidos para el funcionamiento correcto de un centro de cómputo, así como de la protección de sus bienes informáticos, como sistemas computacionales, equipos, instalaciones e información, de los accesos de personal y usuarios, de la prevención de desastres, de los planes contra contingencias y demás posibles riesgos, tanto lógicos como físicos, que repercuten en la seguridad de dicho centro.

En estas auditorías se deben evaluar a fondo las medidas preventivas y correctivas, los métodos y procedimientos y los planes y programas contra contingencias; es decir, los sistemas de seguridad establecidos para evitar los riesgos y contingencias en los sistemas, equipos, instalaciones e información, así como para mantener la seguridad del personal de un centro de cómputo.

Tampoco presentamos ejemplos de esta auditoría, ya que en los puntos siguientes trataremos más a fondo los aspectos que se deben evaluar en una auditoría a la seguridad de los sistemas computacionales.

12.2.7 Auditoría de los consumibles para el funcionamiento de los sistemas

Ésta es una auditoría de carácter contable, en la que se utilizan las herramientas tradicionales de la auditoría financiera para evaluar todo lo relacionado con las instalaciones, equipos adicionales, periféricos, consumibles (disquetes, cintas, papelería y útiles de oficina) y todos los elementos que afectan el funcionamiento de un centro de cómputo, así como para evaluar el control del mantenimiento, tanto preventivo como correctivo, de las instalaciones físicas y lógicas de dicho centro.

Dentro de estas técnicas, métodos y procedimientos de auditoría se incluyen la realización de inventarios, la revisión a los resguardos y asignación de equipos, la seguridad y custodia de sus sistemas operativos, programas y paqueterías de procesa-

miento de información, así como de todo lo relacionado con la salvaguarda, custodia y mantenimiento de los activos del centro de cómputo.

Debido a que estas auditorías son las más comunes y las que más practican los auditores tradicionales, no mencionamos ejemplos de su aplicación en las áreas de sistemas, ya que hay mucha información sobre estas revisiones y la experiencia del auditor contable es fundamental para aplicarlas correctamente.

12.2.8 Auditoría del uso y acceso a los sistemas y programas computacionales

Es la evaluación, con la aplicación de las técnicas, métodos y procedimientos de la auditoría tradicional, del uso de los sistemas computacionales, de los medios y programas de acceso a éstos, así como de los lenguajes, programas y paqueterías utilizadas para el procesamiento de información del área de sistemas y de las áreas de la empresa a las que se les proporcionan estos servicios, ya sean para los sistemas centralizados, descentralizados o compartidos.

En dicha evaluación se incluyen la utilización de sistemas, programas y jerarquías de acceso a la información, las medidas y sistemas de protección para el sistema computacional, los privilegios de acceso lógico, el almacenamiento de la información y de los resultados de los procesamientos de datos, así como todos los medios de operación que repercuten en dicho sistema.

En la evaluación al sistema computacional ampliaremos estos conceptos, pero en esos casos aplicando las herramientas de cómputo para realizar estas evaluaciones.

Para concluir, diremos que con el análisis de este tipo de auditoría podemos entender cómo se aplican las técnicas, métodos y procedimientos tradicionales de la auditoría para evaluar un centro de cómputo, sus actividades y operaciones, con el fin de poder dictaminar sobre el buen desempeño de sus funciones, la protección y uso adecuado de sus sistemas, instalaciones, equipos, periféricos, consumibles, información y personal, así como de sus sistemas de acceso físico y lógico.

Todo esto se realiza sin el uso de la computadora, sólo con las herramientas tradicionales de la auditoría.

Evidentemente, estos tipos de auditoría tienen ciertas limitaciones y se pueden encontrar serias deficiencias al aplicarlos en el ambiente de sistemas computacionales; sin embargo, el propósito de este libro no es señalar las ventajas y desventajas de estas auditorías sin la computadora, sino presentarlas con el único fin de que el auditor las identifique como parte de las auditorías que se pueden practicar a los sistemas computacionales, y para señalarle al auditor ajeno a los sistemas que utilizando sus herramientas tradicionales de evaluación, también puede realizar estas evaluaciones informáticas. La profundidad y utilidad de estas evaluaciones dependerá de la habilidad del auditor, así como de su experiencia y conocimientos sobre las herramientas, métodos y procedimientos que utilice.

12.3 Auditoría a la gestión informática del área de sistemas

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como la planeación, organización, dirección y control de dicho centro. Esta auditoría también se realiza con el fin de verificar el cumplimiento de las funciones y actividades asignadas a los funcionarios, empleados y usuarios de las áreas de sistematización, así también para revisar y evaluar las operaciones del sistema, el uso y protección de los sistemas de procesamiento, de los programas y de la información. Se aplica también para verificar el desarrollo correcto, instalación, mantenimiento y explotación de los sistemas computacionales, así como de sus equipos e instalaciones. Todo esto se lleva a cabo con el propósito de dictaminar sobre la adecuada gestión administrativa de los sistemas computacionales de una empresa y del propio centro informático.*

Este tipo de auditoría sirve para evaluar la gestión administrativa del sistema computacional, el funcionamiento correcto de su hardware, software, componentes asociados, así como las instalaciones, programas, información, mobiliario, equipos y demás activos informáticos del área de sistemas de la empresa; también sirve para evaluar el cumplimiento adecuado de las funciones, operaciones y actividades de carácter administrativo que ayudan a satisfacer las necesidades de información de las áreas de la empresa que utilizan sistemas computacionales, a fin de hacer más eficiente el desempeño del centro de cómputo.

En estas auditorías se debe evaluar la gestión administrativa de la actividad informática de la empresa y del área de sistemas, y también la gestión netamente administrativa de los directivos, empleados y usuarios de dicha área. Sin embargo, con alarmante frecuencia esta evaluación no se realiza, se evita o se realiza muy superficialmente. Esto se debe en gran medida a la poca importancia que algunos "administradores de sistemas" otorgan a esta actividad tan importante.

Lo que realmente se busca con esta auditoría de carácter administrativo es evaluar la gestión administrativa del centro de cómputo de la empresa, aplicando cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro. Esta auditoría bien puede ser realizada por un auditor de sistemas computacionales, administrativo u operacional, siempre y cuando contemple en su revisión, entre otras cosas, los siguientes aspectos:

- *Auditoría a la planeación estratégica en la empresa y el área de sistemas.*
  - *Misión de la actividad informática.*
  - *Visión de la actividad informática.*
  - *Objetivos generales y específicos de la actividad informática.*

— *Estrategias para el funcionamiento de la actividad informática.*
— *Funciones fundamentales para proporcionar el servicio informático a las áreas de la empresa.*
— *Políticas, normas y lineamientos que regulen la actividad informática en la empresa y en el área de sistemas.*
— *Procedimientos generales para proporcionar la actividad informática.*
— *Existencia, difusión, seguimiento y control de la misión, visión, objetivo, políticas, normas, lineamientos y procedimientos para la actividad informática de la empresa.*

- *Auditoría a la estructura de organización del área de sistemas.*
  — *División funcional (u otro criterio) para el área de sistemas.*
  — *Estructura de puestos del área de sistemas.*
  — *Funciones de los puestos del área de sistemas.*
  — *Canales formales e informales de comunicación en el área de sistemas.*
  — *Niveles de autoridad y responsabilidad de los puestos del área de sistemas.*
  — *Reestructuración o actualización de puestos.*
  — *Perfiles de puestos.*
  — *Estructuras para el desarrollo de proyectos, atención a usuarios y operación de las actividades informáticas de la empresa.*
  — *Manuales de organización, procedimientos, operación y demás documentación normativa del área de sistemas.*
- *Auditoría al cumplimiento de las funciones, tareas y operaciones de la actividad informática en la empresa y el área de sistemas.*
  — *Existencia, difusión y cumplimiento de las funciones, tareas y operaciones de la actividad informática en el área de sistemas.*
  — *Seguimiento de los manuales e instructivos del área de sistemas.*
  — *Métodos y procedimientos para la actividad informática en la empresa y el área de sistemas.*
  — *Cumplimiento de los fundamentos y principios administrativos aplicables al área de sistemas de la empresa.*
- *Auditoría a la dirección del área de sistemas.*
  — *Ambiente laboral en el área de sistemas.*
  — *Estilo de liderazgo y ejercicio de autoridad en el área de sistemas.*
  — *Jerarquías de autoridad y responsabilidad en el área de sistemas.*
  — *Coordinación del personal y usuarios del área de sistemas.*

— *Coordinación de los recursos informáticos utilizados para la actividad informática en el área de sistemas y en la empresa.*

— *Relaciones de trabajo jefe-subordinado e iguales.*

— *Ejercicio y control de la toma de decisiones en el área de sistemas.*

— *Integración de grupos de trabajo en el área de sistemas.*

— *Relaciones de comunicación formal (comunicación escrita, verbal, correo electrónico u otras formas de comunicación) en el área de* sistemas.

- *Auditoría a la administración del factor humano en el área de sistemas.**
  — *Coordinación de las funciones, actividades, tareas y operaciones del personal informático del área de sistemas.*
  — *División funcional de las funciones, actividades y operaciones del factor humano del área de sistemas.*
  — *Planes y programas de capacitación, adiestramiento y promoción del personal y usuarios del área de sistemas.*
  — *Rotación y movilidad del personal del área de sistemas.*
  — *Motivación para el personal y usuarios del área de sistemas.*
  — *Procesos de selección de personal para el área de sistemas.*
  — *Remuneración y prestaciones para el personal del área de sistemas.*
  — *Integración de grupos de trabajo.*
  — *Evaluación del cumplimiento de las funciones y actividades del personal, del perfil de puestos y la asignación de actividades en el área de sistemas.*
  — *Estudios ergonómicos para el personal y usuarios del área de sistemas.*
  — *La gestión directiva de funcionarios, empleados y usuarios.*
- *Auditoría a la administración de los recursos informáticos no humanos del área de sistemas.*
  — *Administración de los sistemas computacionales (hardware) del área de sistemas y de los sistemas de las demás áreas de la empresa.*
  — *Administración del sistema computacional (software) del área de sistemas y del sistema de las demás áreas de la empresa.*
  — *Administración de las instalaciones del sistema computacional del área de sistemas y de las instalaciones de las demás áreas de la empresa que cuenten con sistemas.*

* En la sección 9.5.6. del capítulo 9 de este libro, tratamos la división natural del personal que labora en el área de sistemas, el cual se clasifica de la siguiente manera: personal adscrito al área de sistemas, usuarios, asesores y consultores, así como distribuidores, proveedores y desarrolladores externos de sistemas. Esto es totalmente aplicable en la auditoría de este tipo.

  - *— Administración de las telecomunicaciones del sistema computacional del área de sistemas y de las telecomunicaciones de las demás áreas de la empresa que cuenten con sistemas.*
  - *— Administración de las bases de datos e información del área de sistemas y de las bases de datos de las demás áreas de la empresa que cuenten con sistemas.*
  - *— Administración del mobiliario y equipo asignados al área de sistemas y del mobiliario de las demás áreas de la empresa que cuenten con sistemas.*
  - *— Administración de los bienes materiales, consumibles y materiales de oficina utilizados en el área de sistemas y de los materiales de las demás áreas de la empresa que cuenten con sistemas.*
  - *— Administración de las adquisiciones de sistemas computacionales, hardware, software, componentes, periféricos, mobiliario, equipos, consumibles y demás implementos para el funcionamiento de los sistemas de la empresa.*
  - *— Administración de los bienes informáticos y activos del área de sistemas y de los bienes informáticos de las demás áreas de la empresa que cuenten con sistemas.*
  - *— Los planes, programas y presupuestos que afectan al área de sistemas.*
  - *— La gestión financiera y contable de los recursos del áre*a de sistemas.
- *Auditoría a los controles informáticos del área de sistemas.**
  - *— Controles internos sobre la organización del área de sistemas.*
  - *— Controles internos sobre el desarrollo de sistemas.*
  - *— Controles internos sobre la operación del sistema.*
  - *— Controles sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados.*
  - *— Controles internos sobre la seguridad en el área de sistemas.*
- *Evaluación de la existencia, establecimiento y uso de los estándares de sistemas para:*
  - *— Metodologías del análisis y diseño de sistemas.*
  - *— Uso de software, lenguajes y programas de desarrollo para la programación y codificación de sistemas.*
  - *— Elaboración y seguimiento de pruebas y simulaciones de sistemas, programas y lenguajes de cómputo nuevos, así como para erradicar virus informáticos.*
  - *— Liberación e implementación de nuevos sistemas.*
  - *— Capacitación y adiestramiento del personal y los usuarios del área de sistemas.*

* En el capítulo 5 de este libro analizamos el control interno informático. Además, en el capítulo 4 también analizamos el control interno, ambos aplicables en este tipo de auditoría.

— *Documentación de sistemas.*
— *Adquisiciones de sistemas computacionales, así como de sus materiales y demás componentes y consumibles.*
— *Los demás estándares que regulen el desempeño de la función informática en la empresa.*

- *Auditoría a la documentación de los sistemas en al área de informática y a la documentación de las demás áreas de la empresa que cuenten con servicios informáticos*.
  — *Manuales de usuarios.*
  — *Manuales técnicos del sistema.*
  — *Manuales de capacitación.*
  — *Manuales de operación.*
  — *Bitácoras de proyectos nuevos.*
  — *Documentación de pruebas y simulaciones de sistemas.*
  — *Actualización de manuales.*
  — *Existencia, difusión, préstamo y uso de los manuales e instructivos de sistemas computacionales.*

Los puntos señalados anteriormente son algunos de los muchos aspectos que se pueden evaluar en una auditoría de carácter administrativo de un centro de cómputo; estos puntos nos señalan, a grandes rasgos, los asuntos más importantes que se deben tomar en cuenta para evaluar la gestión informática de un área de sistemas.

Sin embargo, es conveniente señalar que esos proyectos de evaluación administrativa se presentan únicamente como sugerencias, ya que el auditor de sistemas tiene la potestad de adaptar aquellos aspectos que le sean útiles para su evaluación, tomando en cuenta las características del área de sistemas que va a evaluar, sus costumbres y lineamientos administrativos esenciales y todos los fundamentos para administrar dicha área. Además, el auditor debe diseñar sus instrumentos de evaluación de acuerdo con su experiencia, conocimientos y habilidades, así como con las peculiaridades de la evaluación administrativa que practique.

Recordemos que con estas auditorías se busca evaluar la participación de la gestión administrativa en el manejo, operación y control de los sistemas computacionales asignados a las áreas de sistematización, con el fin de dictaminar sobre el uso correcto, manejo adecuado y explotación eficiente de esos sistemas en el procesamiento de información. Estas auditorías también sirven para evaluar la administración del personal y de los bienes informáticos asignados a las áreas de sistemas de la empresa, la administración de los sistemas y métodos de seguridad y prevención de contingencias, así como la adquisición de software y hardware de los sistemas computacionales.

12.3.1 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría a la gestión informática

Como recomendación final para la práctica de esta auditoría, sugerimos al auditor que utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de acuerdo con su experiencia, conocimientos y habilidades en el manejo de esta auditoría. Además, ya que en la auditoría a la gestión informática del área de sistemas de la empresa se tocan los aspectos administrativos, sería de mucha utilidad que el responsable de la auditoría contara con la participación de un auditor administrativo, pero bajo un estricto enfoque de administración de sistemas, jamás desde la óptica de la actividad administrativa de las demás áreas de la empresa.

Es recomendable que el auditor de sistemas novato utilice las siguientes herramientas, siguiendo cada uno de los puntos anotados anteriormente para la evaluación de la gestión informática:

- *El diseño de* **entrevistas** (sección 9.1) ***cuestionarios*** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas acordes a las necesidades de su evaluación. Con ello tendrá la oportunidad de revisar los principales aspectos relacionados con la gestión informática del área de sistemas. Además, también debe utilizar las técnicas de* **observación** *del funcionamiento normal de las funciones y actividades de la empresa* (sección 9.4)*, así como los* **inventarios** *de recursos y personal informático* (sección 9.5)*, cuando el caso lo requiera.*

Algunas de las técnicas que complementan la evaluación a esta actividad de las áreas de sistemas son la siguientes:

- *Las técnicas de* **revisión documental** (sección 10.5) *complementadas con la* **matriz de evaluación** (sección 10.7) *o* **la matriz DOFA** (sección 10.8)*, según las preferencias y necesidades de revisión del auditor, ya que así le permitirán analizar las debilidades y fortalezas de la administración del área de sistemas, así como las amenazas a la administración y las áreas de oportunidad de la gestión administrativa de la función informática de dicha área.*

Es indispensable que el responsable de esta auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría a la gestión informática del área de sistemas:

- *Una* **guía de evaluación** (sección 11.1)*, a fin de planear específicamente cada uno los aspectos sustantivos de la actividad administrativa que tiene que evaluar. Para ello es recomendable que tome en cuenta cada uno de los puntos indicados para realizar la auditoría a la gestión informática, adaptándolos e incluso modificándolos conforme a sus propias necesidades de evaluación, así como conforme a las características propias del área de sistemas que vaya a auditar.*

Un buen elemento de control para el responsable de esta evaluación es el siguiente:

- *La* **lista de chequeo** (sección 11.6)*, ya que puede verificar que quien practique la auditoría cubra todos los puntos descritos en su planeación de auditoría. Inclusive, debido a la facilidad para utilizar esta herramienta, puede verificar la existencia y uso adecuado de cada uno de los puntos que audite.*

En todas las sugerencias anteriores se debe tomar en cuenta que son eso, sugerencias, y que es potestad absoluta del auditor responsable de la auditoría utilizar las técnicas, métodos y procedimientos de auditoría que más le agraden, e incluso utilizar o adaptar los puntos indicados inicialmente para realizar esta auditoría.

12.4 Auditoría al sistema computacional

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, así como de su hardware, software y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o externas, así como al diseño, desarrollo y uso del software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se encuentra el equipo de cómputo que será evaluado. Se incluye también la operación del sistema.*

Lo que se busca con este tipo de auditorías es evaluar exclusivamente el equipamiento del sistema computacional, a fin de analizar su funcionamiento adecuado; esto se realiza con los propios sistemas computacionales o con las técnicas, métodos, procedimientos y herramientas diseñadas especialmente para practicar estas auditorías de sistemas. Lo importante de estas revisiones es evaluar, exclusivamente, el sistema computacional, tanto desde el punto de vista físico (hardware) como desde el punto de vista lógico (software), así como todos los elementos que ayudan a su funcionamiento, incluyendo las funciones de su personal y usuarios, la información, telecomunicaciones y demás componentes del sistema.

En la realización de estas auditorías se tienen que considerar las características propias de este tipo de revisiones, lo cual las hace un trabajo muy especializado que sólo pueden realizar los auditores que tienen conocimientos profundos sobre el área de sistemas, debido a que contiene aspectos muy específicos y característicos que son exclusivos de los sistemas computacionales. No obstante, cualquier auditor que no tenga experiencia en sistemas computacionales puede llegar a practicar esta auditoría,

si aplica los recursos informáticos especializados que necesita y los complementa con su experiencia y conocimientos de las herramientas, técnicas y procedimientos necesarios para evaluar estos sistemas, así como con su habilidad para obtener información útil para realizar su auditoría.

Es difícil tratar de englobar en unas cuantas líneas los principales aspectos que deben ser evaluados en una auditoría de sistemas computacionales, ya que es obvio que intervienen muchas particularidades de los propios sistemas computacionales. Debemos considerar que no es lo mismo auditar un sistema de red de área local que uno de área metropolitana, mundial o de red virtual; tampoco es lo mismo evaluar el procesamiento de una plataforma para MS-DOS y Windows, que para Unix o para AS-400, y no es lo mismo evaluar la arquitectura de una PC, de un servidor o de un sistema mayor.

Asimismo, las aplicaciones administrativas para los sistemas comerciales de una empresa comercializadora son diferentes a las de una institución dedicada al desarrollo de software, por citar algunos ejemplos.

En todos los casos existen características propias de los sistemas que los hacen diferentes unos de otros; es evidente que las técnicas, herramientas, procedimientos y métodos de auditoría que se utilizan también son muy diferentes.

En relación con lo anterior, a continuación presentamos algunas de las muchas consideraciones que se deben tomar en cuenta sobre los sistemas computacionales:

- *El tipo del procesador del sistema computacional, así como su velocidad, capacidad, memoria y demás características con los cuales opera el sistema de cómputo.*
- *Los fabricantes del hardware, software y periféricos del sistema computacional.*
- *Las características y especificaciones del diseño del sistema computacional.*
- *Las plataformas, ambientes, el tamaño y configuración del sistema computacional.*
- *Los sistemas operativos, lenguajes, programas de desarrollo y aplicación, utilerías y demás software del sistema computacional.*
- *La forma de administrar el sistema y sus componentes asociados.*
- *El sistema de administración de bases de datos e información manejado.*
- *La arquitectura del sistema, sus periféricos, equipos asociados y demás componentes.*
- *Las aplicaciones concretas para las que está destinado el sistema computacional.*

Además de estos aspectos, se deben tomar en cuenta diversas características que serán diferentes de un sistema a otro, y que por obvias razones variarán de un área de sistemas a otra.

En relación con estos grandes grupos de características, existen muchos puntos que el auditor de sistemas debe tomar en cuenta para evaluar los sistemas computacionales. A continuación presentamos algunos aspectos que se deben evaluar en este tipo de auditorías:

12.4.1 Auditoría al sistema computacional según las características de su hardware

Los aspectos más importantes de un sistema computacional son su parte física (hardware) y su parte lógica (software); por esta razón, el auditor de sistemas debe evaluar todo lo relacionado con los componentes físicos, tanto internos como externos, del sistema, tales como su procesador, periféricos, arquitectura y sus demás partes tangibles, con el propósito de evaluar su funcionamiento correcto.

En este tipo de evaluación, el auditor de sistemas debe conocer las principales características, componentes y funcionamiento de la parte física de los sistemas, a fin de poder evaluar su aplicación, uso y aprovechamiento adecuados en la función informática en la empresa.

Debido a que sería demasiado engorroso tratar de detallar todas y cada una de las partes del hardware que tienen que ser evaluadas, a continuación presentamos los componentes más significativos de la parte física de los sistemas, a fin de que el auditor tenga puntos de referencia para determinar los aspectos concretos y específicos que analizará en su evaluación.

- *Tarjeta madre del sistema.*
  - *Fabricante, tipo, versión del BIOS, configuración y componentes.*
  - *Arquitectura, componentes y características de la tarjeta madre.*
  - *Conjunto de chips.*
  - *Ranuras de expansión para Bus.*
  - *Ranuras de expansión tipo PCI.*
  - *Ranuras de expansión tipo ISA.*
  - *Capacidad máxima en RAM.*
  - *Ranuras de expansión de memoria (SIMM y DIMM).*
  - *Puertos paralelos, seriales y para ratón.*
  - *Socket para multiprocesadores.*
  - *Bahías para unidades accesibles en parte frontal e interna.*
  - *Capacidad del voltaje de la fuente de energía.*
  - *Capacidad máxima en ROM, EROM y EPROM.*
  - *Conexiones periféricas.*
- *Procesador.*
  - *Fabricante, marca, tipo, configuración y características.*
  - *Velocidad de procesamiento en Mhz.*
  - *Máxima memoria en RAM del sistema.*
  - *Memoria caché y RAM externa.*

— *Coprocesador matemático.*
— *Conjunto de chips (fabricante, modelo, capacidad y características).*
— *Administrador de memoria.*

- *Unidades adicionales, características, interfaz y capacidad.*
  — *Unidades de discos flexibles.*
  — *Discos duros (fabricante, capacidad, características y número).*
  — *Unidades de CD-ROM, DVD, CD-R (modelo y velocidad.)*
  — *Unidades de cinta.*
  — *Dispositivos multimedia (sonido, tarjetas, bocinas, multimedia y sintetizador).*
  — *Fax módem (marca, modelo, velocidad en Kbps).*
  — *Soporte para gráficos (fabricante, capacidad en RAM e interfaz).*
  — *Monitor (fabricante, modelo, tamaño y características).*
  — *Teclado, ratón, JOYSTICK.*
- *Tarjetas adicionales al sistema.*
  — *Tarjeta aceleradora de gráficos.*
  — *Tarjetas para red.*
  — *Tarjeta para multimedia.*
  — *Tarjeta para fax módem.*
  — *Muchas otras tarjetas a través de extensiones del sistema.*
- *Periféricos externos asociados al sistema.*
  — *Impresoras (fabricante, modelo, tamaño y características).*
  — *Sistemas de videoconferencia (fabricante, modelo, alcance, nitidez y características).*
  — *Escáner y dictador de textos.*
- *Aprovechamiento y utilidad de cada uno de los componentes internos y periféricos del sistema.*
  — *Monitor, teclado, ratón y unidad de disco flexible.*
  — *CD-ROM, CD-RW, DVD y disco duro.*
  — *Conexiones de periféricos, de conectividad y de comunicación.*
- *Aprovechamiento y utilidad del sistema computacional.*
  — *Capacidad para el crecimiento del sistema.*
  — *Calidad de los componentes del sistema (fabricante, marca y características).*
  — Obsolescencia y durabilidad del equipo (sistema y componentes).
  — Garantía y soporte del fabricante.

- Mantenimiento básico para los sistemas.
  - — Mantenimiento preventivo y correctivo (frecuencia y resultados).
  - — Sistemas reguladores de corriente y no-breaks.
  - — Instalaciones y conexiones eléctricas y de tierra.
  - — Protección del medio ambiente contra humedad, polvo y estática.

12.4.2 Auditoría al sistema computacional según las características de su software

El alma del funcionamiento de un sistema computacional es el sistema operativo, los lenguajes y programas de desarrollo, los programas y paqueterías de aplicación y las utilerías empleadas para su funcionamiento. Todo concentrado en el llamado software del sistema.

A causa del gran volumen, diversidad de lenguajes, paquetes, programas y aplicaciones, así como a su permanente actualización, también sería casi imposible auditar todas y cada una de las actualizaciones y presentaciones del software; por esta razón, a continuación sugerimos los aspectos más significativos que se pueden evaluar de esta parte lógica de los sistemas, agrupados en los renglones más significativos del software, o por lo menos en los más identificados, con el único propósito de que el auditor tenga puntos de referencia para elegir los aspectos específicos para ejecutar su evaluación:

- *Auditoría al sistema operativo.*
  - — *Fabricante, características y operabilidad.*
  - — *Plataforma y ambientes de aplicación.*
  - — *Licencias y permisos.*
  - — *Versión, actualizaciones, cambios e innovaciones.*
  - — *Manuales e instructivos técnicos, de operación, de programación y demás documentación relacionada con el funcionamiento del lenguaje.*
  - — *Facilidad para la administración del sistema operativo.*
  - — *Sistemas, rutinas y programas para la seguridad y protección de los datos y del sistema operativo.*
  - — *Tecnología de aprovechamiento.*
  - — *Compatibilidad y escalabilidad con otros sistemas operativos.*
  - — *Ventajas y desventajas.*
- *Auditoría a los lenguajes de desarrollo.*
  - — *Fabricantes, características y operabilidad del lenguaje.*
  - — *Plataforma y ambientes de aplicación y desarrollo.*

— *Versión, actualización y utilidad para el sistema.*
— *Facilidad de compilación y traducción al lenguaje de máquina.*
— *Uso y generación de códigos y programas fuentes, seudocódigos, programas objeto y programas ejecutables.*
— *Librerías, bibliotecas, herramientas y utilerías para programación.*
— *Facilidad de programación y desarrollo.*
— *Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.*
— *Administración del lenguaje.*
— *Sistemas para la seguridad y protección de los datos y del propio lenguaje.*
— *Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otras plataformas y lenguajes.*
— *Ventajas y desventajas.*
— *Requerimientos de capacitación y especialización.*

- *Auditoría a los programas de desarrollo.*
  — *Fabricantes, características y operabilidad.*
  — *Plataforma y ambientes de aplicación y explotación.*
  — *Versión, actualización y utilidad para el sistema.*
  — *Licencias y permisos.*
  — *Facilidad de traducción, comunicación y compilación en lenguaje de máquina.*
  — *Librerías, bibliotecas, herramientas y utilerías para programación.*
  — *Programas para bases de datos.*
  — *Facilidad de programación (visual y de codificación).*
  — *Uso y generación de programas fuentes, programas objeto, programas gráficos y programas ejecutables.*
  — *Compatibilidad, exportabilidad y escalabilidad con otros lenguajes y programas.*
  — *Sistemas para la seguridad y protección de los datos y del propio programa.*
  — *Administración del programa de aplicación.*
  — *Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.*
  — *Requerimientos de capacitación y especialización.*
  — *Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otros sistemas, plataformas, lenguajes y programas.*
  — *Ventajas y desventajas.*

- *Auditoría a los programas y paquetería de aplicación y explotación.*
  - *— Fabricantes, características y operabilidad del programa.*
  - *— Ambiente de aplicación y uso.*
  - *— Versión, actualización y utilidad para el usuario.*
  - *— Licencias y permisos.*
  - *— Librerías, bibliotecas y utilerías de apoyo.*
  - *— Compatibilidad, exportabilidad y escalabilidad con otros programas y paqueterías de aplicación, de desarrollo o con el sistema operativo.*
  - *— Requerimientos de capacitación y especialización.*
  - *— Paqueterías y programas desarrollados internamente.*
  - *— Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.*
  - *— Ventajas y desventajas de los programas y paqueterías de aplicación.*
- *Auditoría a la administración del software para aplicaciones.*
  - *— Paqueterías y programas integrados (Office y SmartSuite, por ejemplo).*
  - *— Programas y paqueterías para aplicaciones de escritorio (hojas de cálculo, bases de datos, procesadores de texto, agendas y presentaciones).*
  - *— Programas y paqueterías para gráficos, diseño, presentaciones, publicaciones, autoedición y multimedia.*
  - *— Programas y paqueterías de negocios y productividad.*
  - *— Programas y paqueterías para comunicación y red.*
  - *— Aplicaciones y utilerías para Internet.*
  - *— Aplicaciones para la administración de redes, cliente/servidor y sistemas mayores.*
  - *— Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.*
  - *— Otro software para aplicaciones y productividad.*
- *Auditoría a las utilerías para el funcionamiento del sistema.*
  - *— Utilerías para el archivo de información.*
  - *— Utilerías para la compresión de datos.*
  - *— Utilerías para la administración del sistema.*
  - *— Utilerías Windows para la administración del sistema Windows.*
  - *— Utilerías, librería y bibliotecas para el manejo de redes.*
  - *— Utilerías para Internet y telecomunicación.*

  Otras utilerías para el manejo del sistema.

12.4.3 Auditoría al diseño lógico del sistema

Así como es importante evaluar el funcionamiento del software del sistema computacional del área de sistemas de una empresa, también lo es auditar los aspectos lógicos que intervienen en el funcionamiento de dicho sistema, de acuerdo con las propias características de dichos sistemas computacionales y con sus peculiaridades de operación.

A continuación presentamos algunas evaluaciones de los aspectos lógicos más significativos de los sistemas, con la intención de que el auditor tenga valiosos puntos de referencia para realizar su auditoría:

- *Auditoría a los componentes lógicos del sistema operativo, de desarrollo, de comunicaciones, bases de datos y de los programas de aplicación.*
- *Características lógicas del funcionamiento del hardware, software, periféricos, instalaciones y componentes asociados al sistema.*
- *Auditoría a los procesos lógicos para la captura y procesamiento de datos y elaboración de informes.*
- *Auditoría a la arquitectura y configuración lógicas (internas y externas) del sistema, así como de sus periféricos y archivos.*
- *Auditoría al funcionamiento de las capas OSI y de los protocolos de comunicación de datos del sistema.*
- *Auditoría a los componentes lógicos del sistema para las capas y protocolos de comunicación entre datos y archivos.*
- *Auditoría a las aplicaciones lógicas para el desarrollo y la programación de nuevos sistemas.*
- *Auditoría a las aplicaciones lógicas para los métodos de accesos, consulta y operación del sistema.*
- *Auditoría a la administración y control de los niveles lógicos de acceso a los administradores, operadores y usuarios del sistema, así como su uso y explotación.*
- *Auditoría a los métodos y sistemas lógicos para la seguridad y protección de lenguajes, programas, paqueterías, utilerías y demás software institucional.*
- *Auditoría a las aplicaciones de los esquemas de seguridad lógica para protección de accesos, privilegios y manejo de las bases de datos y respaldos de información.*

12.4.4 Auditoría al diseño físico del sistema

Así como es importante evaluar el funcionamiento del software del sistema computacional del área de sistemas de una empresa, también lo es auditar los aspectos físicos relacionados con dicho sistema, con lo cual se complementará la evaluación del funcionamiento de ese sistema. La auditoría de estos componentes internos y externos se debe hacer conforme a las características del sistema computacional y a sus peculiaridades de operación. A continuación presentamos algunas evaluaciones de los aspectos físicos más significativos de los sistemas:

- *Auditoría a la arquitectura interna y configuración física del sistema computacional, así como de sus equipos periféricos, componentes e instalaciones.*
- *Auditoría a la arquitectura externa del área de sistemas y a la configuración física del sistema computacional, mobiliario, equipos e instalaciones.*
- *Auditoría a los componentes físicos del sistema, así como a sus periféricos y equipos complementarios que permiten su funcionamiento adecuado.*
- *Auditoría al diseño físico de los circuitos, compuertas y cableado interno y externo del sistema computacional.*
- *Auditoría a las instalaciones eléctricas, de comunicación de datos y de comunicación telefónica del sistema computacional.*
- *Auditoría a la administración y control de los métodos de acceso, seguridad y protección física del área de sistemas, así como de la seguridad de los administradores, operadores y usuarios del sistema, de la información y del propio sistema computacional.*
- *Auditoría a la distribución física del mobiliario, equipo y sistemas.*
- *Auditoría a los periféricos más comunes del sistema:*
  - *Teclado y ratón (mouse) del sistema: marca, modelo, ergonomía, utilidad, durabilidad y características.*
  - *Monitores: marca, modelo, características, aceleradores de gráficos, tarjetas de expansión y funcionamiento.*
  - *Impresoras: marca, modelo, características, velocidad de impresión, búferes, compatibilidad, manejo de papel y tamaño/peso.*
  - *CD-ROM: velocidad de lectura/acceso, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad de sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI y software para respaldo.*
  - *CR-RW: velocidad de lectura/grabación, velocidad de lectura/acceso, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad con sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI, tecnología para grabación de copia, software para funcionamiento, compatibilidad y multimedia.*
  - *DVD: velocidad de lectura/grabación, velocidad de acceso/lectura, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad con sonido, imágenes y datos, soporte multimedia, compatibilidad DVD/CD-ROM e interfaz IDE/SCSI.*
  - *Fax-módem: velocidad de acceso (Mbps), software de soporte, compatibilidad y protocolos de comunicación.*
  - *Otros periféricos.*

12.4.5 Auditoría a la administracion y control de accesos y salidas de datos

También se debe auditar la entrada/salida de datos del sistema computacional del área de sistemas de una organización, a fin de evaluar el funcionamiento de dicho sistema. La auditoría a estos accesos de información se hace de acuerdo con las características de dichos sistemas y con sus peculiaridades de operación. A continuación presentamos algunas evaluaciones de los aspectos más significativos de la entrada/salida de datos del sistema:

- *Auditoría a los estándares para entradas y salidas de datos del sistema.*
- *Auditoría a las especificaciones, privilegios, características y formas de accesos de datos y emisión de información.*
- *Auditoría a los procedimientos administrativos y técnicos para el acceso y salida de datos.*
- *Auditoría a la administración y control de privilegios, permisos, contraseñas y niveles de accesos y salidas de información para administradores, operadores y usuarios del sistema.*
- *Auditoría a las normas, políticas y procedimientos para el acceso, procesamiento y salida de datos del sistema computacional.*
- *Auditoría a los procedimientos de acceso al procesador, terminales, sistemas operativos, programas y paqueterías para el manejo de información.*
- *Auditoría a las incidencias de fallas, al mantenimiento y actualización para la entrada, procesamiento y salida de información del sistema.*
- *Auditoría a los periféricos para el acceso y salida de información del sistema.*
- *Auditoría a la administración de la mesa de control de acceso y salida de datos del sistema.*

12.4.6 Auditoría a la administración y control del procesamiento de datos

El principal quehacer del sistema computacional del área de sistemas es evaluar el procesamiento de la información que ingresa en él; por esta razón, el auditor de sistemas debe evaluar la forma en que se realiza el procesamiento de datos en el sistema, de acuerdo con su capacidad, volumen, confiabilidad, veracidad y oportunidad en ese procesamiento, así como con todas las características específicas del sistema, de acuerdo con su procesador, sistema operativo, lenguajes, programas y paqueterías. La auditoría al procesamiento de la información se hace de acuerdo con las características del sistema computacional y con sus peculiaridades de operación. A continuación presentamos algunas evaluaciones de los aspectos más significativos de la administración y procesamiento de datos:

- *Auditoría a los estándares e instrucciones de operación y manipulación para el procesamiento de datos, de acuerdo con el propio sistema y su software.*

- *Auditoría a la estandarización del uso de sistemas operativos, lenguajes, programas y paqueterías para el procesamiento de información en el sistema.*
- *Auditoría a los procesos lógicos y físicos para el procesamiento de datos.*
- *Auditoría a los procesos en línea, en lote, multiprocesamiento y procesos compartidos por el sistema.*
- *Auditoría a la administración y control de la frecuencia, volumen, repetitividad e incidencias en los procesamientos de datos y operaciones lógico-matemáticas de las actividades que se realizan en el sistema.*
- *Auditoría a la administración centralizada y descentralizada de sistemas para el procesamiento de información.*

12.4.7 Auditoría a los controles de almacenamiento

El activo más valioso de la actividad informática es la información; por esta razón, el área de sistemas es la responsable directa del almacenamiento y protección de la información que se procesa en sus sistemas computacionales, ya sea por los usuarios o por la propia área de sistemas de la empresa; debido a lo anterior, el auditor tiene que evaluar todo lo relacionado con el almacenamiento de datos en el sistema, ya sea que éstos sean archivados en los dispositivos propios del sistema o en sus dispositivos periféricos, tomando en cuenta la capacidad y volumen de datos que aceptan éstos, la confiabilidad de su almacenamiento y la oportunidad en el acceso y recuperación de esos datos, así como la custodia y salvaguarda de dicha información.

En esta auditoría, el auditor de sistemas también debe evaluar el diseño de los archivos de las bases de datos, así como su administración y control, incluyendo los respaldos, respaldos periódicos, su custodia y recuperación, de acuerdo con las características específicas del sistema, con su procesador, sistema operativo, lenguajes, programas y paqueterías para la administración de esas bases de datos. A continuación presentamos algunas evaluaciones de los aspectos más significativos de los controles de almacenamiento:

- *Auditoría al diseño de archivos, bases de datos y medios establecidos para el almacenamiento de información de la empresa.*
- *Auditoría a la administración y control de archivos de información del área de sistemas y de la empresa.*
- *Auditoría a los planes y programas de prevención de contingencias relacionadas con el manejo de la información en el área de sistemas.*
- *Auditoría a la administración y control de respaldos de información y de datos del sistema, así como de los programas institucionales para el manejo de los archivos del centro de cómputo.*
- *Auditoría a la administración y control de la seguridad y protección de respaldos de información y de datos.*

- Auditoría a las normas, políticas y procedimientos para el almacenamiento, custodia, protección y seguridad de la información del área de sistemas y de las área de la empresa que cuenten con sistemas computacionales.

12.4.8 Auditoría a los controles de seguridad del sistema computacional

El área de sistemas es la encargada de proporcionar la seguridad y protección a todos los sistemas computacionales de la empresa; esto incluye al propio sistema computacional, a sus componentes físicos (hardware), sus sistemas operativos, lenguajes, programas, paqueterías, utilerías, librerías y demás software; además, esta área es responsable del almacenamiento, custodia y protección de la información que se procesa en los sistemas computacionales.

Atendiendo a lo anterior, el auditor de sistemas tiene que evaluar todo lo relacionado con la protección del sistema, tanto en el aspecto técnico y lógico (el software para la protección del propio sistema) como en el aspecto físico, así como la forma en que el personal del área o los usuarios manejan los sistemas de la empresa o cualquier otro aspecto relacionado con la seguridad de éstos.

En las siguientes secciones de este capítulo trataremos con mayor profundidad la seguridad de los sistemas computacionales; sin embargo, a continuación mencionaremos algunos aspectos que el auditor debe tomar en cuenta para auditar la seguridad del sistema computacional:

- *Auditoría a los métodos, sistemas, rutinas de programación, procedimientos y medidas de seguridad y protección de los sistemas operativos, lenguajes, programas, paquetes, utilerías y demás software del sistema computacional.*
- *Auditoría a los métodos, sistemas, rutinas de programación, procedimientos y medidas de seguridad y protección de los componentes físicos (internos y externos) del sistema computacional, como son los periféricos, dispositivos asociados y demás componentes físicos.*
- *Auditoría a los sistemas, rutinas de programación, procedimientos y medidas de seguridad y protección de la información que se procesa en el sistema computacional.*
- *Auditoría a los métodos, procedimientos y sistemas de administración y control para los accesos (lógicos y físicos), uso, consulta, captura de datos y modificación de información del sistema computacional del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*
- *Auditoría a los métodos, procedimientos y sistemas de administración y control para los accesos (lógicos y físicos) al procesador, terminales, programas e información del sistema computacional.*
- *Auditoría a la administración y control de los niveles de accesos, privilegios, permisos y contraseñas para los administradores, operadores, usuarios, fabricantes, proveedores y desarrolladores externos al área de sistemas.*

- *Auditoría a los métodos, procedimientos y sistemas de administración y control para los accesos remotos al sistema computacional, al procesador, a las terminales y a los programas e información del área de sistemas por medio de redes, Internet, intranet, fax-módem, redes virtuales y demás comunicación externa.*
- *Auditoría a los métodos, procedimientos y sistemas de administración y control para la protección contra virus informáticos, hackers, crackers y personas ajenas al sistema computacional de la empresa.*

12.4.9 Auditoría a los controles adicionales para la operación del sistema

En el área de sistemas existe un sinnúmero de controles para el manejo y administración de los componentes físicos (hardware), sistemas operativos, lenguajes, programas, paqueterías, utilerías, librerías y demás software de los sistemas computacionales, además de una gama inmensa de procedimientos, sistemas y controles administrativos para el manejo y procesamiento de la información. A continuación presentamos algunas evaluaciones de los aspectos más significativos de estos controles:

- *Auditoría de la existencia, difusión, acceso y uso de manuales e instructivos del usuario, de operación, técnicos, de procedimientos, de elaboración de proyectos informáticos, de programación y los demás manuales e instructivos para el manejo de los sistemas de la organización.*
- *Auditoría de la difusión y uso de metodologías y estándares para el desarrollo de nuevos sistemas en la organización.*
- *Auditoría de la existencia, difusión y uso de estándares para el uso y programación de sistemas operativos, lenguajes, programas y paqueterías de desarrollo y aplicación de la empresa.*

12.4.10 Auditoría a la administración del área de sistemas computacionales

En la sección anterior, Auditoría a la gestión informática del área de sistemas, tocamos los principales aspectos que deben ser evaluados sobre esta actividad; sin embargo, como parte de la auditoría al sistema computacional, también conviene sintetizar algunos aspectos que deben ser auditados sobre la administración de los sistemas computacionales, con el fin de verificar la administración y el control adecuados de dichos sistemas; esto incluye el manejo administrativo de los propios sistemas computacionales, sus componentes físicos (hardware), sus sistemas operativos, lenguajes, programas, paqueterías, utilerías, librerías y demás software del sistema. A continuación presentamos algunas evaluaciones a este manejo administrativo:

- *Auditoría al diseño de la estructura de organización del sistema y áreas de trabajo relacionadas con la administración del sistema computacional.*

- *Auditoría a la administración y control centralizado, descentralizado, desconcentrado e independiente de los sistemas computacionales, redes, sistemas personales, archivos y procesamiento de datos.*
- *Auditoría a la administración y control de los recursos informáticos asignados para la administración del sistema computacional, personal informático, usuarios, hardware, software, información e instalaciones.*
- *Auditoría a los estándares, políticas y procedimientos para la adquisición de hardware, software, mobiliario, equipos e instalaciones para el sistema computacional.*
- *Auditoría a la administración de estándares, procedimientos, políticas y normas para la selección, capacitación y desarrollo del personal encargado del sistema computacional.*
- *Auditoría a la a supervisión y control de funciones, tareas, operaciones y actividades del personal del área de sistemas y usuarios de los sistemas computacionales.*
- *Auditoría de la existencia, difusión y cumplimiento de los reglamentos de operación, uso y acceso al sistema computacional.*
- *Auditoría a la salvaguarda y custodia de los activos informáticos, incluyendo el resguardo de los sistemas computacionales, así como las licencias y permisos para su uso.*

12.4.11 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría de sistemas computacionales

Recomendamos al auditor que practique esta auditoría utilizar cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro, adaptándolas al aspecto técnico que se requiere en esta revisión al sistema computacional, de acuerdo con cada uno de los aspectos señalados al principio de este subcapítulo, los cuales son la base de una auditoría de sistemas computacionales. Claro está, sujetando estos puntos a su experiencia, conocimientos y habilidades, y modificándolos, adaptándolos o sustituyéndolos de acuerdo con la evaluación del sistema, con sus características, plataformas y facilidades.

Incluso sería de mucha utilidad que el responsable de la auditoría contara con la participación del personal especializado en el manejo de los sistemas computacionales auditados, siempre y cuando él mismo cuente con los conocimientos mínimos indispensables para poder determinar los aspectos del sistema que desea evaluar, e incluso para que él mismo realice las pruebas y simulaciones necesarias, pero siempre bajo un estricto enfoque de auditoría de sistemas computacionales; jamás desde el punto de vista de la actividad informática de desarrollo, programación o administración del sistema, porque perdería la objetividad de la evaluación del sistema.

Es recomendable que el auditor de sistemas computacionales utilice las siguientes herramientas para evaluar el sistema computacional, siguiendo cada uno de los puntos anotados anteriormente:

- *El diseño de* **entrevistas** (sección 9.1) **cuestionarios** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas acordes a las necesidades de su evaluación sobre el funcionamiento, uso, aprovechamiento y demás aspectos relacionados con la operación técnica de los sistemas. Con ello tendrá la oportunidad de revisar los principales aspectos relacionados con la administración, control y seguridad del propio sistema, de sus componentes físicos (hardware), sus sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software utilizado para el funcionamiento adecuado del sistema computacional del área de sistemas y de las áreas de la empresa que cuenten con estos sistemas.*
- *Las técnicas de* **observación** (sección 9.4) *para evaluar el funcionamiento normal de las operaciones y actividades de captura de datos, procesamiento y emisión de información en el sistema computacional; también puede realizar la observación oculta, participativa o los demás tipos de observación descritos en esa sección.*
- *Los* **modelos de simulación** (sección 11.3) *para hacer la simulación del procesamiento de información, para el monitoreo de actividades, accesos al sistema o cualquier otra prueba de simulación necesaria para evaluar el funcionamiento del sistema computacional, siempre y cuando esto no interfiera en la operación normal de la actividad informática de la empresa.*
- *Las técnicas de* **revisión documental** (sección 10.5) *para revisar los manuales, instructivos, resguardos de sistemas, proyectos de sistemas, bitácoras de mantenimiento y evaluación, planes, programas y presupuestos para la adquisición de sistemas y todas las demás evaluaciones que tenga que realizar a la documentación utilizada para el manejo del sistema computacional.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** (sección 10.8), *según sus preferencias y sus necesidades de revisión, para auditar las fortalezas y debilidades del sistema computacional, así como las áreas de oportunidad de servicio y las amenazas de la tecnología para el funcionamiento adecuado de dicho sistema.*

Es indispensable que el responsable de esta auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría a la gestión informática del área de sistemas:

- *La elaboración de una guía de evaluación (sección 11.1), a fin de planear específicamente cada uno de los aspectos importantes que deben ser evaluados sobre la actividad administrativa. Para ello le sugerimos que tome en cuenta cada uno de los puntos indicados en las secciones anteriores, utilizándolos tal cual y adaptándolos a sus necesidades específicas de evaluación y conforme a las características del sistema computacional.*

Algunos elementos de control que el responsable de la evaluación del sistema computacional puede tomar en cuenta son los siguientes:

- *El uso de la* **lista de chequeo** (sección 11.6)*, ya que mediante esta herramienta el auditor podrá verificar que la persona que practique la auditoría de los sistemas computacionales cubra todos los puntos descritos en su planeación de auditoría.*
- *El uso de las técnicas de* **muestreo** (sección 9.6)*, debido a que en el procesamiento de información de datos sería casi imposible, a la vez que inoperante, revisar todas las actividades que realiza el sistema computacional para evaluar sus actividades y resultados; por eso es necesario utilizar muestras representativas de su funcionamiento, de acuerdo con las necesidades y características del sistema y con la necesidad de uso de datos reales o datos falsos. Esto independientemente del método de muestreo que se utilice en esta evaluación. El muestreo se puede utilizar para evaluar tanto las actividades de los propios sistemas, como sus comunicaciones, así como muchos otros aspectos.*

Para evaluar el hardware y software de los sistemas computacionales, el uso de sus componentes asociados, así como el comportamiento de los sistemas adquiridos o desarrollados en el área de sistemas, el responsable de la auditoría puede utilizar las siguientes herramientas:

- *La* ***experimentación*** (sección 9.7) *con cada uno de los sistemas computacionales, a fin de evaluar su funcionamiento adecuado; la experimentación se puede realizar con todo el sistema o con cada uno de sus componentes por separado; con ello el auditor estará en condiciones de opinar sobre el uso del hardware, software e información que se maneja en dicho sistema. Asimismo, la experimentación debe estar bien fundamentada y soportada sobre pruebas reales o simuladas y perfectamente controladas para que no repercuta en el comportamiento normal del sistema en evaluación.*
- *La* **ponderación** (sección 11.2), *que es una herramienta muy útil que le permite al auditor evaluar el funcionamiento adecuado de cada uno de los componentes de los sistemas, así como darle a cada parte el peso que le corresponde según su participación en el sistema computacional auditado. Recordemos que con esta técnica se busca darle un peso específico a cada una de las partes del sistema, de acuerdo con un criterio de evaluación para hacer más equitativa dicha evaluación. La ponderación se puede adoptar de cada una de las subsecciones que conforman este subcapítulo; la responsabilidad del auditor será darle el peso a cada una de las subsecciones en que se dividió esta parte de la auditoría y aplicar cualquiera de los otros métodos de evaluación sugeridos para cada parte ponderada, según las características del sistema.*
- *También puede y debe aplicar la técnica de* **inventarios** (sección 9.5) *para evaluar el hardware, procesadores, periféricos, dispositivos asociados y resguardos,*

así como los sistemas operativos, lenguajes, programas, paquetes, licencias y demás software y activos informáticos de cada uno de los sistemas asignados al área de sistemas y de los sistemas de las demás áreas de la empresa.

En todas las sugerencias anteriores se debe tomar en cuenta que son eso, sugerencias, y que es potestad absoluta del auditor responsable de la auditoría utilizar las técnicas, métodos y procedimientos de auditoría que más le agraden, e incluso utilizar o adaptar los puntos indicados en las secciones para realizar esta auditoría conforme a sus necesidades concretas de evaluación.

12.5 Auditoría alrededor de la computadora

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión específica que se realiza a todo lo que está alrededor de un equipo de cómputo, como son sus sistemas, actividades y funcionamiento, evalúa los métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del centro de cómputo, los aspectos operacionales y financieros, la gestión administrativa de accesos al sistema, la atención a usuarios y al desarrollo de nuevos sistemas, las comunicaciones internas y externas, y en si todos aquellos aspectos que contribuyen al buen funcionamiento de una área de sistematización.

Con este tipo de auditoría es posible evaluar todos los aspectos involucrados en el funcionamiento de los sistemas computacionales de la empresa. Por esta razón, al realizar esta auditoría no es necesario estar en contacto directo con el sistema computacional, pero sí con todo lo que implica el cumplimiento de las acciones relacionadas con el trabajo cotidiano de la función informática de las áreas de sistemas, las cuales sí repercuten de alguna manera en el desempeño de las actividades, operaciones y funciones del centro de cómputo de la empresa o de aquellas áreas que también cuentan con sistemas computacionales.

Para realizar esta auditoría es necesario considerar todas las situaciones que repercuten de alguna manera en el funcionamiento del área de sistemas, a fin de lograr que realice su función informática de manera eficiente y funcional. A continuación presentamos algunos aspectos del entorno de la computadora que deben ser evaluados:

- *El diseño físico del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales.*
- *El análisis y aprobación de las propuestas para la adquisición del software, hardware, periféricos, equipos adicionales, bienes muebles, consumibles y materiales diversos que permiten el funcionamiento del sistema.*

- *El medio ambiente de trabajo en el que se realiza la función informática de la empresa.*
- *La gestión administrativa de la función informática de la empresa.*
- *El diseño de proyectos de nuevos sistemas computacionales en el área de sistemas.*
- *El diseño de formatos, formas y métodos para la recopilación de información que será procesada en el sistema.*
- *La administración y control de los sistemas de seguridad y salvaguarda de los activos informáticos, la información, el personal y los usuarios del sistema.*
- *La administración y control de accesos a las instalaciones del área de cómputo, a los sistemas, a la información y los bienes informáticos del área.*
- *Todos aquellos aspectos especiales que intervienen de alguna manera en el aprovechamiento y explotación del sistema computacional y en la gestión administrativa del centro de cómputo. Con la condición indiscutible de no interferir directamente en el uso del equipo de cómputo.*

Estos aspectos que para el lector pueden parecer casi iguales a los indicados en la auditoría sin la computadora o en la auditoría a la gestión informática, en realidad son complementarios entre sí, ya que no existe una frontera real entre esos modelos de auditorías y la auditoría en el entorno de la computadora; incluso podrían conjuntarse los tres tipos de auditoría en una misma.

La deferencia real para clasificarla como auditoría en el entorno de la computadora es que en esta evaluación el auditor **sí debe** tomar en cuenta los sistemas computacionales para realizar su auditoría, pero sin auditarlos directamente; **en las otras no**; en estos casos, se revisa concretamente todo lo que rodea a la función informática de la empresa. Además, el auditor de sistemas puede practicar este tipo de evaluaciones, ya que posee un profundo conocimiento del ambiente de sistemas; sin embargo, también la podría realizar algún otro auditor, de preferencia un especialista en el ámbito administrativo, operativo o contable, debido a que la práctica de este tipo de auditoría exige conocimientos mínimos sobre el ámbito en donde están los sistemas.

Cabe señalar que existe un sinnúmero de criterios para la aplicación de una *auditoría alrededor de la computadora*; por ejemplo, los que únicamente consideran la evaluación de los puntos que influyen directamente en la administración del área de sistemas, como la capacitación de personal y usuarios, elaboración de los manuales e instructivos de operación, la seguridad de los bienes informáticos e instalaciones del centro de informática, las actividades de organización y métodos, la aplicación y seguimiento de presupuestos, planes y programas del centro de informática de la empresa, hasta el criterio de los que evalúan todo lo relacionan con los sistemas, incluso sus actividades y funciones.

A continuación presentamos los aspectos generales que intervienen en una auditoría alrededor de la computadora, ya que esta auditoría se debe realizar de acuerdo con las características, necesidades y repercusiones de la administración del área de sistemas de cada empresa o del propio equipo procesador:

- *Auditoría a la administración del software de la empresa.*
  - *Lenguajes y programas de desarrollo, aplicaciones y explotación del software institucional del área de sistemas y del software de las demás áreas de la empresa que cuenten con sistemas.*
  - *Especificaciones de acceso y uso de los datos e información del sistema, así como de los procesos y operación del propio sistema.*
  - *Estándares y métodos de entradas de datos y salidas de Información.*
  - *Estándares para la operación y manipulación de datos del sistema.*
  - *Formas de procesamiento de información y procesos de datos en línea o lote.*
  - *Administración de archivos, programas e información institucional*
  - *Medidas para evitar la piratería de software, así como la instalación de programas ilegales en el área de sistemas y en las demás áreas de la empresa que cuentan con sistemas.*
  - *Administración y control de las licencias, resguardos y custodia del software institucional.*
  - *Manuales e instructivos de operación, técnicos, de procedimientos, así como de las instalaciones y demás documentación relacionada con el funcionamiento del sistema.*
  - *Metodologías y estándares para el desarrollo de nuevos sistema.*
  - *Estándares de programación y documentación de sistemas.*
  - *Adquisición, desarrollo e instalación de nuevos sistemas computacionales.*
  - *Mantenimiento preventivo y correctivo del sistema computacional, del hardware, software, de la información y demás componentes de los sistemas de la empresa.*
- *Auditoría a la configuración física del área de sistemas de la empresa.*
  - *Configuración, ubicación y adecuación de las áreas físicas del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas, en relación con el aire acondicionado, pisos falsos, iluminación, instalaciones y demás componentes físicos para el bienestar y comodidad de los usuarios de sistemas.*
  - *Configuración del sistema computacional, redes, procesadores, periféricos, componentes e instalaciones físicas internas y externas del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas computacionales.*
  - *Configuración y características físicas de locales, instalaciones, mobiliario y equipos.*
  - *Distribución de los equipos, componentes y configuración física del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas.*

— *Instalaciones eléctricas (tipos de cableados y conexiones, tierra física, no-breaks, reguladores de corriente, etc.), de comunicación y de datos del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*

— *Medio ambiente físico del área de sistemas (sistemas de calefacción, polvo, ruido, estática, aire acondicionado, etc.) y los demás elementos ambientales que pueden influir en el desarrollo adecuado de la función informática en la empresa.*

— *Sistemas de acceso, seguridad y protección físicos del área de sistemas, así como la seguridad de sus activos informáticos, personal y usuarios.*

— *Distribución del mobiliario, equipo y sistemas.*

— *Usuarios de los sistemas de red, PCs individuales, de correo electrónico, grupales y usuarios de cualquier otro sistema.*

— *Componentes externos del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*

- *Auditoría a los métodos de acceso, seguridad y salvaguarda de los activos informáticos del área de sistemas.*

  — *Planes y programas de prevención contra contingencias en el funcionamiento del sistemas, en la información y datos de la empresa y en los demás bienes informáticos del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas.*

  — *Identificación de accesos, almacenamiento y custodia de la información, sistemas operativos, lenguajes, archivos y programas institucionales.*

  — *Evaluación de controles y sistemas de seguridad, protección y salvaguarda de los activos, del personal, instalaciones, información, mobiliario y equipo del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*

  — *Planes contra contingencia para seguridad y protección de los programas, información, instalaciones, empleados y usuarios del sistema computacional.*

  — *Sistemas de control de accesos lógicos al sistema y a las bases de datos.*

  — *Sistemas de control de accesos físicos al centro de cómputo.*

  — *Prevención y erradicación de virus informáticos.*

  — *Sistemas de protección y supresión de sistemas piratas y juegos en los sistemas computacionales de la empresa.*

- *Auditoría a la administración del área de sistemas.*

  — *Diseño de la estructura de organización del sistema, de las áreas de trabajo y de las funciones y líneas de autoridad y responsabilidad de funcionarios, empleados y usuarios del área de sistemas.*

— *Administración centralizada de sistemas, archivos y procesamiento de información.*

— *Administración desconcentrada de sistemas, archivos y procesamiento de información.*

— *Administración y control de los recursos informáticos, personal, instalaciones, mobiliario y equipo del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*

— *Estándares, normas y políticas para la evaluación y adquisición del hardware, software, periféricos, mobiliarios, equipos, instalaciones y artículos de consumo para el área de sistemas.*

— *Estándares para la selección, capacitación y desarrollo del personal y usuarios del centro de cómputo.*

— *Supervisión, coordinación y control de funciones y actividades de funcionarios, personal y usuarios del área de sistemas computacionales.*

— *Supervisión, coordinación y control de la operación de los sistemas, equipos, periféricos e información del área de sistemas.*

— *Evaluación de los aspectos técnicos del sistema, en cuanto a características, configuración, procesamiento de información, componentes y demás peculiaridades de la función informática en la empresa.*

— *Administración y control del sistema operativo, de los lenguajes, programas y paqueterías institucionales utilizados en el procesador del sistema computacional.*

— *Administración y control de los sistemas de red, cliente/servidor, multiusuarios y microcómputo de la empresa.*

— *Administración y control de sistemas de telecomunicación de datos y teleprocesamiento de información.*

— *Prevención y control de la contaminación informática.*

— *Actualización permanente de acuerdo con los cambios computacionales y tecnologías informáticas de vanguardia.*

— *Diseño e implementación de estándares de operación, adquisición, capacitación, desarrollo de sistemas, accesos al sistema, procesamiento de datos y demás estándares relacionados con la administración y control del centro de cómputo.*

- *Auditoría a los aspectos técnicos del sistema.*

  — *Administración y control de la configuración de servidores, terminales y PCs de la empresa, en cuanto a procesadores, tarjetas madre, cableado interno y externo, componentes del sistema computacional y demás peculiaridades de los sistemas de la empresa.*

— *Administración y control de los sistemas operativos, lenguajes de operación, desarrollo y aplicación para la programación y explotación del sistema.*

— *Administración y control de los sistemas de red (LAN, MAN o WAN), sistemas mayores, cliente/servidor, multiusuarios y de PC personal.*

— *Determinación y aplicación de normas y estándares para la instalación de sistemas computacionales en la empresa, relacionados con los procesadores, tarjetas madre, velocidades de procesos, memorias, medios de almacenamiento secundario y demás componentes de los sistemas de la empresa.*

— *Administración y control de las bibliotecas del sistema, sean maestras, fuente, de parámetros, de procedimientos, de carga, de objetivos y demás bibliotecas según los sistemas operativos, lenguajes y programas de dicho sistema.*

— *Administración y control de los archivos del sistema, de los archivos de los usuarios y de los específicos de producción, pruebas de sistemas, operación de pruebas, nuevos proyectos y resguardos de la información institucional.*

— *Administración y control de las bases de datos del sistema y de los usuarios, en relación con su estructura, configuración, características, lenguajes y programas, resguardos, custodia interna y externa y demás formas de administración de las bases de datos.*

— *Administración y control de la arquitectura de comunicación, de los sistemas de telecomunicación, teleprocesamiento, transmisión, retransmisión, interconexión y de los sistemas utilizados para la transmisión vía módem, cableado o satelital.*

— *Prevención, control y erradicación de la contaminación informática, piratería y virus informáticos.*

— *Actualización permanente de acuerdo con los cambios computacionales y tecnológicos que impactan la función informática en la empresa.*

— *Administración y control de los estándares, velocidades, procesadores, memorias y demás características de los sistemas computacionales de la empresa.*

- *Auditoría a la administración del sistema.*

  — *Administración estratégica de la función informática, visión, misión y objetivos del área de sistemas, así como de las estrategias, los planes y programas, normas, políticas, lineamientos y procedimientos para regular la actividad de sistemas en la empresa.*

  — *Los planes, programas y presupuestos financieros que afectan la administración del centro de cómputo.*

  — *La estructura de organización, puestos, funciones, niveles de autoridad y canales de comunicación del centro de cómputo, según su tamaño, características y sistemas de procesamiento.*

- *La selección, capacitación, formación, adiestramiento y contratación de funcionarios, personal y usuarios del área de sistemas.*
- *El establecimiento y uso de los sistemas y métodos de control para el acceso a los sistemas e información institucionales.*
- *La aplicación de las técnicas y métodos de dirección, supervisión, toma de decisiones, coordinación y de motivación del personal y usuarios del centro de cómputo.*
- *Administración de proyectos de sistemas informáticos en la empresa, así como de la adquisición, adecuación o desarrollo interno de sistemas.*
- *Existencia, difusión, actualización y uso de la documentación técnica y administrativa del área de sistemas, manuales de usuarios, de operación del sistema, manuales de organización, de procedimientos y de operación administrativa del área de sistemas.*
- *Existencia, difusión, y actualización de resguardos de sistemas computacionales, licencias de lenguajes, programas y paquetes del sistema.*
- *Administración y control de los materiales y consumibles del área de sistemas.*
- *Evaluación de los perfiles de puestos del área de sistemas y cumplimiento de los requisitos del puesto.*
- *Análisis del entorno de los sistemas, en relación con la comunicación de las áreas de la empresa y la atención a usuarios.*
- *Cumplimiento de las funciones administrativas de los funcionarios del área de sistemas, en lo referente a la planeación, organización, dirección y control de las funciones informáticas de la empresa.*

12.5.1 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría alrededor de la computadora

Como pudimos observar en lo expuesto anteriormente, esta auditoría se realiza a todo lo que está en torno al sistema computacional, pero no a éste; no sólo se evalúa lo puramente administrativo, sino también todos los demás aspectos relacionados con la administración y control de las actividades y operaciones que contribuyen al desempeño de la función informática en la empresa. Por esta razón recomendamos al auditor que practique esta auditoría en el entorno de la computadora que utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro, adaptándolas a los aspectos de carácter administrativo y técnico requeridos para evaluar las acciones encaminadas a favorecer la actividad eficiente de la función informática en la empresa. Pero jamás debe realizar esta auditoría al sistema computacional.

Tomando como base lo indicado en cada uno de los aspectos señalados al principio de este subcapítulo, los cuales son la base de una auditoría alrededor de la computadora, es recomendable utilizar algunas de las técnicas señaladas en los capítulos 9, 10 y 11

de este libro. Claro está, el responsable de esta auditoría debe utilizar estos puntos de acuerdo con su experiencia, conocimientos y habilidades, a fin de que esos puntos sean utilizados tal y como ahí se describen, e incluso adaptándolos o sustituyéndolos por aquellos requerimientos específicos que sean necesarios, de acuerdo con las características, plataformas, facilidades y demás distintivos propios de esta auditoría.

En esta parte sería de mucha utilidad que el responsable de la auditoría contara con la participación de auditores especializados en la auditoría administrativa u operacional; siempre y cuando estos especialistas cuenten con los suficientes conocimientos de sistemas computacionales para poder determinar cuáles aspectos del entorno del sistema deben ser evaluados, e incluso para que ellos mismos realicen las pruebas y simulaciones necesarias, pero bajo un estricto enfoque de auditoría de sistemas computacionales; jamás desde la óptica de la auditoría administrativa o contable, porque se perdería la objetividad de la evaluación del sistema.

Sugerimos al auditor de sistemas computacionales que, siguiendo cada uno de los puntos anotados anteriormente para la evaluación a todo lo que rodea al sistema computacional, utilice las siguientes herramientas:

- *El diseño de* **entrevistas** (sección 9.1) **cuestionarios** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas acordes con las necesidades de su evaluación sobre el funcionamiento, uso, aprovechamiento y otros aspectos de la actividad informática del área de sistemas y de las demás áreas de la empresa que cuenten con esos sistemas. Con ello tendrá la oportunidad de revisar los principales aspectos relacionados con la administración y control de las funciones, actividades, acciones y tareas encaminadas al funcionamiento adecuado del sistema computacional.*

Además, quizá como una de las primeras acciones de evaluación, el auditor también puede utilizar las siguientes herramientas:

- *El levantamiento de* ***inventarios*** (sección 9.5)*, a fin de hacer un recuento de los bienes informáticos del área de sistemas; para llevar a cabo esto, es recomendable realizar los siguientes inventarios:*
  - *— Inventarios de los equipos de cómputo, contemplando las marcas, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con estos equipos.*
  - *— Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas.*
  - *— Inventario del personal informático y usuarios del sistema, a fin de evaluar sus perfiles de puestos, conocimientos, características y preparación para el uso de los sistemas computacionales de la empresa.*

— *Inventario de bienes muebles, inmuebles, materiales y consumibles del área de sistemas.*

— *Inventario de los sistemas de redes, cuando el sistema esté diseñado de esta manera.*

— *Inventario de instalaciones físicas, protecciones, características y funcionalidad de las áreas de sistemas, contemplando su medio ambiente de trabajo, iluminación, aire acondicionado, ruidos, temperatura, estática y demás peculiaridades de su funcionamiento.*

— *Otros inventarios acordes con las necesidades de la auditoría.*

Algunas de las herramientas que serán más utilizadas en estas auditorías son las siguientes:

- *Las técnicas de* **observación** (sección 9.4) *para evaluar el funcionamiento normal de las operaciones y actividades de las áreas de sistemas, sus funciones, actividades y acciones de apoyo para la captura de datos, procesamiento y emisión de información en el sistema computacional, así como la observación oculta, participativa y demás tipos de observación descritos en esa sección, cuando el caso lo requiera.*
- *Las técnicas de* **revisión documental** (sección 10.5) *para revisar los manuales, instructivos, resguardos y proyectos de sistemas, bitácoras de mantenimiento y evaluación, los planes, programas y presupuestos para la adquisición de sistemas y todas las demás evaluaciones que se tengan que realizar a la documentación utilizada para el manejo del sistema computacional. Siempre y cuando esta revisión sea para evaluar lo que está alrededor del sistema, mas no el sistema.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** (sección 10.8) *según sus preferencias y necesidades de revisión; el auditor puede auditar con estas herramientas las fortalezas y debilidades del área de sistemas y las de las demás áreas de la empresa que los tengan, así como las áreas de oportunidad de servicio y las amenazas de la tecnología para el funcionamiento adecuado de estos sistemas.*

Es indispensable que el responsable de esta auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría a la gestión informática del área de sistemas:

- *La elaboración de una* **guía de evaluación** (sección 11.1), *a fin de planear específicamente cada uno los aspectos sustantivos que tenga que evaluar sobre la actividad administrativa. Para ello es recomendable que tome en cuenta cada uno de los aspectos señalados en esta sección, así como lo señalado en las secciones de la gestión informática, adaptándolos o modificándolos para configurarlos conforme a sus propias necesidades de evaluación, y conforme a las características propias del sistema computacional que será auditado.*

Un buen elemento de control para el responsable de esta evaluación es el siguiente:

- *El uso de la* **lista de chequeo** (sección 11.6), *ya que con esta herramienta puede verificar que quien realice la auditoría cubra todos los puntos descritos en su planeación de auditoría. Inclusive, de acuerdo con el diseño de esta lista de chequeo, también puede auditar todos los aspectos que están alrededor del sistema computacional, considerando el cumplimiento de cada uno de los puntos contemplados en dicha herramienta.*
- *El uso de las* **técnicas de muestreo** (sección 9.6), *debido a que al evaluar el cumplimiento de las funciones, tareas y operaciones del área de sistemas, sería casi imposible, a la vez que inoperante, revisar todas las actividades que realiza el sistema en la actividad administrativa de este centro, por eso tiene que utilizar muestras representativas de su cumplimiento, de acuerdo con las necesidades y características de la auditoría. Esto independientemente del método de muestreo que utilice en esta evaluación. Puede hacer lo mismo con las actividades de los propios sistemas, con sus comunicaciones y con todos los aspectos que puedan ser evaluados mediante el muestreo.*

El responsable de la auditoría puede utilizar las siguientes herramientas para evaluar las funciones de los funcionarios, empleados y usuarios de sistemas, así como el desempeño de todo lo que está alrededor de los sistemas del área de sistemas:

- *La* **ponderación** (sección 11.2)*, la cual le permite evaluar el funcionamiento adecuado de cada una de las partes que rodean a la computadora, dándole a cada parte el peso que le corresponde según el apoyo que brinda al sistema computacional para que cumpla con la función informática en la empresa. Recordemos que con esta técnica es posible darle un peso específico a cada una de esas partes, de acuerdo con un criterio para hacer más equitativa la evaluación. Aquí se puede adoptar la ponderación de cada una de las subsecciones que conforman este subcapítulo; la responsabilidad del auditor será darle el peso a cada una de estas subsecciones en que se dividió esta parte de la auditoría y aplicar a cada parte ponderada cualquiera de los otros métodos de evaluación sugeridos, según las características del sistema.*

Otra herramienta que puede utilizar el responsable de la auditoría, en caso de ser necesario, es la siguiente:

- *El* **acta testimonial** (sección 10.6), *debido a que es una herramienta muy útil para confirmar, confrontar y asentar por escrito las anomalías, deficiencias e incidencias que requieren de un sustento documental para fundamentar la opinión que emite. En la auditoría alrededor de la computadora se pueden encontrar muchas incidencias que deben ser documentadas, como la falta de algún bien informático; en este caso, el auditor deberá levantar esta acta; también*

podría encontrar software no institucional y una serie de circunstancias que, en ese momento, harán necesario el uso de esta acta documental. Recordemos que en algún caso extremo, este documento se puede utilizar como prueba testimonial de alguna incidencia especial.

La práctica de esta auditoría tiene mucho de las evaluaciones tradicionales, por lo que se pueden utilizar otras herramientas de la auditoría tradicional, como las que mencionamos a continuación:

- *El examen (sección 10.1), la inspección (sección 10.2), la confirmación (sección 10.3) y la comparación (sección 10.4).*

El responsable de la auditoría debe tomar las sugerencias anteriores sobre los aspectos que pueden ser evaluados mediante la auditoría alrededor de la computadora de acuerdo con sus necesidades específicas de evaluación, debido a que es su potestad absoluta utilizar esas sugerencias, modificarlas, adaptarlas o sustituirlas por aquellos puntos concretos que ayuden a su auditoría. Asimismo, tiene la facultad de utilizar las técnicas, métodos y procedimientos de auditoría que más le agraden, que más conozca o las que pueda utilizar o adaptar a sus necesidades concretas de evaluación.

12.6 Auditoría de la seguridad de los sistemas computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema computacional, de sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, de las bases de datos, redes, sistemas, instalaciones y usuarios del mismo. Es también la revisión de los planes contra contingencias y mediadas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí es la evaluación de todos aquellos aspectos que contribuyen a la protección y salvaguarda del buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos.

El crecimiento de la tecnología informática ha sido tan desmesurado que hoy en día no existe una empresa que no cuente con sistemas computacionales para desarrollar sus actividades; sin embargo, a la par de ese avance tecnológico, también han crecido los problemas relacionados con la administración de la seguridad de los sistemas computacionales y han surgido múltiples problemáticas que repercuten en el trabajo adecuado de dichos sistemas. Y no únicamente en las empresas, sino en las casas, las escuelas y en muchos lugares donde la informática está presente.

Precisamente, con la auditoría de sistemas computacionales se puede evaluar la repercusión de la seguridad, protección y salvaguarda de los sistemas de la empresa, analizando sus impactos en los siguientes aspectos:

- *En los sistemas computacionales y dispositivos periféricos.*
- *En la información institucional y bases de datos.*
- *En los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional.*
- *En los activos informáticos del área de sistemas.*
- *En el personal informático y los usuarios del sistema.*
- *En la protección y conservación de locales, instalaciones, mobiliario y equipos.*
- *En los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software.*
- *En la arquitectura de las telecomunicaciones.*
- *En los sistemas de redes, sistemas mayores y PCs.*
- *En la piratería informática.*
- *En los virus informáticos.*

Éstos son algunos de los muchos aspectos de la seguridad de los sistemas computacionales de las empresas que se deben evaluar, aunque esto se puede aplicar también para las populares computadoras de las casas, escuelas y pequeñas empresas.

A continuación analizaremos los principales aspectos que se deben contemplar en la auditoría de la seguridad de los sistemas computacionales, mismos que presentaremos de manera general, ya que su real aplicación se debe hacer de acuerdo con las características y necesidades de la administración de la seguridad, protección y salvaguarda de los bienes informáticos o del sistema computacional del área de cómputo de cada empresa:

- *Auditoría de la seguridad en las condiciones e instalaciones físicas del área de sistemas.*
- *Protección contra los riesgos y contingencias de origen natural relacionadas con el medio ambiente de trabajo.*
  - *Las condiciones generales de trabajo de los sistemas computacionales, para el bienestar y comodidad de los empleados y usuarios del sistema.*
  - *Protección contra la humedad del medio ambiente.*
  - *Medidas para prevenir que los sistemas computacionales, las instalaciones eléctricas, telefónicas y de datos tengan contacto con el agua.*
  - *Protección contra las partículas de polvo y desechos volátiles de cualquier tipo en el medio ambiente, a fin de evitar desperfectos en los sistemas computacionales, medios de almacenamiento y el deterioro de los activos informáticos del área de sistemas.*

— *Protección contra la estática e imantación producidas por fibras sintéticas, metales, por algunos plásticos y por el cabello humano y animal que pueden repercutir en el funcionamiento de los sistemas computacionales de la empresa.*

— *Análisis de los sistemas de acondicionamiento y pisos falsos.*

— *Análisis de la regulación de temperatura y aire acondicionado.*

— *Análisis de los suministros de energía, comunicaciones y procesamiento de datos.*

— *Análisis de la limpieza del área de sistemas.*

- *Protección contra riesgos y contingencias relacionados con el medio ambiente de trabajo en las áreas de sistemas de la empresa.*
  - — *La iluminación artificial del área de sistemas y la iluminación por medio de luz solar.*
  - — *Las instalaciones eléctricas, de datos y de comunicación.*
  - — *Los accesos y salidas en las áreas de sistemas.*
  - — *La repercusión de los aspectos de carácter ergonómico.*
  - — *Las adaptaciones de los equipos de cómputo.*
  - — *Las condiciones de trabajo con computadora.*
  - — *Protección contra contingencias causadas por la temperatura del sistema de aire acondicionado.*
  - — *La ventilación natural de las áreas y espacios.*
- *Protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables.*
  - — *Por precipitación pluvial, de nieve, de granizo y otras precipitaciones.*
  - — *Por vientos, huracanes, ciclones y fenómenos atmosféricos.*
  - — *Por terremotos y temblores.*
  - — *Por inundaciones, marejadas, maremotos y fenómenos marítimos.*
  - — *Por tormentas eléctricas.*
  - — *Por incendios accidentales.*
  - — *Otros fenómenos de origen natural que afectan a las áreas de sistemas y a los propias sistemas computacionales.*
- *Protección contra riesgos y contingencias derivados del suministro de la energía eléctrica.*
  - — *Prevención de interrupciones del suministro de energía eléctrica para el funcionamiento de los sistemas computacionales.*
  - — *Continuidad del suministro de la energía eléctrica, por medio de la red pública o plantas de emergencia, fuentes ininterrumpidas de poder y no-breaks.*

- *— Previsión en la funcionalidad, distribución adecuada y seguridad de las instalaciones eléctricas del área de sistemas.*
- *— Prevención de fallas y deficiencias de la red pública de suministro de electricidad.*
- *— Protección contra las variaciones de voltaje, así como el uso de reguladores de corriente, contactos supresores de picos y sistemas de no-breaks.*
- *— El análisis del cableado público de las instalaciones eléctricas que están fuera de la empresa.*
- *— El análisis del cableado, construcciones y adaptaciones eléctricas, contactos, tierra física y demás instalaciones eléctricas internas del área de sistemas.*

- *Protección y seguridad de los espacios físicos de las instalaciones de cómputo.*
  - *— En los sistemas de vigilancia de las áreas de sistemas.*
  - *— En los accesos a las instalaciones de las áreas de cómputo.*
  - *— En las áreas restringidas y de accesos exclusivos.*
  - *— En las áreas de trabajo de sistemas, almacenamiento, cintotecas (bóvedas) y otros espacios de sistemas.*
  - *— En la administración y control de los medios de seguridad, observación y vigilancia de los sistemas computacionales.*
  - *— En la vigilancia del mobiliario, equipo y activos informáticos de las áreas de sistemas.*
  - *— En la vigilancia del almacenamiento de información, datos y software institucional en las áreas de cómputo.*
  - *— En la vigilancia de accesos a los sistemas computacionales en las áreas ajenas al centro de cómputo.*
  - *— En la seguridad, salvaguarda y protección de las cintas, disquetes y otros medios magnéticos utilizados en el área de sistemas.*
  - *— En la seguridad y protección de manuales, instructivos, datos, información y reportes del área de sistemas.*
  - *— La totalidad, veracidad y confiabilidad de la captura de información.*
- *El análisis a los planes de contingencias informáticas.*
  - *— Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias de sistemas.*
  - *— Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.*
  - *— Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.*

- *Auditoría de la seguridad y protección en el diseño de las instalaciones del área de sistemas de la empresa o empresas de cómputo.*
  - *En el análisis de los estudios de localización de planta para instalar el área de sistemas.*
  - *En el análisis para la localización de instalaciones físicas del área de sistemas.*
  - *En el análisis de los estudios de la densidad de población.*
  - *En el análisis de la infraestructura pública de servicios.*
  - *En el análisis de los medios de comunicación pública, y de los medios de transporte de pasajeros.*
  - *En el análisis de los estudios de composición del suelo para prevenir desastres naturales.*
  - *En el análisis del cableado telefónico interno para el funcionamiento del área de sistemas.*
  - *En el análisis del cableado externo y redes públicas del servicio telefónico, así como de telecomunicación para el funcionamiento del área de sistemas.*
- *Auditoría de la seguridad en los sistemas computacionales.*
  - *Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.*
  - *Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización.*
  - *Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del área de sistemas.*
  - *Evaluar el rendimiento, aplicación y utilidad del equipo de cómputo, mobiliario y demás equipos.*
  - *Evaluar la seguridad en el procesamiento de información.*
  - *Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.*
- *Auditoría de la seguridad del hardware.*
  - *Realizar inventarios de hardware, equipos y periféricos asociados.*
  - *Evaluar la configuración del equipo de cómputo (hardware).*
  - *Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.*
  - *Evaluar el estado físico del hardware, periféricos y equipos asociados.*
- *Auditoría de la seguridad del software.*
  - *Realizar inventarios de software, paqueterías y desarrollos empresariales.*
  - *Evaluar las licencias, permisos y usos de los sistemas computacionales.*

— *Evaluar el rendimiento y uso del software de los sistemas computacionales.*

— *Verificar que la instalación del software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta última.*

- *Auditoría de la seguridad en los sistemas computacionales.*
  - — *Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.*
  - — *Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización.*
  - — *Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del centro de cómputo.*
  - — *Evaluar el rendimiento, aplicación y utilidad del equipo de cómputo, mobiliario y demás equipos.*
  - — *Evaluar la seguridad en el procesamiento de la información.*
  - — *Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.*
- *Auditoría para verificar la captura, procesamiento de datos y emisión de resultados.*
  - — *Evaluar la totalidad, veracidad y confiabilidad de la captura de información.*
  - — *Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias en los sistemas.*
  - — *Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.*
  - — *Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.*
- *Auditoría de la prevención de actos premeditados que afecten el funcionamiento de los sistemas computacionales.*
- *Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.*
  - — *Contra sabotajes.*
  - — *Por extorsión.*
  - — *Por alteración o destrucción de datos.*
  - — *Por fraudes.*
- *Protección contra el mal uso de la información.*
  - — *Por invasión de privacidad.*
  - — *Para mal uso de la confiabilidad.*
  - — *Por uso inadecuado de los datos.*

- *Protección contra la piratería y robo de información.*
  - *— Con medidas preventivas.*
  - *— Con la protección de archivos.*
  - *— Con limitación de accesos.*
  - *— Con protección contra robos.*
  - *— Con protección ante copias ilegales.*
- *Protección para el almacenamiento de la información.*
  - *— Respaldos de programas e información.*
  - *— Almacenamiento y custodia de cintas, disquetes, etcétera.*
  - *— Lugares adecuados, como cintotecas (bóvedas), discotecas, etcétera.*
  - *— El control y uso de información, programas y paquetes.*
- *Protección contra actos no intencionales.*
  - *— Por negligencia y descuido.*
  - *— Por fallas del equipo y del sistema.*
  - *— Por fallas de carácter externo.*
- *Protección contra virus informático.*
  - *— Medidas preventivas y correctivas.*
  - *— Uso de vacunas y buscadores de virus.*
  - *— Protección de archivos, programas e información.*
- *Protección y seguridad para el desarrollo de programas y proyectos de sistemas.*
  - *— Desarrollo de programas y nuevos proyectos de sistemas.*
  - *— Protección contra deficiencias de programas y lenguajes.*
  - *— Prevención de fallas del sistema operativo.*
  - *— Protección en el establecimiento de estándares de proyectos.*
- *Protección y seguridad para los accesos al sistema computacional y a la información.*
  - *— En el uso de contraseñas.*
  - *— Establecimiento de niveles de acceso y uso de archivos.*
  - *— Para el uso de sistemas de encriptación.*
  - *— Para el uso de estándares de seguridad y protección.*
- *Protección y seguridad del hardware, componentes del sistema, periféricos y equipos asociados.*
  - *— Protección a la CPU.*
- *Mantenimiento preventivo y correctivo a la CPU.*

— *Medidas de seguridad y protección.*
— *Rutinas internas para el inicio del sistema.*
— *Rutinas internas de auditoría y verificación de componentes.*

- *Mantenimiento preventivo y correctivo al sistema.*
  — *Rutinas internas de auditoría y verificación de conexiones.*
  — *Con el uso de manuales e instructivos de operación.*
- *Mantenimiento preventivo y correctivo a los periféricos.*
  — *Rutinas internas de auditoría y verificación de periféricos.*
  — *Para el uso adecuado de los periféricos.*
- *Mantenimiento preventivo y correctivo al equipo adicional.*
  — *Rutinas internas de auditoría y verificación de equipos.*
- *Resultados de auditorías de sistemas.*
  — *Seguridad ante fenómenos sociales.*
  — *Protección contra mítines, revueltas, etcétera.*
- *Prevención de huelgas.*
- *Prevención ante cambios sociales, económicos, legales, etc.*
- *Prevención ante cambios tecnológicos.*

12.6.1 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría de la seguridad de los sistemas computacionales

En esta auditoría se evalúan todos los aspectos relacionados con la seguridad de los sistemas computacionales, de la información, del personal de sistemas y de todo lo relacionado con los bienes informáticos de las áreas de sistemas de la organización que contribuyen al mejor desempeño de la administración y control de las actividades y operaciones de la función informática en la empresa. Por esa razón recomendamos al auditor encargado de practicar esta auditoría que utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro, adaptándolas a los aspectos de carácter administrativo y técnico requeridos para evaluar las medidas preventivas y correctivas encaminadas a favorecer la seguridad, protección y salvaguarda de la función informática. Claro está, sujetando estos puntos a su experiencia, conocimientos y habilidades, y modificándolos, adaptándolos o sustituyéndolos de acuerdo con las necesidades de evaluación del sistema, con sus características, plataformas y facilidades.

Sugerimos al auditor de sistemas computacionales que, siguiendo cada uno de los puntos anotados anteriormente para la evaluación a todo lo que rodea la seguridad, protección y salvaguarda de los bienes informáticos, utilice las siguientes herramientas:

- *El diseño de* **entrevistas** (sección 9.1) **cuestionarios** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas acordes con las necesidades de su evaluación sobre la seguridad, protección y salvaguarda de activos, información y personal informáticos, así como sobre las medidas preventivas y correctivas relacionadas con la seguridad de la actividad informática del área de sistemas y de las demás áreas de la empresa que cuenten con esos sistemas.*

Además, quizá como una de las primeras acciones de evaluación, el auditor también puede utilizar las siguientes herramientas:

- *El levantamiento de* ***inventarios*** (sección 9.5), *a fin de hacer un recuento de los bienes informáticos del área de sistemas cuya seguridad se tenga que evaluar; para llevar a cabo esto, es recomendable realizar los siguientes inventarios:*
  - *— Inventarios de los equipos de cómputo, contemplando la seguridad, protección y salvaguarda de los bienes informáticos y sistemas computacionales, sus marcas, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con el inventario de la seguridad de estos equipos.*
  - *— Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas, a fin de valorar su protección y custodia.*
  - *— Inventario del personal informático y usuarios del sistema, a fin de evaluar la protección de este importante recurso.*
  - *— Inventario de las medidas de seguridad y protección para los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo sus licencias, resguardos y copias de seguridad.*
  - *— Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, a fin de valorar su protección y uso adecuados.*
  - *— Inventario de los accesos a los sistemas de redes o sistemas mayores, dependiendo del diseñado del sistema, así como del acceso a la información y a los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o sistemas mayores.*
  - *— Inventario de las instalaciones físicas, a fin de evaluar la vigilancia y los accesos establecidos para la protección y seguridad de los bienes informáticos del área de sistemas.*
  - *— Inventario de las normas, políticas, reglamentos y medidas preventivas y correctivas del área de sistemas, a fin de evaluar la seguridad establecida para satisfacer las necesidades de protección en la función informática.*

— *Otros inventarios relacionados con la seguridad, protección y salvaguarda de los bienes informáticos del área de sistemas.*

Asimismo, algunas de las herramientas que serán más utilizadas en estas auditorías son las siguientes:

- *Las técnicas de* **observación** (sección 9.4) *para evaluar los accesos a las áreas de sistemas, al propio sistema computacional, a la información y al software, y para observar el desarrollo normal de las operaciones y actividades de las áreas de sistemas, a fin de evaluar las medidas de seguridad establecidas en ellas; incluso para observar los simulacros contra contingencias de sistemas. Asimismo, cuando el caso lo requiera, el auditor podrá realizar la observación oculta, participativa y demás tipos de observación descritos en esa sección.*
- *Las técnicas de* **revisión documental** (sección 10.5) *para revisar los planes contra contingencias, manuales e instructivos de seguridad, licencias y resguardos de sistemas, bitácoras de reportes de incidencias que afectan al área de sistemas, proyectos de sistemas, bitácoras de mantenimiento y evaluación, así como los planes, programas y presupuestos para satisfacer los requerimientos de seguridad en el área de sistemas computacionales. Siempre y cuando esta revisión sea para evaluar lo que se refiere a la salvaguarda y custodia de los activos informáticos, personal, información y sistemas.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** (sección 10.8), *según sus preferencias y sus necesidades de revisión; el auditor puede auditar las fortalezas y debilidades de la seguridad del área de sistemas, tales como los planes contra contingencias adecuados, la vigilancia adecuada de los accesos y contraseñas seguras. Además puede analizar las áreas de oportunidad para fortalecer la seguridad de los sistemas de la empresa con nuevas tecnologías de protección y barreras para impedir accesos de personas ajenas a la empresa, y puede evaluar las posibles amenazas de la tecnología para evitar la fragilidad en la seguridad de los sistemas.*

Es indispensable que el responsable de la auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría de la seguridad de los sistemas computacionales:

- *La elaboración de una* **guía de evaluación** (sección 11.1), *a fin de planear específicamente cada uno los aspectos sustantivos que tenga que evaluar sobre la seguridad de los sistemas. Para ello es recomendable que tome en cuenta cada uno de los puntos indicados en esta sección, adaptándolos a las necesidades específicas de seguridad de la empresa, e incluso modificándolos para configurarlos conforme con sus propias necesidades de evaluación, y conforme a las características propias del sistema computacional que será evaluado.*

Un buen elemento de control para el responsable de esta evaluación es el siguiente:

- *El uso de la* **lista de chequeo** (sección 11.6), *ya que con esta herramienta puede verificar que quien realice la auditoría cubra todos los puntos descritos en su planeación de auditoría. Inclusive, de acuerdo con el diseño de esta lista de chequeo, también puede auditar todos los aspectos que repercuten en la protección y salvaguarda de la información, del software institucional, de los bienes informáticos, del personal y de los usuarios del área de sistemas, considerando la evaluación del cumplimiento de cada uno de los puntos contemplados en dicha herramienta.*
- *El uso de las* **técnicas de muestreo** (sección 9.6), *debido a que al evaluar el cumplimiento de las funciones, tareas y operaciones relativas a la seguridad en el área de sistemas, sería casi imposible, a la vez que inoperante, revisar todas las actividades que realiza para analizar los aspectos de seguridad. Por esa razón tiene que utilizar muestras representativas de su cumplimiento, de acuerdo con las necesidades y características de la seguridad adoptada en la empresa, su volumen de trabajo y la magnitud de acciones a estudiar. Esto, independientemente del método de muestreo que utilice en esta evaluación, puede hacer lo mismo con las actividades de los propios sistemas, sus comunicaciones y todos aquellos aspectos que puedan ser evaluados mediante el muestreo.*

Otra herramienta que puede utilizar el responsable de la auditoría, en caso de ser necesario, es la siguiente:

- *El* **acta testimonial** (sección 10.6), *debido a que en la evaluación de la seguridad de los sistemas se pueden observar muchas incidencias y con ellas fincar responsabilidades; estas actas testimoniales son una herramienta muy útil para que el auditor confirme, confronte o asiente por escrito las anomalías, deficiencias y acontecimientos que requieren de un sustento documental para fundamentar la opinión que emite. En la auditoría a los sistemas computacionales se pueden encontrar muchas incidencias, deficiencias y problemas relacionados con la seguridad del área, mismos que se deben documentar mediante esta herramienta, ya que se pueden dar casos de falta de algún bien informático; en este caso, el auditor deberá levantar esta acta; también podría encontrar software no institucional y una serie de circunstancias que, en ese momento, harán necesario el uso de esta acta documental. Recordemos que en algún caso extremo, este documento se puede utilizar como prueba testimonial de alguna incidencia especial.*

El responsable de la auditoría puede utilizar las siguientes herramientas para evaluar las funciones de los ejecutivos, empleados y usuarios de sistemas, así como el desempeño de todo lo que está alrededor de los sistemas del área de sistemas:

- *La* **ponderación** (sección 11.2), *ya que le permite evaluar el funcionamiento adecuado de cada una de las partes de la seguridad de los sistemas computacionales, dándole a cada parte el peso que le corresponde según su participa-*

ción en cada parte en que se dividan las áreas de seguridad de la función informática en la empresa. Recordemos que con esta técnica es posible darle un peso específico a cada una de las partes en que se divide la seguridad, de acuerdo con un criterio para hacer más equitativa la evaluación. Aquí se puede adoptar la ponderación de cada una de las subsecciones que conforman este subcapítulo; la responsabilidad del auditor será darle el peso a cada una de estas subsecciones en que se dividió esta parte de la auditoría y aplicar a cada parte ponderada cualquiera de los otros métodos de evaluación sugeridos, según las características del sistema.

Otras herramientas que pueden ser de gran utilidad en la evaluación de la seguridad de los sistemas computacionales son las siguiente:

- *Los* **modelos de simulación** (sección 11.3), *ya que con ellos es posible hacer simulacros de la seguridad de los sistemas, de los accesos a las áreas físicas y de los accesos a los sistemas y a la información; también se pueden realizar pruebas simuladas planeadas previamente, con las que el auditor busca vulnerar las medidas de seguridad establecidas en los sistemas computacionales, para de esta manera valorar el grado de efectividad de dichas medidas. También puede hacer todo tipo de simulaciones, de acuerdo con las necesidades de evaluación y con su experiencia.*
- *El* **análisis de la diagramación de sistemas** (sección 11.7), el cual *también puede ser una herramienta valiosa para el auditor, ya que le permite hacer el seguimiento de cualquiera de las actividades de captura, procesamiento de información y emisión de resultados de los sistemas, así como de las rutinas de programación de los sistemas, de los flujos que se siguen en la información y de las actividades y funciones relacionadas con la seguridad que se realizan en el área de sistemas, con lo cual se puede analizar la seguridad en la empresa.*

El auditor responsable de la auditoría debe tomar las sugerencias sobre los aspectos que se pueden evaluar mediante la auditoría alrededor de la computadora de acuerdo con sus necesidades específicas de evaluación, debido a que es su potestad absoluta utilizar las sugerencias, adaptarlas, modificarlas o sustituirlas por los puntos concretos que le ayuden en su auditoría. Asimismo, también tiene la facultad de utilizar las técnicas, métodos y procedimientos de auditoría que más le agraden o que conozca mejor.

12.7 Auditoría a los sistemas de redes

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de re-

des, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.

En la actualidad, las redes han invadido el entorno de los sistemas computacionales y lo más común es encontrar empresas que comparten los recursos del sistema por medio de redes computacionales para satisfacer más su actividad informática; la red más popular y de mayor aplicación en el trabajo de sistemas es la *red de área local* (**LAN:** ***L****ocal* ***A****rea* ***N****etwork*), aunque la *red de área metropolitana* (**MAN:** ***M****etropolitan* ***A****rea* ***N****etwork*) y la *red de área amplia* (**WAN:** ***W****ide* ***A****rea* ***N****etwork*), esta última de cobertura mundial, también son muy utilizadas; dentro de este grupo de redes también está la popular red mundial Internet, la más conocida por quienes cuentan con sistemas computacionales.

Cada vez es más difícil encontrar empresas que no utilicen redes de cómputo para cumplir con el registro y control de información de sus actividades cotidianas; debido a ello, es necesario realizar una auditoría a los sistemas de redes de cómputo para evaluar el comportamiento informático de muchas organizaciones. Este tipo de auditoría ha cobrado una importancia tal, que hoy en día su aplicación es altamente demandada en casi todas las instituciones en donde se realizan auditorías de sistemas.

Con la práctica de una auditoría a los sistemas de redes de cómputo, evidentemente se busca valorar todos los aspectos que intervienen en la creación, configuración, funcionamiento y aplicación de las redes de cómputo, a fin de analizar la forma en que se comparten y aprovechan en la empresa los recursos informáticos y las funciones de sistemas; también se evalúan la distribución de cargas de trabajo, la centralización de los sistemas de redes computacionales y la repercusión de la seguridad, protección y salvaguarda de información, personal y activos informáticos.

Para analizar el impacto de las redes en las empresas, se propone examinar las siguientes orientaciones que permitirán evaluar los principales aspectos que impactan el funcionamiento de los sistemas de red de área local, metropolitana y amplia, así como de Internet; estudiaremos estos aspectos a través de los siguientes rubros:

- *Los objetivos de una red de cómputo.*
- *Las características de la red de cómputo.*
- *Los componentes físicos de una red de cómputo.*
- *La conectividad y comunicaciones de una red de cómputo.*
- *Los servicios que proporciona una red de cómputo.*
- *Los sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas de la red de cómputo.*
- *Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.*

- *Los protocolos de comunicación interna de la red.*
- *La administración de una red de cómputo.*
- *La seguridad de las redes de cómputo.*

Debido al persistente y continuo avance tecnológico en el ambiente de sistemas de redes, es preciso señalar que la práctica de la auditoría a los sistemas de redes de cómputo cada vez se vuelve más compleja, minuciosa y especializada; además, debido a los constantes cambios y avances en las redes computacionales obligan al auditor de sistemas a actualizarse constantemente, en especial en los sistemas de redes. Esto es necesario si el auditor quiere contar con el suficiente conocimiento informático que le permita analizar los principales rubros que conforman una red de cómputo.

A continuación presentamos, de manera general, los principales, y más trascendentales puntos que se deben considerar en esta evaluación. Cabe aclarar que el auditor experto puede encontrar aparentes repeticiones de conceptos y puntos que se deben evaluar; sin embargo, vale la pena correr el riesgo de parecer repetitivos, en algunos casos, en aras de una mayor cobertura de los principales aspectos que se deben evaluar de los sistemas de redes de cómputo.

Como lo hemos dicho en las secciones anteriores de este capítulo, es potestad absoluta del responsable de esta auditoría utilizar los puntos tal y como aquí se proponen, modificarlos o eliminar los que no considere necesarios, de acuerdo con su experiencia, conocimientos y habilidades; siempre y cuando su objetivo sea obtener mejores resultados en su revisión. Todo de acuerdo con las características específicas de la red de cómputo que vaya a evaluar y con las peculiaridades de la administración de estos sistemas. Recordemos que no es lo mismo administrar una red de área local que una de área amplia, ni mucho menos una como Internet.

12.7.1 Evaluación del diseño, instalación y aprovechamiento de la red de cómputo

En esta parte de la auditoría se analizan las razones por las que fue necesario implantar una red de cómputo en la empresa, investigando desde cómo se hizo el análisis de las necesidades del proyecto, el diseño de la red y su configuración lógica y física, hasta su implementación y aprovechamiento.

A grandes rasgos, el auditor de sistemas debe analizar, mediante el uso de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro, los aspectos relacionados con los sistemas de red que presentamos a continuación:*

* Al auditar los sistemas de redes de la empresa, el auditor puede encontrar alguno o todos los tipos de configuración de redes, ya sean de área local (LANs), de área metropolitana (MANs) o de área amplia (WANs); por esta razón deberá adaptar los puntos que se presentan a las necesidades concretas del tipo de red que esté auditando. Aquí se presentan de manera muy general todos los aspectos que se pueden contemplar en este tipo de evaluación, sin hacer ninguna distinción si son aplicados a uno u otro tipo de red.

- *Evaluación del análisis de una red de cómputo.*
- *Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de redes de cómputo.*
- *Análisis de la definición de la problemática y solución para instalar redes de cómputo en la empresa.*
- *Análisis del cumplimiento de los objetivos fundamentales de la organización para instalar una red de cómputo, evaluando en cada caso:.*
  - *La forma de compartir los recursos informáticos de la organización, especialmente la información y los activos.*
  - *La cobertura de los servicios informáticos para la captura, procesamiento y emisión de información en la organización.*
  - *La cobertura de los servicios de comunicación.*
  - *La frecuencia con que los usuarios recurren a los recursos de la red.*
  - *La confiabilidad y seguridad en el uso de la información institucional.*
  - *La centralización, administración, operación, asignación y control de los recursos informáticos de la organización.*
  - *La distribución equitativa de los costos de adquisición y operación de los recursos informáticos de la organización.*
  - *La escalabilidad y emigración de los recursos computacionales de la organización.*
  - *La satisfacción de las necesidades del poder computacional de la organización, sea con redes, cliente/servidor o mainframe.*
  - *La solución a los problemas de comunicación de información y datos en las áreas de la organización.*
- *Análisis de la delimitación de los proyectos de red, a fin de evaluar la manera en que se cumple con:*
  - *La delimitación temporal, por el tiempo en que se instalará la red.*
  - *La delimitación espacial, por las dimensiones físicas y lógicas del proyecto de red.*
  - *La delimitación conceptual, por el análisis específico de las necesidades que se deben satisfacer con la red de cómputo.*
  - *La delimitación tecnológica, por los requerimientos y conocimientos informáticos específicos en sistemas de red.*
- *Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa, en relación con:*
  - *El estudio de factibilidad tecnológica.*

— *El Estudio de factibilidad económica.*
— *El estudio de factibilidad administrativa.*
— *El estudio de factibilidad operativa.*
— *Otros estudios de factibilidad que repercuten en el diseño e instalación de la red en la organización.*
  - *Análisis de la escalabilidad y aprovechamiento de los recursos informáticos de la empresa para instalar una red de cómputo.*
  - *Análisis de la tolerancia de las posibles fallas de la red.*

— *Análisis de la transparencia del trabajo para los usuarios de la red.*

- *Evaluación del diseño e implementación de la red según el ámbito de cobertura.**
  — *Análisis de las redes de multicomputadoras.*
    - *Evaluar el funcionamiento la cobertura de punto a punto.*
    - *Evaluar el funcionamiento la tecnología que se usa con un solo cable entre las máquinas conectadas.*
    - *Evaluar el funcionamiento de las aplicaciones, usos y explotación de estas redes.*

  — *Análisis de la red de área local (LAN).*
    - *Evaluar su cobertura de 10 metros a 1 kilómetro.***
    - *Evaluar el uso adecuado y confiable de la tecnología utilizada internamente para la transmisión de datos, como el cable coaxial, cable par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas en todas las computadoras conectadas a la LAN.****
    - *Evaluar la restricción adoptada para establecer el tamaño de la red.*
    - *Evaluar el tiempo promedio de transmisión de la red (entre el peor y el mejor caso de transmisiones conocidas de datos).*
    - *Evaluar que las velocidades utilizadas normalmente en su transmisión estén en el rango de 10 a 100 Mbps.*****

* En los siguientes puntos mostraremos los diferentes aspectos que el auditor puede llegar a encontrar en la evaluación de una red de cómputo, los cuales se pueden presentar según el tamaño y configuración del sistema en uno u otro de los puntos señalados, o varios de éstos a la vez. Lo importante es que el auditor cuente con el conocimiento de los aspectos de redes que debe evaluar.

** Para evaluar las coberturas entre estas redes se deben actualizar los estándares para el alcance de la comunicación de la red; actualmente se tienen establecidas: LANs de 0.1 a 10 km^2, MANs de 10 a 100 km^2 y WANs de más de 100 km^2.

*** Para evaluar la tecnología utilizada para la transmisión de datos, también se tienen que actualizar los medios de comunicación física, como el cable coaxial, cable par trenzado, fibra óptica o de transmisión de radio, microondas, satélites, infrarrojo o cualesquier otros mecanismos de comunicación sin cable.

**** Mbps (megabits por segundo; un megabit está compuesto por 1.000.000 de bits).

— *Análisis de la red de área metropolitana (MAN).*
- *Evaluar su cobertura de 10 a 100 km.*
- *Evaluar los criterios adoptados para establecer el tamaño y cobertura de la red.*
- *Evaluar el funcionamiento de la tecnología utilizada internamente en la transmisión de datos, como el cable coaxial, cable par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas en todas las máquinas conectadas en la red LAN.*
- *Evaluar el tiempo promedio de transmisión de la red.*
- *Evaluar las velocidades utilizadas normalmente en su transmisión.*

— *Análisis de la red de área amplia (WAN)*
- *Evaluar su cobertura de 100 a 1,000 km.*
- *Evaluar el funcionamiento de la composición, consistente en la colección de hosts (computadoras interconectadas) o LANs de hosts conectados por medio de subredes.**
- *Evaluar la forma de enviar los paquetes de un enrutador router a otro, según las características de envío de la red.***
- *Evaluar el uso adecuado y confiable de la tecnología utilizada (interna y externamente) en la transmisión de datos, como el cable coaxial, cable par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas en todas las máquinas conectadas a las LANs y a la WAN.*
- *Evaluar la conveniencia del tiempo promedio de transmisión de la red entre LANs y entre subredes.*
- *Evaluar que las velocidades utilizadas normalmente en su transmisión, sean conforme a los rangos establecidos para este tipo de redes.*

— *Análisis de las redes públicas (también incluida Internet).*
- *Evaluar su cobertura de 10,000 a 100,000 km.*
- *Evaluar la composición de esta red, consistente en la integración de la red Internet a la vinculación con puertas de enlace (gateways), computadoras que pueden traducir entre formatos incompatibles.*
- *Evaluar el uso adecuado y confiable de la tecnología y sistemas de interconexión utilizados (interna y externamente) en la transmisión de datos, como el cable coaxial, cable par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas.*

* La subred consiste en las líneas de transmisión y los *enrutadores,* que son computadoras dedicadas a cambiar de ruta.

** Éstos son *packet* ***switching,*** *por medio de* paquetes de enrutador o ***store-and-forward****, porque son de* guardar y reenviar.

  - *Evaluar las velocidades utilizadas normalmente en su transmisión.*
- — Análisis de la redes inalámbricas.
  - *Evaluar el uso adecuado de este tipo de red según sus características.*
  - *Evaluar el uso adecuado y confiable de la transmisión de datos por medio de radio, microondas, satélites o infrarrojo o cualesquier otros mecanismos de comunicación sin cable.*
  - *Evaluar La posibilidad de combinar las redes inalámbricas con otras computadoras móviles u otras redes.*
  - *Evaluar las posibilidades de integrar Internet o su vinculación con puertas de enlace u otros sistemas de computadoras que pueden traducir entre formatos incompatibles.*

- *Evaluación del diseño e instalación de la red según su configuración básica.*
  - *— Análisis del diseño e implementación de los tipos de redes establecidos en la empresa:*
    - *Red basada en el concepto de servidor único.*
    - *Red basada en el concepto cliente/servidor.*
    - *Red de punto a punto (uno a uno).*
    - *Redes de multipunto (uno a muchos, muchos a muchos).*
    - *Red lógica, basada en el concepto de conexión entre terminales sin cables.*
    - *Red virtual basada en el concepto de tecnología y comunicación vía Internet.*
  - *— Análisis del diseño e implementación de la topología de cobertura de la red, en cuanto a:*
    - *Estudio de las necesidades de cobertura con la topología física de la red.*
    - *Estudio de las necesidades de cobertura con la topología lógica de la red.*
  - *— Análisis del diseño de los modelos de comunicación ISO de la red de la empresa, en cuanto al funcionamiento de las siguientes capas:*
    - *Capas físicas.*
    - *Capas de enlace.*
    - *Capas de red.*
    - *Capas de transporte.*
    - *Capa de sesión.*
    - *Capa de presentación.*
    - *Capa de aplicación.*
  - *— Análisis de los estándares adoptados para el funcionamiento de las siguientes redes:*

- *Ethernet (norma IEEE 802.3).*
- *Token Ring (norma IEEE 802-5).*
- *ARCnet (Attached Resource Computer Network, Red de Computadoras de Recursos Conectados).*
- *IPX (Internetwork Packet Exchange, Intercambio de Paquetes entre Redes).*

• *Evaluación del diseño e implementación de la red según sus características.*

— *Análisis de la confiabilidad en el funcionamiento de los medios de transmisión y del medio físico que utiliza la red para la comunicación entre las computadoras que la integran.*

- *Cableado.*
- *Transmisión por radio, microondas, satelital, infrarrojo y cualesquier otros tipos de comunicación sin cable.*
- *Combinación de ambos medios de transmisión.*

— *Análisis de las técnicas de transmisión que determinan cómo se utilizan los medios físicos para la comunicación entre las computadoras de la red, estudiando el funcionamiento de:*

- *La transmisión síncrona.*
- *La transmisión asíncrona.*
- *La transmisión analógica.*
- *La transmisión digital.*
- *La codificación de datos en señales analógicas.*
- *La transmisión en paralelo.*
- *La transmisión en serie.*
- *Los códigos de comunicación de datos.*

— *Análisis del funcionamiento y confiabilidad de los dispositivos para conectar las redes, tales como:*

- ***Repetidores.** Sirven para amplificar o regenerar las señales, con lo cual se pueden utilizar cables más largos.*
- ***Puentes (bridges).** Son los dispositivos de guardar y reenviar los datos en la red, y operan en el nivel de enlace y pueden cambiar los campos de los marcos.*
- ***Enrutadores (routers) de protocolos múltiples.** Son como los puentes que admiten el funcionamiento de la red en este nivel y que permiten la conexión de redes con distintos protocolos.*
- ***Puertas de enlace (gateways) de transporte.** Que permiten la conexión de las redes en el nivel de transporte.*

  - ***Puertas de enlace de aplicación.*** *Conectan dos partes de una aplicación, aunque éstas utilicen formatos distintos.*
- *— Análisis del funcionamiento de las técnicas de transferencia de datos.*
  - ***Simplex.*** *Solamente en un sentido.*
  - ***Half-duplex.*** *En ambos sentidos, pero uno a la vez.*
  - ***Full-duplex.*** *En ambos sentidos a la vez.*
- *— Análisis de los tipos de topologías utilizados en el diseño de la red.*
  - *Topología de bus.*
  - *Topología de estrella.*
  - *Topología de anillo.*
  - *Topología de malla.*
  - *Topología de doble anillo.*
- *— Análisis de los métodos de acceso al medio y de la manera en que se conectan los dispositivos de la red para utilizar la transmisión por el medio físico.*

• *Evaluación del diseño e implementación de los componentes de la red de cómputo.*

- *— Análisis del diseño e implementación del tipo de servidor principal para la red.*
  - *Servidores dedicados.*
  - *Servidores no dedicados.*
- *— Análisis del diseño e implementación de los servidores de apoyo.*
  - *Servidores de archivos (distribuidos, dedicados y no dedicados).*
  - *Servidores de discos (dedicados y no dedicados).*
  - *Servidores de impresión.*
  - *Servidores de comunicación.*
  - *Concentradores.*
  - *Otros tipos de servidores.*
- *— Análisis del diseño e implementación de las estaciones de trabajo.*
  - *Características y componentes de la terminal o estación de trabajo.*
  - *Número de terminales o estaciones de trabajo.*
  - *Aplicaciones de la terminal o estación de trabajo.*
  - *Privilegios, información y uso de la terminal o estación de trabajo.*
- *— Análisis del diseño e implementación de los nodos de la red.*
- *— Análisis del uso de las tarjetas de la red.*
  - *Tarjetas de interfaz de red.*

- *Adaptador de 2Mbps (este adaptador soporta longitudes de hasta 500 metros de cable par trenzado sin blindaje o UTP).*
- *Adaptador Ethernet AE-1/t de bajo costo y número limitado por número de puertos HUB y velocidad de transferencia de 10 Mbps.*
- *Adaptador Ethernet AE-2; es un adaptador inteligente con autoconfiguración de selección de parámetros óptimos de funcionamiento.*
- *Adaptador Ethernet AE-2/t para conexiones de cable UTP y cable coaxial.*
- *Adaptador Ethernet AE-3 para soportar tres tipos de cable: UTP, Coaxial grueso y coaxial delgado.*

— *Análisis del funcionamiento y confiabilidad de los elementos de enlace físico de la red.*

- *Cable par trenzado de amplio rango, sin blindaje y UTP.*
- *Cable coaxial.*
- *Cable de banda base para un solo canal con un solo mensaje a la vez y velocidades de 10 a 80 Mbps.*
- *Cable de banda ancha; este cable maneja varias bandas a la vez y en diferentes frecuencias de manera simultánea, con sistema dual de cable o un solo cable y amplificadores bidireccionales.*
- *Cable de fibra óptica.*

— *Análisis de la confiabilidad y funcionamiento correcto de los elementos establecidos para la expansión de la red.*

- *Repetidores, para recibir y retransmitir datos, compensando las pérdidas de señal.*
- *Puentes (bridges) y dispositivos para la capa de enlace OSI, para manejar datos de rigen y destino de la información.*
- *Puentes/enrutadores, dispositivo de interconexión de la red.*
- *Enrutadores relacionados directamente con los protocolos de comunicación.*
- *Puertas de enlace, dispositivos para la conexión de minicomputadoras y macrocomputadoras (mainframes).*

• *Evaluación del diseño e implementación de los protocolos de comunicación de la red.*

— *Análisis de la adopción de jerarquías de protocolos en la red de la empresa, en relación con:*

- *El software para controlar las redes y las estructurar para manejar la complejidad.*
- *La organización en la mayor parte de las redes en una pila de niveles.*

- *Los niveles que ofrecen ciertos servicios a los niveles superiores y la implementación de estos servicios en el nivel inferior siguiente para brindarlos.*
- *El nivel de comunicación **n** de una computadora con el nivel **n** de otra computadora.*
- *Las reglas y convenciones que controlan la conversación entre las computadoras, según el nivel **n** de los protocolos.*
- *Las entidades en niveles correspondientes de comunicación entre computadoras distintas.*
- *La transferencia de los datos directamente del nivel **n** de otro nivel, a fin de pasar la información hacia abajo de un nivel a otro hasta que llegue al nivel del medio físico.*
- *Los niveles donde están las interfaces permiten cambios en el establecimiento de un nivel sin afectar el nivel superior.*
- *El nivel que tiene que transmitir un paquete a otra computadora para que ésta pueda agregar un encabezamiento al paquete y puedan identificar el mensaje y el destino al nivel de la mayor parte de las redes para imponer el límite en el tamaño de los paquetes.*

— *Análisis del funcionamiento del modelo OSI (Open Systems Interconection Reference Model; Modelo de Referencia de Interconexión de Sistemas Abiertos) para la red, estudiando el comportamiento de los siguientes niveles:*

- ***Nivel físico.** Para las relaciones de los voltajes, la duración de un bit, el establecimiento de una conexión, el número de polos de enchufe y demás aspectos técnicos de este nivel.*
- ***Nivel de enlace.** Para convertir el medio de transmisión inicial en uno que esté libre de errores de transmisión de datos en cuanto al remitente de los datos de entrada, el procesamiento del acuse de datos y el manejo de los marcos perdidos, dañados o duplicados, y en cuanto a la regulación de la velocidad del tráfico.*
- ***Nivel de red.** Para determinar el ruteo de los paquetes desde sus fuentes a sus destinos, manejando la congestión a la vez y su incorporación a la función de contabilidad.*
- ***Nivel de transporte.** Es el primer nivel de comunicación directa de su par en el destino (los anteriores niveles son de computadora a computadora). Este nivel suministra varios tipos de servicio: abrir conexiones múltiples de red para proveer capacidad alta, se puede utilizar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples entrando en una máquina y abastece el control de flujo entre los hosts.*

- ***Nivel de sesión.*** *Parecido al nivel de transporte, pero provee servicios adicionales, ya que puede manejar Token (objetos abstractos y únicos) para controlar las acciones de participantes o puede hacer checkpoints (puntos de recuerdo) en las transferencias de datos.*
- ***Nivel de presentación.*** *Provee funciones comunes a muchas aplicaciones, tales como traducciones entre juegos de caracteres, códigos de números, etcétera.*
- ***Nivel de aplicación.*** *Define los protocolos usados por las aplicaciones individuales, de la red, entre estas aplicaciones tenemos el manejo de E-mail y de Telnet, entre otros.*

— *Análisis del funcionamiento adecuado de los protocolos X.25 para la red, estudiando el comportamiento de sus siguientes capas:*

- *Capa física.*
- *Capa de bloque.*
- *Capa de paquetes.*

— *Análisis del funcionamiento adecuado de los protocolos TCP/IP (Transmission Control Protocol/Internet Protocol, Protocolo de Control de Transmisión/Protocolo Internet).*

- *Evaluar en cumplimiento de los objetivos, la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.*
- *Evaluar la aplicación de red packet switching (o de conmutación de paquetes), basada en un nivel de Internet sin conexiones.*
- *Evaluar la aplicación y el funcionamiento de los niveles físico y de enlace (nivel de hosts a red) y su definición (si es que la hay) en esta arquitectura.*
- *Evaluar el funcionamiento del* ***nivel de Internet****, en el que los hosts introducen paquetes en la red que viajan independientemente del destino, pero sin garantías de entrega ni de orden.*
- *Evaluar la definición que provee el ruteo y control de congestión en el nivel del IP (Protocolo Internet).*
- *Evaluar el funcionamiento del* ***nivel de transporte****. Esto permite que los pares en los hosts de fuente y destino puedan conversar en sus dos protocolos: TCP (Transmission Control Protocol, Protocolo de Control de Transmisión), el cual permite que dos computadoras conectadas a Internet establezcan una conexión confiable para la entrega sin errores de un flujo de bytes; también maneja el control de flujo. Y el UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario). Este protocolo es menos confiable que el TCP y no intenta establecer una conexión con una*

computadora remota para la entrega de mensajes discretos o para la entrega rápida, cuando ésta es más importante que la entrega garantizada.

- *Evaluar el funcionamiento del **nivel de aplicación**. Como en OSI. No usa los niveles de sesión o presentación.*
- *Evaluar el funcionamiento del **protocolo Telnet** para terminales virtuales.*
- *Evaluar el funcionamiento del **SMTP** (Simple Mail-Transport Protocol-/Protocolo Simple de Transporte de Correo).*
- *Evaluar el funcionamiento del **FTP** (File Transfer Protocol, Protocolo de Transferencia de Archivos).*
- *Evaluar el funcionamiento del **SNMP** (Simple Network Management Protocol, Protocolo Simple de Administración de Red).*

— *Análisis del funcionamiento de los protocolos.*

- *IP (Internet Protocol, Protocolo Internet).*
- *ICPM (Internet Control Message Protocol, Protocolo de Mensajes de Control en Internet).*
- *TCP (Transmisión Control Protocol, Protocolo de Control de la Transmisión).*
- *UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario).*
- *FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos).*
- *SMTP (Simple Mail Transport Protocol, Protocolo Simple de Transporte de Correo).*
- *SNMP (Simple Network Management Protocol, Protocolo Simple de Administración de Red).*
- *DNS (Domain Name System, Sistema de Nombres de Dominio).*
- *Telnet (Telecommunication Network, Red de Telecomunicaciones).*

— *Análisis de otros protocolos de transmisión de una red.*

— *Análisis del funcionamiento del método de transmisión de datos CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Acceso Múltiple por Percepción de Portadora con Detección de Colisiones).*

- *Evaluación de la instalación física de la red.**
  — *Análisis del diseño arquitectónico de las instalaciones de la red.*
  — *Análisis de los elementos de enlace y cableado de la red.*
  — *Análisis del mantenimiento físico, correctivo y preventivo de los foros donde están las instalaciones de la red.*

* Se refiere a los mismos aspectos señalados en *Auditoría al diseño e implementación a los componentes de la red de cómputo y Auditoría al diseño e implementación de los protocolos de comunicación de la red, solo que adaptadores a la evaluación física de éstos*.

— *Análisis de la instalación, funcionamiento y mantenimiento de las tarjetas que configuran la red.*

— *Análisis de la instalación, funcionamiento y mantenimiento de los servidores y terminales de la red de la empresa.*

— *Auditoría de los elementos de expansión de la red.*

- *Evaluación de los aspectos técnicos de la red de cómputo.**
  — *Análisis de los estándares de redes locales, según la referencia y formatos que se utilicen para el funcionamiento de la red de la empresa.*
    - *Modelo de Referencia OSI (Open System Interconnection, Interconexión de Sistemas Abiertos).*
    - *Norma IEEE 802 (Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos).*
    - *Métodos de acceso CSMA/CD (Carrier Sense Multiple Access With Collision Detection, Acceso Múltiple por Percepción de Portadora con Detección de Colisiones).*
    - *IPX (Internetwork Packet Exchange).*
    - *SPX (Secuenced Packet Exchange).*
  — *Análisis del funcionamiento técnico de los sistemas operativos de la red.*
- *Evaluación de la administración y control de la red de cómputo.***
  — *Análisis del acceso a los siguientes aspectos de la red:*
    - *A la información institucional por áreas, privilegios y niveles de operación de los datos.*
    - *A los sistemas y software.*
  — *Análisis del cambio periódico de niveles, privilegios y contraseñas de acceso al sistema.*
  — *Análisis de los reportes de incidencias, contingencias y circunstancias que afecten el funcionamiento de la red, a su información o software.*
  — *Análisis de la atención y rapidez de respuesta para satisfacer las necesidades informáticas de los usuarios del sistema.*
  — *Análisis de la existencia, acatamiento y actualización de las políticas y reglamentos de uso de los sistemas computacionales de la red.*

* Para realizar esta auditoría se recomienda adaptar algunos puntos establecidos en la **auditoría al sistema computacional** (sección 12.4), ya que son muy similares a los que se tratan en esta evaluación.
** Para realizar esta auditoría se recomienda adaptar algunos puntos señalados en la **auditoría a la gestión informática** del área de sistemas (sección 12.3), ya que son muy similares a los que se tratan en esta evaluación.

— *Análisis del cumplimiento de la actividad informática de los servidores, terminales, sistemas y programas de cómputo utilizados para satisfacer las necesidades de los usuarios del sistema.*

— *Análisis de la atención y solución de algunas diferencias en la operación entre redes:*

- ***La clase de servicio.*** *Evaluando su orientación permanente a la conexión o no-conexión de las terminales de servicio, de acuerdo con las políticas del área de sistemas.*
- *El funcionamiento adecuado de los protocolos de la red.*
- *El funcionamiento correcto de direcciones, ya sean por un nivel o jerárquicas.*
- *El manejo de los tamaños de paquetes que se manejan en la red, según su máximo.*
- *El control de errores para la entrega confiable y en orden o sin orden de la información que se transmite en la red.*
- *Control del flujo y de velocidad de transmisión de los datos de la red.*
- *Control de congestión del manejo de la información, transmisión y protocolos de la red.*
- *Administración y control de la problemática de seguridad de la red, la información, los usuarios, los sistemas computacionales y de las instalaciones físicas.*
- *Contabilidad de los tiempos de uso del sistema, ya sea por conexión de las terminales, por paquete, por byte, por proceso o por cualquier otra actividad que se realiza en los sistemas de la red.*

• *Evaluación de la seguridad y protección de la red y de los activos informáticos de la empresa.**

— *Análisis del funcionamiento de los mecanismos de control de acceso a las instalaciones, información y software institucionales.*

— *Análisis de la prevención de accesos múltiples, sin permisos, dolosos y de todas aquellas acciones para ingresar al sistema sin la autorización correspondiente.*

— *Análisis del procesamiento de información en los sistemas de red.*

— *Análisis de la administración y el control de la asignación de los de niveles de acceso, privilegios y contraseñas para los usuarios para ingresar al sistema y la información.*

— *Análisis del monitoreo de las actividades de los usuarios.*

* Aquí se recomienda utilizar los puntos señalados en la **auditoría de la seguridad de los sistemas computacionales** (sección 12.6), salvo que en este caso tiene que adaptar específicamente las necesidades de la auditoría a la configuración, topología y demás características de la red de cómputo que audite.

— *Análisis de las medidas correctivas y preventivas para evitar la piratería de información, software, activos informáticos y consumibles del área de sistemas.*

— *Análisis de la realización, actualización y custodia de los respaldos de sistemas e información que se procesan en la red.*

— *Análisis de las Auditorías periódicas del funcionamiento de la red.*

— *Análisis de las medidas preventivas y correctivas para erradicar de la red los virus informáticos.*

— *Análisis del establecimiento de las barreras físicas y lógicas para proteger los accesos de intrusos, piratas, hackers y crackers informáticos y cualquier otra intromisión, accidental o dolosa.*

- *Evaluación del uso y funcionamiento adecuado del software de la red.*

— *Análisis de los sistemas operativos para el funcionamiento de la red.*

— *Análisis de los lenguajes y programas de desarrollo de la red.*

— *Análisis de los programas y paquetes de aplicación de la red.*

— *Análisis a las utilerías, librerías y bibliotecas de la red.*

— *Análisis de la disponibilidad de licencias y permisos de instalación del software de la red.*

— *Análisis de la actualización informática y de los proveedores de sistemas de la red.*

— *Análisis del diseño de nuevos proyectos informáticos para el funcionamiento de la red.*

— *Análisis de la actualización tecnológica del software desarrollado en la empresa y del que se encuentra en el mercado.*

— *Análisis de la administración y control de las utilerías, librerías y bibliotecas para el funcionamiento adecuado de la red.*

— *Análisis de las utilerías para el funcionamiento del software y juegos no autorizados (piratas).*

- *Evaluación del mantenimiento de la red.*

— *Análisis de los reportes y servicios de mantenimiento correctivo y preventivo de la red.*

— *Análisis de las bitácoras y estadísticas de incidencias de la red.*

— *Análisis de las estadísticas de incidencias, descomposturas, caídas del sistema, colisiones, pérdidas de información y demás detalles que repercuten en la operación de la red.*

Como pudimos observar en el estudio de estos puntos, la auditoría a la red de cómputo es mucho más especializada y, por lo tanto, para realizarla es necesario tener un amplio conocimiento en el ambiente de los sistemas de red, así como una amplia

experiencia en el manejo de los aspectos concretos que se deben auditar sobre su administración y operación, según la configuración, tipo, características, tamaño y componentes de la red de cómputo de la organización, tanto de su hardware y software como del espacio físico donde está instalada.

Debemos señalar nuevamente que el responsable de la auditoría debe seleccionar de los puntos señalados anteriormente aquellos que considere que satisfacen sus necesidades de evaluación; asimismo, el auditor está en libertad absoluta de modificar o eliminar los puntos que le servirán para una mejor evaluación de la red de cómputo.

12.7.2 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría a los sistemas de redes

En esta auditoría se evalúan los aspectos específicos de la red de cómputo, considerando las características de la red, su tamaño y cobertura, configuraciones física y lógica, topologías, protocolos de comunicación y aspectos técnicos de su composición; también se evalúa la forma en que se aprovechan los recursos informáticos de la organización, la información y todo lo relacionado con la función informática en la institución. Esto con el objeto de validar la administración adecuada de la red, su funcionamiento correcto y el aprovechamiento de las actividades informáticas de la empresa.

Por esta razón se recomienda al auditor que practique esta auditoría a los sistemas de redes que utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro.

El responsable de esta auditoría puede adaptar esas herramientas a los aspectos de carácter técnico que se requieren para evaluar todo lo señalado en esta sección. Claro está, como en los casos anteriores, utilizando esos puntos de acuerdo con su experiencia, conocimientos y habilidades, e incluso adaptándolos o sustituyéndolos por aquellos requerimientos específicos que sean necesarios de acuerdo con la evaluación, con sus características, plataformas, facilidades y demás distintivos propios de esta auditoría.

Es recomendable que el auditor de sistemas computacionales utilice las siguientes herramientas, siguiendo cada uno de los puntos anotados anteriormente, para evaluar todo lo que rodea a los sistemas de redes:

- *El diseño de* **entrevistas** *(sección 9.1),* **cuestionarios** *(sección 9.2) y* **encuestas** *(sección 9.3) elaborados con preguntas acordes con las necesidades de su evaluación sobre la configuración de la red, el análisis y diseño para su instalación, la configuración e instalación física y lógica de la red, así como sobre la actualización informática, emigración de sistemas, las medidas preventivas y correctivas relacionadas con la seguridad de la actividad informática del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.*
- *También puede utilizar dichas herramientas para evaluar la opinión de los usuarios de sistemas, respecto al funcionamiento de la red, la frecuencia de fallas, si las hay, la satisfacción de sus necesidades informáticas, la disponibilidad de los*

sistemas y el manejo de la información de sus áreas, así como sobre la administración de sistemas de red en la empresa.

Además, quizá como una de las primeras acciones de evaluación, el auditor de sistemas también puede utilizar esta herramienta:

- *El levantamiento de* **inventarios** *(sección 9.5), a fin de hacer un recuento de los bienes informáticos destinados al funcionamiento de la red y del área de sistemas, así como de los bienes informáticos que se pueden analizar en el funcionamiento de los sistemas que conforman la red. Para llevar a cabo esto, es recomendable realizar los siguientes inventarios:*
  - *Inventarios de los componentes de las redes de cómputo de la empresa, que incluyan servidores, terminales, cableados, componentes y demás bienes informáticos que integran la red, así como los fabricantes, marcas, modelos procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con el inventario de la seguridad de estos equipos.*
  - *Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, así como de las licencias, resguardos, originales, copias autorizadas y copias pirata, a fin de valorar la protección y custodia de dichos sistemas.*
  - *Inventario de la seguridad y protección de la información y de los datos del sistema de red.*
  - *Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, a fin de valorar su protección y uso.*
  - *Inventario de los accesos a los sistemas de redes, así como del acceso a la información que se maneja en ellos y los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o de equipos mayores en red.*
  - *Inventario de las instalaciones físicas de las redes, a fin de evaluar los accesos establecidos para la protección de los bienes informáticos del área de sistemas, así como su uso.*
  - *Inventario de configuraciones, protocolos, tarjetas y demás características técnicas del funcionamiento de los sistemas de red.*
  - *Inventario de las normas, políticas, reglamentos y medidas preventivas y correctivas del área de sistemas, a fin de evaluar la seguridad establecida para satisfacer las necesidades de protección de la función informática.*
  - *Otros inventarios relacionados con la seguridad, protección y salvaguarda de los bienes informáticos del área de sistemas.*

Otras herramientas que es recomendable utilizar en estas auditorías son las siguientes:

- *Las técnicas de* **observación** (sección 9.4)*, a fin de evaluar el funcionamiento normal del sistema operativo de la red, el procesamiento y uso de la información y del software de la empresa, así como para observar el desarrollo normal de las operaciones y actividades de los usuarios de la red, actividades y acciones de éstos para comprobar las medidas de seguridad establecidas para la red, e incluso para la observación de su comportamiento durante simulacros realizados de acuerdo con los planes contra contingencias de los sistemas de la red. Asimismo, cuando el caso lo requiera, el auditor podrá realizar la observación oculta, el monitoreo, la observación participativa y los demás tipos de observación descritos en esa sección.*
- *Las técnicas de* **revisión documental** (sección 10.5) *para revisar los proyectos de instalación de la red, planos de configuración de cableado, configuraciones, distribución de los componentes de la red, los planes contra contingencias, manuales e instructivos de seguridad, licencias y resguardos de sistemas, bitácoras de reportes de incidencias que afectan a la red y al desarrollo de proyectos de redes y de nuevos sistemas, bitácoras de mantenimiento y evaluación, así como planes, programas y presupuestos para satisfacer los requerimientos de operación y funcionalidad de la red de cómputo. Siempre y cuando esta revisión se realice para evaluar lo que se refiera a la administración y control de las funciones de la red, de los activos informáticos que la integran, así como el manejo de su información y sus sistemas.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** *(sección 10.8), según las preferencias y necesidades de revisión del auditor; con estas herramientas puede auditar las fortalezas y debilidades del funcionamiento de la red de cómputo, tales como la administración del servidor, las terminales, el software, la información, el aprovechamiento de los recursos informáticos de la empresa y la respuesta a las necesidades informáticas. También puede analizar las áreas de oportunidad para fortalecer la comunicación entre los sistemas de la empresa, la actualización de tecnologías de protección y las barreras para proteger los accesos del exterior. También puede analizar las posibles amenazas del avance de la tecnología de redes y de comunicación para evitar la fragilidad en la actualización de los sistemas de red.*

Es indispensable que el responsable de esta auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría a los sistemas de redes:

- *La elaboración de una* **guía de evaluación** (sección 11.1)*, a fin de planear específicamente cada uno los aspectos importantes del funcionamiento de las redes que tiene que evaluar, tanto en lo técnico, como en la configuración, operación, compatibilidad, comunicación y demás aspectos relacionados con el funciona-*

miento de la red. Para ello es recomendable que tome en cuenta cada uno de los puntos indicados en el inicio de esta sección, adaptándolos a las necesidades específicas de la red en la empresa, e incluso modificándolos para adecuarlos conforme a sus propias necesidades de evaluación, y conforme a las características propias del sistema de red, a su tamaño, componentes, configuración y demás peculiaridades de la red.

Un buen elemento de control para el responsable de esta evaluación es el siguiente:

- *El uso de la* **lista de chequeo** (sección 11.6), *ya que con esta herramienta puede verificar que quien realice la auditoría cubra todos los puntos descritos en su planeación de auditoría. Inclusive, de acuerdo con el diseño de esta lista de chequeo, también puede auditar todos los aspectos que repercuten en la red de la empresa.*
- *El uso de las técnicas de* **muestreo** (sección 9.6), *debido a que al evaluar el cumplimiento de las funciones, tareas y operaciones relativas a la administración y funcionamiento de una red de cómputo, sería casi imposible, a la vez que inoperante, revisar todas las actividades que se realizan en la red, más aún cuando ésta es WAN o Internet. Por esta razón tiene que utilizar muestras representativas del cumplimiento de las operaciones de la red, de acuerdo con las necesidades y características de la red adoptada en la organización, así como con su configuración, componentes y la magnitud de interacciones que ocurren en la transmisión de datos de la red. Esto independientemente del método de muestreo que se utilice en esta evaluación.*
  Puede hacer lo mismo con las actividades de los protocolos de transmisión de información, el manejo de sus sistemas de comunicación, el procesamiento de información y operaciones que permiten el funcionamiento de la red y todos aquellos aspectos que se puedan evaluar mediante el muestreo de las actividades de la red.

El responsable de la auditoría puede utilizar la siguiente herramienta para evaluar las funciones de los ejecutivos, empleados y usuarios de sistemas, así como el desempeño de todo lo que está alrededor del funcionamiento de una red de cómputo:

- *La* **ponderación** (sección 11.2) *es una herramienta muy útil , ya que le permite evaluar el funcionamiento adecuado de cada una de las partes de la red de cómputo, al asignarle a cada parte el peso que, según su criterio, le corresponda, para hacer más equitativa la evaluación, en este caso a cada una de las partes consideradas como división fundamental del funcionamiento de una red; por ejemplo, la evaluación del diseño de la red, del funcionamiento de los protocolos, de la parte técnica de su funcionamiento o cualquier otra división establecida por el auditor*
  Recordemos que con esta técnica es posible darle un peso específico a cada una de las partes en que se divide la actividad de las redes, y que la ponderación se tiene que adoptar de cada una de las subsecciones que conforman este

subcapítulo. La responsabilidad del auditor será darle el peso a cada una de estas subsecciones en que se dividió esta parte de la auditoría y aplicar a cada parte ponderada cualquiera de los otros métodos de evaluación sugeridos, según las características de la red.

Otras herramientas que pueden ser de gran utilidad en la evaluación de la red de cómputo son las siguientes:

- *Los* **modelos de simulación** (sección 11.3), *ya que con ellos es posible hacer simulacros del funcionamiento de la red, de los accesos a las áreas físicas y de los accesos a los sistemas y a la información de la red; también se pueden realizar el desarrollo de pruebas simuladas, planeadas previamente, con las que el auditor realiza actividades concretas para utilizar la red de una manera inadecuada y ver su comportamiento. También puede hacer todo tipo de simulaciones, de acuerdo con las necesidades de evaluación y con su experiencia.*
- *El* **análisis de la diagramación de sistemas** (sección 11.7), *el cual también puede ser una herramienta valiosa para el auditor, ya que le permite hacer el seguimiento de las redes de cómputo, de su instalación, diseño e implementación, así como el seguimiento de cualquier actividad de captura, procesamiento y emisión de resultados de los sistemas de red, de los flujos que se siguen en la transmisión de la información entre las partes que la integran, además del seguimiento de las rutinas de los programas de ésta o de las actividades y funciones que se realizan en ella.*

El responsable de la auditoría debe tomar las sugerencias anteriores sobre los aspectos que se pueden evaluar mediante la auditoría a los sistemas de redes de acuerdo con sus necesidades específicas de evaluación, ya que es su potestad absoluta utilizarlas como están, adaptarlas e inclusive sustituirlas por aquellos puntos concretos que le ayuden a realizar su auditoría. También debe utilizar las técnicas, métodos y procedimientos de auditoría que le convengan más o las que conozca más.

12.8 Auditoría outsourcing en los sistemas computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

Es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad, eficiencia y oportunidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra. Esto se lleva a cabo con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas.

Conviene iniciar el tratamiento de esta auditoría analizando brevemente el concepto **outsourcing**, vocablo derivado de **out**: fuera y **source**: manantial, fuentes; su definición es la siguiente:

> *"Estamos hablando de la subcontratación de servicios, partiendo del supuesto de que sí existe un tercero capaz de hacer el trabajo con mayor eficiencia y a menor costo de lo que se puede lograr al interior de la organización. Éste es, como muchos otros en la administración moderna, un término nuevo para un viejo concepto".*[3]

Este concepto antiguo se refiere con el nombre nuevo a la prestación de un servicio, generalmente especializado, que un particular proporciona a una empresa que lo contrata, a fin de realizar las actividades que ésta no puede, no quiere o no está capacitada para realizar por sí misma; estos servicios son muy diversos, pero los más conocidos y populares son los siguientes:

- ***Servicio de comedor para los empleados.*** *Es cuando la empresa proporciona este servicio a sus empleados, pero contrata a un particular para que lo realice por ella, sea en instalaciones propias o del prestador del servicio.*
- ***Contratación y capacitación de empleados.*** *Es cuando la empresa solicita los servicios de un tercero para la selección y capacitación de su personal, en lugar de realizarlo ella misma.*
- ***Servicios de limpieza y mantenimiento.*** *Es cuando la institución contrata a terceros para que realicen el aseo, la limpieza y el mantenimiento en sus instalaciones, evitando con ello la carga de esta función y el manejo de personal en esta actividad.*
- ***Servicios contables de auditoría, legales y trámites administrativos.*** *Es cuando la empresa contrata a un tercero para que le realice todas las actividades inherentes al aspecto contable y administrativo, así como la representación legal y auditorías en la empresa.*

Podemos definir el concepto outsourcing informático de la siguiente manera:

> *Es la subcontratación de los servicios de cómputo, a fin de que la empresa contratante libere a su personal e instalaciones de la práctica de la actividad informática y encomendar su realización en otros especialistas con más conocimientos, más eficiencia y a un costo menor.*

Está claro que la actividad informática desarrollada con recursos propios muchas veces eleva considerablemente los costos de su realización, debido a que son excesivos, comparados con los beneficios que obtiene la empresa de esta actividad. Sin embargo, en la actualidad es indispensable que las empresas cuenten con esta importante actividad de apoyo para el registro y manejo de su información, a pesar de los elevados costos de dicha actividad. Hoy en día las empresas tienen que estar a la vanguardia en el ámbito de sistemas, a pesar del costo que estas actividades representan para ellas.

Debemos tomar en cuenta que las empresas tienen que desembolsar una cantidad inicial para adquirir los sistemas computacionales necesarios para el funcionamiento de estas áreas, así como el hardware, periféricos y software para el desarrollo y aplicación de los sistemas, el mobiliario especializado para los equipos y el mobiliario de oficina, y la adaptación de las instalaciones; además continuamente tienen que realizar gastos para la contratación de funcionarios y empleados y para consumibles y materiales de oficina del área de sistemas, y deben tomar en cuenta los gastos fijos para el mantenimiento del área de sistemas, tales como energía eléctrica, vigilancia y mantenimientos, entre muchos otros gastos periódicos. En algunos casos también existen gastos, programados o no programados, por la constante actualización del hardware y software y los activos informáticos para mantener vigente la función informática de la organización.

A causa de estos altos costos en los sistemas, en la actualidad las empresas tienen que recurrir a las instituciones y profesionales que proporcionan estos servicios de cómputo (outsourcing informático), con lo cual se liberan no sólo de los altos gastos que implican estas áreas sino también de su administración y del manejo y gasto de personal que las maneja; reduciendo considerablemente las erogaciones por esta actividad informática.

Una variante de este servicio de sistemas es el llamado **HelpDesk** (ayuda de escritorio), mismo que podemos definir de la siguiente manera:

> *Es la prestación del servicio interno de sistemas y del apoyo para la solución de las problemáticas que se les presentan a los usuarios en sus sistemas; este servicio lo presta personal especializado, contratado ex profeso para ello; el cual proporciona los servicios o auxilio informáticos a las áreas de la empresa, a fin de mantener el funcionamiento de los sistemas de la institución; por lo general, dicho servicio se presta por medio de la red de cómputo, y la mayoría de servicios se realizan vía telefónica o a través de la propia red.*

Con la auditoría outsourcing en los sistemas computacionales se busca evaluar la eficiencia y eficacia de los servicios que se proporcionan a las organizaciones, enfocándolos principalmente desde dos puntos de vista: por un lado, aquel en el cual se auditan las actividades, funciones y operaciones del prestador de servicios, en cuanto a la administración de sus recursos informáticos, la confiabilidad, oportunidad y eficiencia con las que trata la información de las organizaciones, los resultados que obtiene del procesamiento de datos y la eficiencia y eficacia de sus servicios. Por otro lado, aquel en donde se evalúa la forma en que se lleva a cabo la actividad de outsourcing en la empresa que lo proporciona, analizando la calidad, rapidez, oportunidad, confiabilidad, eficacia y eficiencia con las que trabaja para suministrar de una manera adecuada la actividad informática a la institución contratante.

En ambos casos, el auditor de sistemas deberá realizar dicha auditoría a los siguientes aspectos:

- *La infraestructura informática para la prestación de los servicios outsourcing.*

- *La administración adecuada y el control en la prestación del servicio de outsourcing informático.*
- *La eficiencia y eficacia de los sistemas de comunicación entre prestador y contratante de los servicios informáticos.*
- *La confiabilidad, veracidad, integridad, oportunidad, suficiencia y calidad con las que se procesa la información de la empresa que contrata los servicios.*
- *La configuración, composición e integración de los sistemas computacionales para evaluar la capacidad y suficiencia del prestador de los servicios de cómputo.*
- *El mantenimiento preventivo y correctivo de los servicios de cómputo, tanto del prestador como del que los contrata.*

Esta auditoría se realiza para evaluar todo lo relacionado con la prestación de servicios informáticos (outsourcing informático), enfocándola hacia el análisis de los sistemas computacionales que tiene el que proporciona el servicio y también la forma en que lleva a cabo esta actividad. Dicha evaluación se puede realizar en varias formas.

A continuación realizaremos, desde varias perspectivas, un análisis sobre los aspectos que se deben evaluar en la auditoría outsourcing en los sistemas computacionales:

Los servicios prestados por medio de sistemas compartidos son aquellos en los que se tienen sistemas computacionales conectados a una red principal, administrada por el prestador del servicio, en la que se realiza todo la captura, procesamiento, custodia y administración de la información de la empresa contratante; en dicha red también se administra el uso de los sistemas de desarrollo y aplicación; además se proporciona ayuda en línea para resolver cualquier problemática de los usuarios a los que se les proporciona este servicio informático.* Aquí se debe aplicar la auditoría a los sistemas de redes (sección 12.7), analizando los aspectos señalados para las redes, pero enfocándola con especial énfasis a la prestación de servicios.

Cuando se suministran los servicios con equipos individuales, no conectados a la red, éstos se utilizan únicamente para llevar a cabo el procesamiento de la información en la empresa contratante; dichos equipos pueden estar en las instalaciones del receptor del servicio, con el fin de realizar ahí todas las actividades necesarias para la captura, procesamiento de información y emisión de resultados, Para lo cual fue contratado.** Para realizar esta auditoría, es recomendable utilizar los mismos procedimientos señalados para la auditoría al sistema computacional (sección 12.4), eva-

* Los servicios *outsourcing* en sistemas de cómputo se pueden proporcionar mediante sistemas en línea conectados a una red de computadoras administrada por el proveedor; en la que se lleva el control de la captura y procesamiento de información y emisión de resultados; esto hace que las computadoras instaladas en la empresa que recibe el servicio, en este caso terminales de la red, sean consideradas como parte de una red, con los privilegios de acceso, niveles de consulta, contraseñas y demás restricciones que permiten las redes, para así contar con la confiabilidad necesaria para el manejo confidencial de la información de la empresa. También se proporciona la ayuda en línea para solucionar las problemáticas que se les presentan a los usuarios *outsourcing*.

** Este tipo de servicios se utiliza, por lo general, sólo para pequeñas aplicaciones, como la nómina, la contabilidad, cobranzas, enseñanza o cualesquier otras aplicaciones, pero de manera individualizada y, casi siempre, para pequeñas y medianas empresas o áreas especiales que no necesitan grandes aplicaciones.

luando todo lo señalado en ese apartado, además de los puntos que trataremos posteriormente.

En ambos casos, además de esos puntos indicados, la auditoría outsourcing en los sistemas computacionales se tiene que complementar con las evaluaciones que presentamos a continuación.

12.8.1 Auditoría a los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios outsourcing

En esta auditoría se evalúa la eficiencia y eficacia con las que el prestador de servicios proporciona los servicios informáticos a la organización que lo contrató; para realizar esta evaluación se deben tomar en cuenta estos criterios: **si el servicio se proporciona a través de sistemas de redes,** entonces se debe aplicar lo señalado para la auditoría a los sistemas de redes (sección 12.7), analizando los aspectos señalados para las redes, pero enfocando la evaluación en la prestación de servicios informáticos. Pero **si los servicios se prestan con sistemas individuales,** entonces se sugiere utilizar los procedimientos señalados para la auditoría al sistema computacional (sección 12.4), pero adaptándolos para analizar la forma en que terceras personas suministran los servicios informáticos.

Para ambas posibilidades se sugiere aplicar la auditoría que corresponda al tipo de prestación de servicios, junto con los aspectos que complementan la auditoría outsourcing, mismos que presentamos a continuación:

- *Evaluación de la prestación de los servicios outsourcing informáticos.*
  - *Existencia del contrato de servicios outsourcing informáticos, contemplando las clausuras de servicio, seguridad, costos, tipo de servicios y todos los detalles inherentes a la prestación de la actividad informática.*
  - *Análisis de la planeación estratégica del servicio outsourcing, en relación con:*
    - *La administración de la prestación/recepción de servicios outsourcing informáticos.*
    - *El cumplimiento de la misión, visión y objetivo de la actividad outsourcing informática, tanto del prestador de servicios como de quien los contrata.*
    - *La existencia y aplicación de las estrategias, procedimientos y funciones sustantivas para proporcionar el servicio outsourcing informático.*
    - *La existencia, aplicación y seguimiento de las políticas, normas y lineamientos que regulen la actividad informática en la empresa y en el área de sistemas.*
    - *La existencia, difusión, seguimiento y control de la misión, visión, objetivo, políticas, normas, lineamientos y procedimientos para cumplir con la actividad y el servicio outsourcing informáticos en la organización.*

- *Evaluación de las estructuras de organización del área de sistemas del prestador de servicios y de la empresa receptora del servicio outsourcing informático, en cuanto a los siguientes aspectos:*
  - *División funcional (u otro criterio) para el servicio outsourcing informático, tanto del prestador como del receptor del servicio.*
  - *Estructura y perfiles de puestos para el servicio outsourcing informático, tanto del prestador como del receptor del servicio.*
  - *Cumplimiento en las funciones, canales de comunicación (formales e informales), niveles de autoridad y responsabilidad de los puestos para el servicio outsourcing informático en el área de sistemas del prestador del servicio.*
  - *Estructuras para el desarrollo de proyectos, atención a usuarios y operación de las actividades outsourcing informáticas.*
- *Evaluación de la administración de las funciones, actividades, tareas y operaciones del prestador del servicio para cumplir con la actividad outsourcing informática de la empresa contratante.*
  - *Existencia, difusión, cumplimiento y seguimiento de los compromisos, funciones, actividades, tareas y operaciones de la actividad outsourcing informática en el área de sistemas.*
  - *Cumplimiento de los métodos, procedimientos, fundamentos y principios administrativos, así como de manuales e instructivos aplicables a la actividad outsourcing informática por parte del prestador de servicios.*
  - *Evaluación de la dirección del área de prestación/recepción de servicios outsourcing informáticos de la empresa contratante y de la empresa que presta el servicio.*
    - *Análisis del ambiente laboral en la prestación/recepción del servicio outsourcing informático.*
    - *Análisis del estilo de liderazgo, relaciones de trabajo, jerarquías de autoridad y ejercicio de autoridad en la prestación/recepción del servicio outsourcing informático.*
    - *Evaluación del cumplimiento de la responsabilidad en la recepción o en la prestación del servicio outsourcing informático.*
    - *Análisis de la coordinación del personal, usuarios y recursos informáticos del área utilizados para la prestación/recepción del servicio outsourcing informático.*
    - *Evaluar la forma en que se ejerce y se controla la toma de decisiones para la prestación/recepción del servicio outsourcing informático.*
    - *Análisis de la integración de grupos de trabajo para la prestación/recepción del servicio outsourcing informático, así como de las relaciones de comunicación formal (comunicación escrita, verbal, correo electrónico u otras formas de comunicación).*

- *Evaluación de la administración del factor humano del área de sistemas.**
- *Coordinación de las funciones, actividades, tareas y operaciones del personal informático destinado a la prestación/recepción del servicio outsourcing informático.*
- *División de las funciones, actividades y operaciones del factor humano dedicado a la prestación/recepción del servicio outsourcing informático.*
- *Evaluación de la existencia y cumplimiento de los planes y programas de capacitación, adiestramiento y promoción del personal dedicado a la prestación/recepción del servicio outsourcing informático.*
- *Análisis de la rotación y movilidad en el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de los procesos de selección de personal para esta actividad.*
- *Análisis de la remuneración y prestaciones para el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de la motivación para que permanezca y progrese en esta actividad.*
- *Análisis de la integración de grupos de trabajo dedicados a la prestación/recepción del servicio outsourcing informático, así como de la gestión directiva de funcionarios, empleados y usuarios.*
- *Análisis de la asignación y cumplimiento de las funciones y actividades del personal dedicado a la prestación/recepción del servicio outsourcing informático, así como del perfil de puestos de dicho personal.*
- *Análisis de la existencia y aplicación de estudios ergonómicos para el personal y usuarios dedicados a la prestación/recepción del servicio outsourcing informático.*

• *Evaluación de la administración de los recursos informáticos no humanos del área de sistemas*

- *Análisis de la administración del sistema computacional, en relación con el hardware, software y con las instalaciones dedicadas a la prestación/recepción del servicio outsourcing informático.*
- *Análisis de la administración de las telecomunicaciones, bases de datos e información del sistema computacional dedicado a la prestación/recepción del servicio outsourcing informático.*
- *Análisis de la administración del mobiliario, equipo, bienes materiales, consumibles y materiales de oficina utilizados en la prestación/recepción del servicio outsourcing informático, así como del manejo financiero de los bienes informáticos.*
- *Análisis de la administración de las adquisiciones de sistemas computacionales, hardware, software, periféricos, mobiliario, consumibles y demás implementos para la prestación/recepción del servicio outsourcing informático.*

* En la sección 9.5.6. del capítulo 9 determinamos la división natural del personal que labora en el área de sistemas, clasificándolo en: personal del área de sistemas, usuarios, asesores y consultores, proveedores y distribuidores de sistemas. Esto es totalmente aplicable en la evaluación de la prestación del servicio outsourcing informático.

- *Análisis de los planes, programas y presupuestos que afectan a la gestión financiera y contable de sus recursos dedicados a la prestación/recepción del servicio outsourcing informático.*

- *Evaluación de los controles informáticos del área de sistemas dedicada a la prestación/recepción del servicio outsourcing informático.**
  - *Análisis de la aplicación de los controles internos a los servicios outsourcing informáticos.*
    - *Controles internos sobre la organización de la prestación/recepción del servicio outsourcing informáticos.*
    - *Controles internos sobre el desarrollo de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*
    - *Controles internos sobre la operación de los sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*
    - *Controles sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados con el servicio outsourcing informático.*
    - *Controles internos sobre la seguridad en la prestación/recepción del servicio outsourcing informático.*
  - *Evaluación de la existencia, establecimiento y uso de los estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*
    - *Metodologías del análisis y diseño de sistemas dedicados a la prestación-/recepción del servicio outsourcing informático.*
    - *Análisis del uso de software, lenguajes y programas de desarrollo para la programación y codificación de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*
    - *Análisis de la elaboración y seguimiento de pruebas y simulaciones de sistemas, programas y lenguajes de cómputo nuevos dedicados a la prestación/recepción del servicio outsourcing informático, así como el análisis de la liberación e implementación de nuevos sistemas, de la capacitación y adiestramiento del personal y los usuarios del área de sistemas y de la documentación de los sistemas*
    - *Análisis de las adquisiciones de sistemas computacionales, materiales y demás componentes y consumibles dedicados a la prestación/recepción del servicio outsourcing informático.*
  - *Auditoría a la documentación y demás estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*

* En el capítulo 5 de este libro analizamos el control interno informático aplicable en una auditoría a los sistemas computacionales. Además, en el capítulo 4 también analizamos el control informático contable, igualmente aplicable en este tipo de auditoría.

- *Existencia, difusión, préstamo y uso de los manuales de usuarios, manuales técnicos de los sistemas, manuales de capacitación, manuales de operación y bitácoras de nuevos proyectos.*
- *Análisis de la documentación de pruebas y simulaciones de sistemas, de la actualización de manuales e instructivos de sistemas computacionales, manuales de organización, procedimientos, operación y demás documentación normativa del área de sistemas.*

Hemos presentado los conceptos anteriores, de manera muy general, para evaluar la prestación del servicio outsourcing informático; sin embargo, al igual que en los tipos de auditoría anteriores, el responsable de la auditoría debe utilizar los puntos propuestos según sus necesidades y de acuerdo con las características específicas de los servicios outsourcing informáticos proporcionados a los usuarios de la empresa. Asimismo, es potestad del responsable de la auditoría determinar los criterios adecuados para medir la eficacia y eficiencia de esta actividad en la empresa que audita.

12.8.2 Evaluación de la forma en que la empresa contratante recibe el servicio outsourcing

Con la realización de esta auditoría se busca evaluar la calidad, suficiencia, eficiencia y eficacia de la recepción de servicios outsourcing informáticos en la empresa, encauzando la revisión hacia el análisis de los sistemas computacionales con los cuales se proporciona el servicio a los usuarios de la empresa, así como la forma en que se lleva a cabo esta actividad. En dicha evaluación se deben tomar en cuenta los mismos criterios señalados en el tipo de auditoría outsourcing anterior:

Cuando los servicios se proporcionan con equipos individuales, no conectados en red, éstos se utilizan únicamente para llevar a cabo el procesamiento de la información en la empresa receptora; dichos equipos pueden estar en las instalaciones de la empresa contratante del servicio y ahí, en sus instalaciones, es donde se debe realizar la evaluación de todas las actividades que se realizan para la captura de datos, procesamiento de información y emisión de resultados en sistemas computacionales particulares.

Los servicios prestados por medio de sistemas compartidos son aquellos en los que la empresa que proporciona el servicio administra los sistemas computacionales de la empresa contratante por medio de una red principal; en dicha red se realiza toda la captura, procesamiento, custodia y administración de la información de la organización contratante, así como la administración del uso de sus sistemas; además, la empresa contratante recibe ayuda en línea para resolver cualquier problemática de sus usuarios.*

* Recordemos que los servicios *outsourcing* en sistemas computacionales se pueden proporcionar mediante sistemas en línea conectados a una red de computadoras, administrada por el proveedor, en donde se lleva el control de la actividad informática y de la información, con los privilegios de acceso, niveles de consulta, contraseñas y demás restricciones que permiten las redes, para así contar con la confiabilidad necesaria para el manejo confidencial de la información de la empresa contratante. Además, dicha empresa obtiene la ayuda en línea para solucionar las problemáticas de sus usuarios.

Es recomendable aplicar la auditoría que corresponda a cualquiera de los dos tipos de recepción de servicios que tratamos anteriormente, junto con los aspectos que complementan la auditoría outsourcing, mismos que presentamos a continuación:

- *Inventarios de la prestación de servicios outsourcing informáticos.*
  - *Inventarios de los componentes de las redes de cómputo o sistemas individuales de la empresa receptora de los servicios outsourcing informáticos, contemplando dentro de sus instalaciones:*
    - *Inventario de los servidores, terminales, cableados, componentes de la red, medios de comunicación y demás bienes informáticos que integran la red de prestación de servicios outsourcing informáticos instalada en la organización contratante.*
    - *Inventario de la configuración de los sistemas individuales con los que se presta el servicio outsourcing informático en la organización contratante, contemplando en forma particular: los fabricantes, marcas, modelos, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relativos al inventario de estos equipos para recibir el servicio outsourcing informático.*
    - *Inventario del software de desarrollo y de aplicación que está a disponibilidad de los usuarios que reciben el servicio outsourcing informático, a fin de comprobar que se satisfagan las necesidades informáticas de la empresa receptora de dicho servicio.*
    - *Inventario del personal destinado a la recepción de los servicios outsourcing informáticos en la organización receptora, así como del personal informático del prestador de los servicios.*
- *Evaluación de la recepción de los servicios outsourcing informáticos.**
  - *Evaluación de la existencia y cumplimiento del contrato del servicio outsourcing informático, contemplando las clausuras de servicio, seguridad, costos, tipo de servicios y todos los detalles inherentes a la prestación de la actividad informática.*
  - *Análisis de la administración estratégica de la prestación/recepción de los servicios outsourcing informáticos, en relación con:*
- *Evaluación de las estructuras de organización del área de sistemas del prestador de servicios outsourcing informáticos, así como de las de la empresa que contrata dichos servicios, en cuanto a:*

* Para no ser repetitivos en estos conceptos, se deben aplicar los mismos aspectos señalados para la **auditoría a los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de servicios outsourcing** (sección 12.8.1); por esta razón, únicamente se mencionan los principales puntos a considerar; pero enfocados hacia la recepción de los servicios *outsourcing*.

- *Evaluación de la administración de las funciones, actividades, tareas y operaciones del prestador del servicio para cumplir con la actividad outsourcing informática de la empresa contratante.*
  - *Cumplimiento de los métodos, procedimientos, fundamentos y principios administrativos, así como de manuales e instructivos aplicables a la actividad outsourcing informática por parte del prestador de servicios.*
  - *Evaluación de la dirección del área de prestación/recepción de los servicios outsourcing informáticos de la empresa contratante y de la empresa que presta el servicio.*
  - *Auditoría a la administración del factor humano del área de sistemas.**
  - *Coordinación de las funciones, actividades, tareas y operaciones del personal informático destinado a la prestación/recepción del servicio outsourcing informático.*
  - *División de las funciones, actividades y operaciones del factor humano dedicado a la prestación/recepción del servicio outsourcing informático.*
  - *Evaluación de la existencia y cumplimiento de los planes y programas de capacitación, adiestramiento y promoción del personal dedicado a la prestación/recepción del servicio outsourcing informático.*
  - *Análisis de la rotación y movilidad en el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de los procesos de selección de personal para esta actividad.*
  - *Análisis de la remuneración y prestaciones para el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de la motivación para que permanezca y progrese en esta actividad.*
  - *Análisis de la integración de grupos de trabajo dedicados a la prestación/recepción del servicio outsourcing informático, así como de la gestión directiva de funcionarios, empleados y usuarios.*
  - *Análisis de la asignación y cumplimiento de las funciones y actividades del personal dedicado a la prestación/recepción del servicio outsourcing informático, así como del perfil de puestos de dicho personal.*
  - *Análisis de la existencia y aplicación de estudios ergonómicos para el personal y usuarios dedicados a la prestación/recepción del servicio outsourcing informático.*
- *Evaluación de la administración de los recursos informáticos no humanos del área de sistemas.*
  - *Análisis de la administración del sistema computacional, en relación con el hardware, software y con las instalaciones dedicadas a la prestación/recepción del servicio outsourcing informático.*

* En la sección 9.5.6 del capítulo 9 determinamos la división natural del personal que labora en el área de sistemas, clasificándolo en: personal del área de sistemas, usuarios, asesores, consultores, distribuidores y proveedores de sistemas. Esto es totalmente aplicable en la evaluación de la recepción del servicio *outsourcing* informático.

- *Análisis de la administración de las telecomunicaciones, bases de datos e información del sistema computacional dedicado a la prestación/recepción del servicio outsourcing informático.*
- *Análisis de la administración del mobiliario, equipo, bienes materiales, consumibles y materiales de oficina utilizados en la prestación/recepción del servicio outsourcing informático, así como del manejo financiero de los bienes informáticos.*
- *Análisis de la administración de las adquisiciones de sistemas computacionales,* hardware, software, periféricos, mobiliario, consumibles y demás implementos para la prestación/recepción del servicio outsourcing informático.
- *Análisis de los planes, programas y presupuestos que afectan a la gestión financiera y contable de sus recursos dedicados a la prestación/recepción del servicio outsourcing informático.*

• *Auditoría de los controles informáticos del área de sistemas dedicada a la prestación/recepción del servicio outsourcing informático.*

- *Análisis de la aplicación de los controles internos a los servicios outsourcing informáticos.*
- *Evaluación de la existencia, establecimiento y uso de los estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*
- *Auditoría a la documentación y demás estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.*

Hemos presentado estos conceptos, de manera muy general, para evaluar la actividad outsourcing informática; el propósito es indicar los principales aspectos a considerar para auditar lo relacionado con la recepción de servicios outsourcing informáticos en la empresa; sin embargo, al igual que en los tipos de auditoría anteriores, el responsable de la auditoría debe utilizar los puntos propuestos según las necesidades y características específicas de los servicios outsourcing informáticos que reciben los usuarios de la empresa. Asimismo, es potestad del responsable de la auditoría determinar los criterios adecuados medir la eficacia y eficiencia de esta actividad en la empresa que audita.

12.8.3 Evaluación del servicio HelpDesk (ayuda en línea) de la empresa

El servicio HelpDesk está concebido para ayudar a resolver, dentro de la misma empresa, los problemas que se les presentan a los usuarios en el manejo de sus sistemas computacionales; con esta ayuda se abarcan todos los problemas que ocurren durante la actividad informática. Lo mismo desde el simple manejo de los sistemas, tales como no poder prender la computadora, que no enciende la pantalla o no funciona la impresora, hasta la solución a problemáticas más complicadas en el manejo del software institucional, las deficiencias técnicas en la aplicación de los sistemas y el mantenimiento correctivo y preventivo a éstos o a sus aplicaciones informáticas. Lo fundamental de es-

te servicio es que ayuda a corregir cualquier deficiencia en la práctica de la actividad informática de la empresa.

Para que se preste con eficiencia y eficacia el servicio HelpDesk, es indispensable que los equipos de los usuarios estén conectados con la red de servicio, a fin de que, al recibir una llamada de auxilio del usuario, el encargado de solucionar el problema pueda identificar la problemática y, de ser posible, se aboque a la aplicación de rutinas y procedimientos de solución desde su terminal. En la práctica real, casi todos los servicios se solucionan desde una terminal, y son muy pocos los casos en los que el especialista se tiene que desplazar al área física donde está la computadora para resolver ahí el problema. Aunque esto último también es ayuda de escritorio.

La función del auditor es, precisamente, evaluar todos los aspectos relativos a la calidad, rapidez y confiabilidad con la que se proporciona este servicio a los usuarios.

- *Evaluación del soporte técnico, de asistencia y capacitación a los usuarios, así como del mantenimiento de los sistemas y detección de incidencias de problemáticas para la solución a los reportes de los usuarios.**
  - *Análisis de la oportunidad en la atención y solución de las problemáticas reportadas por los usuarios del sistema.*
  - *Evaluación estadística de las incidencias de mayor problemática reportadas, y valoración de los tiempos de solución a esos reportes.*
  - *Análisis de la capacidad de respuesta del personal especializado para solucionar las problemáticas que reportan los usuarios.*
  - *Evaluación de la comunicación en línea entre los usuarios y el servicio HelpDesk, tanto de la comunicación telefónica como en red.*
  - *Evaluación de la eficacia y eficiencia de las formas de comunicación, ya sea telefónica, escrita, vía fax, correo electrónico o cualquier otro medio, entre el prestador del servicio y el usuario solicitante de las ayudas.*
  - *Análisis de las bitácoras de reportes y de servicios, a fin de evaluar.*
    - *La calidad en la atención de las solicitudes de servicios.*
    - *La oportunidad, en días u horas promedio, en que se proporciona el servicio, desde que entra la llamada hasta su solución final.*
    - *La capacitación técnica y psicológica para la atención a los usuarios solicitantes de servicios, aun en caso de desconocimiento del manejo elemental de los sistemas computacionales.*

* Para la práctica de esta auditoría, también se tienen que incluir la evaluación a cada uno de los aspectos señalados para **la auditoría a los *sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios outsourcing*** (sección 12.8.1) y **la evaluación de la forma en que la empresa contratante recibe el servicio outsourcing** (sección 12.8.2); debido a que éstos forman parte sustancial de la evaluación de estos servicios además de los aspectos que ahí se agregan.

- *La frecuencia de las incidencias y problemáticas que reportan los usuarios, evaluando estadísticamente las mayores ocurrencias, sus soluciones y las medidas para evitar que se presenten.*
- *La confiabilidad en la solución a los problemas reportados, en grado de aceptación y porcentaje de soluciones.*

— *Acciones de capacitación para los usuarios, sobre la base de los reportes de incidencias, a fin de evitar la frecuencia de los reportes.*
— *Evaluación de las actividades en línea para la solución de las problemáticas reportadas por los usuarios.*

- *Evaluación de las actividades técnicas para proporcionar asistencia y mantenimiento a los sistemas computacionales.**
  — *Análisis de los objetivos, características, componentes, conectividad y comunicación de la red para la atención en línea HelpDesk y su aplicación en la solución de las problemáticas reportadas por los usuarios del sistema.*
  — *Análisis de las características de configuración de la red, en cuanto a topologías, tipo de red, componentes, protocolos de comunicación, servidores, terminales, instalaciones de comunicación y demás aspectos de la red utilizada para proporcionar la ayuda en línea a los usuarios de dicha red.*
  — *Análisis de los componentes internos, externos y de la arquitectura física y lógica del sistema de red, a fin de evaluar que cuente con los elementos técnicos necesarios para prestar la ayuda en línea a los usuarios del sistema.*
  — *Análisis de la confiabilidad y funcionalidad de los medios de transmisión, medios físicos, instalaciones telefónicas, de datos y de energía eléctrica que se utilizan para mantener la comunicación entre el usuario demandante de auxilio y el prestador de la ayuda en línea.*
  — *Análisis del diseño y funcionamiento de los servidores, estaciones de trabajo, componentes, periféricos, sistemas de instalaciones, protocolos de comunicación y enlace físico de la red, a fin de evaluar la eficiencia de las comunicaciones para la ayuda en línea de los usuarios.*
  — *Análisis del diseño y aplicación del software especializado de atención, solución, desarrollo y aplicación para atender y solucionar las necesidades de cómputo de los usuarios del sistema.*
  — *Análisis de las utilerías, bibliotecas y demás software que se utiliza en la red.*
  — *Análisis de la protección, resguardo, respaldo y custodia de la información de los usuarios que solicitan ayuda en línea, así como el respaldo de dicha in-*

* En esta auditoría se sugiere aplicar los mismos puntos señalados para la **auditoría al sistema computacional** (sección 12.4) y la **auditoría a los sistemas de redes** (sección 12.7), ya que ambos casos se aplican a la prestación de este servicio; dándoles el enfoque de servicios de HelpDesk; también se puede complementar con lo señalado en la **auditoría alrededor de la computadora** (sección 12.5), pero dándole el enfoque de evaluación de servicios *HelpDesk*.

formación, evaluando la ayuda y capacitación proporcionadas a los usuarios para el manejo óptimo de su información.

— *Análisis de la administración y control de la red de servicios en línea, evaluando el cumplimiento de:*

- *La confiabilidad, privilegios, niveles de acceso y contraseñas para ingresar a la red y a las terminales que solicitan ayuda en línea, a fin de mantener la integridad del sistema y proporcionar la atención solicitada en dicha red.*
- *El funcionamiento técnico y operativo de los sistemas de red de ayuda en línea y del software especializado de atención a usuarios y mantenimiento físico.*
- *La seguridad de la red y protección de los activos informáticos de la red de servicios* y de los sistemas computacionales para la atención HelpDesk, a fin de mantenerlos en condiciones óptimas para la prestación de la ayuda en línea a los usuarios.*

12.8.4 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría outsourcing en los sistemas computacionales

Como hemos señalado, en esta auditoría outsourcing en los sistemas computacionales se busca evaluar la eficiencia y eficacia con las que la empresa prestadora de estos servicios proporciona dichos servicios a la empresa que los contrata, enfocándolos a la administración de la actividad de outsourcing; analizando la calidad, rapidez, oportunidad, confiabilidad, eficacia y eficiencia con las que trabaja para administrar la actividad informática y la información de la institución contratante; también, sus recursos informáticos, el manejo, confiabilidad, oportunidad y calidad, el tratamiento de la información y los resultados.

Por esta razón, se recomienda al auditor que practique esta auditoría, que utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro, y que las adapte a los aspectos concretos, de carácter técnico y de servicio, que se requieren para evaluar todo lo señalado en el servicio outsourcing y HelpDesk analizados en esta sección. Claro está, como en los casos anteriores, utilizando estos puntos de acuerdo con su experiencia, conocimientos y habilidades.

Es recomendable que el auditor de sistemas computacionales utilice las siguientes herramientas, siguiendo cada uno de los puntos anotados para la auditoría outsourcing en los sistemas computacionales:

- *El diseño de* **entrevistas** (sección 9.1) **cuestionarios** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas acordes con las necesidades de su eva-*

* En esta parte se recomienda utilizar los puntos señalados en la **auditoría de la seguridad de los sistemas computacionales** (sección 12.6), con las adaptaciones necesarias para evaluar la seguridad de la red de ayuda en línea.

luación sobre la prestación del servicio outsourcing informático y ayuda en línea, sobre la calidad, rapidez, eficiencia, eficacia y confiabilidad de la atención; así como sobre la funcionalidad, configuración e instalaciones física y lógica de la red utilizada para la atención y ayuda a los usuarios; también en la indagatoria de la actualización del sistema, las medidas preventivas y correctivas relacionadas con la prestación de la actividad informática del área de sistemas y de la pronta atención a los problemas relacionados con la actividad informática de la empresa.

- *También puede aplicar dichas herramientas para evaluar la opinión de los usuarios de sistemas, respecto al funcionamiento de la red de servicios, frecuencia de fallas, el tiempo de respuesta y la calidad de la atención, así como sobre la satisfacción de sus necesidades informáticas, la disponibilidad de los sistemas, el manejo de la información de sus áreas y, por último, sobre la administración outsourcing de los sistemas de red de la empresa.*

Además, quizá como una de las primeras acciones de evaluación, el auditor de sistemas también puede utilizar la siguiente herramienta:

- *El levantamiento de* ***inventarios*** (sección 9.5)*, a fin de hacer un recuento de los bienes informáticos destinados al funcionamiento de la red de servicios para atender las necesidades outsourcing y ayuda en línea de las áreas de la empresa contratante, así como de los bienes informáticos que se pueden analizar en el funcionamiento de los sistemas que conforman la red de servicios. Para llevar a cabo esto, es recomendable realizar estos inventarios:*
  - *Inventario de los componentes de las redes de servicio outsourcing o sistemas individuales que cumplan con la prestación de servicios informáticas en la organización, contemplando los servidores, terminales, cableados, componentes y demás bienes informáticos que integran la red, así como los fabricantes, marcas, modelos procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con dicho inventario.*
  - *Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias pirata, a fin de valorar la prestación de los servicios informáticos y la ayuda en línea con estos sistemas.*
  - *Inventario de la seguridad y protección de la información y datos del sistema de red de servicios, a fin de evaluar la confiabilidad en el manejo de los recursos informáticos de la empresa que presta los servicios informáticos y la ayuda en línea.*
  - *Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, para valorar su protección y uso adecuados.*

— *Inventario de los medios, privilegios, niveles y métodos de acceso a los sistemas de los usuarios en línea, a fin de valorar la confiabilidad en el acceso a su información y a los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o de los equipos mayores en red.*

— *Inventario de las instalaciones físicas de las áreas que reciben y proporcionan los servicios outsourcing y ayuda en línea, a fin de evaluar la calidad, confiabilidad, control y vigilancia del uso de los bienes informáticos en las actividades outsourcing informáticas y ayuda en línea.*

— *Inventario de las configuraciones, protocolos, tarjetas y demás tecnología utilizada para el funcionamiento de los sistemas de red de servicios outsourcing y ayuda en línea, así como de los sistemas individuales de servicios.*

— *Inventarios de las normas, políticas, reglamentos, medidas preventivas y correctivas del área de sistemas, a fin de evaluar la satisfacción de las necesidades de servicios outsourcing informáticos y ayuda en línea de la empresa.*

— *Otros inventarios relacionados con la prestación/recepción de los servicios outsourcing informáticos y ayuda en línea (HelpDesk) para los usuarios de sistemas de la empresa.*

Es indispensable que el responsable de esta auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría a los sistemas de redes utilizados para brindar el servicio outsourcing informático:

- *La elaboración de una* **guía de evaluación** (sección 11.1), *a fin de planear específicamente cada uno los aspectos importantes del funcionamiento de las redes que tiene que evaluar, tanto en lo técnico, como en la configuración, operación, compatibilidad, comunicación y demás aspectos relacionados con el funcionamiento de la red. Para ello es recomendable que tome en cuenta cada uno de los puntos indicados en el inicio de esta sección, adaptándolos a las necesidades específicas de la red en la empresa, e incluso modificándolos para adecuarlos conforme a sus propias necesidades de evaluación, y conforme a las características propias del sistema de red, a su tamaño, componentes, configuración y demás peculiaridades de la red.*

Otras herramientas que es recomendable utilizar en estas auditorías son las siguientes:

- *Las técnicas de* **observación** (sección 9.4)*, a fin de evaluar el funcionamiento del sistema operativo de la red de servicios, así como el procesamiento de la información y el uso del software institucional, para comprobar la calidad, confiabilidad, oportunidad, eficacia y eficiencia de los servicios outsourcing informáticos y la ayuda en línea proporcionados a los usuarios, ya sea por medio de sistemas individuales o con las redes de servicios. Asimismo, cuando el caso lo requiera, el*

auditor podrá realizar la observación oculta, participativa, el monitoreo y los demás tipos de observación descritos en esa sección.

- *Las técnicas de* **revisión documental** (sección 10.5) *para revisar la prestación del servicio outsourcing informático y la eficiencia de la atención en línea, mediante el análisis de los documentos que avalen el tipo de servicios que se deben recibir/proporcionar, los proyectos de instalación de la red de servicios, de configuración y distribución de los componentes de la red, así como para evaluar los planes de atención a contingencias, los manuales e instructivos de seguridad, las licencias y resguardos de sistemas, bitácoras de reportes de incidencias de atención a los servicios solicitados y acciones de mantenimiento. con esta técnica también se puede hacer el análisis de los planes, programas y presupuestos para valorar la satisfacción de los requerimientos de operación y funcionalidad de la actividad informática contratada. Obviamente, esta revisión se debe hacer para evaluar lo que se refiera a la administración y control de los servicios outsourcing informáticos y la ayuda en línea que integran la prestación/recepción de estos servicios.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** (sección 10.8), *según las preferencias y necesidades de revisión del auditor; con estas herramientas puede analizar las fortalezas y debilidades del servicio outsourcing informático, tales como la administración del servicio, la calidad en la atención a los usuarios y las ventajas y desventajas de dicho servicio en la empresa; asimismo, puede evaluar las fortalezas y debilidades en el manejo de los sistemas a través de terceros, el manejo de software e información, el mejor aprovechamiento de la cobertura de necesidades informáticas de la empresa y la respuesta a las solicitudes de servicios outsourcing informáticos y de ayuda en línea para los usuarios.*
  También puede analizar las áreas de oportunidad para fortalecer la función de comunicación entre los sistemas de la empresa que proporciona el servicio outsourcing y la ayuda en línea y los usuarios de la empresa que los recibe, evaluando las amenazas y fortalezas de la actualización en las tecnologías de servicio, las necesidades de áreas internas de cómputo, los costos de la actividad informática, así como el avance de la tecnología de redes y comunicación para evitar la fragilidad en la actualización de la actividad informática de la institución que recibe los servicios.

Un buen elemento de control para el responsable de esta evaluación es el siguiente:

- *El uso de la* **lista de chequeo** (sección 11.6) *es muy importante, ya que, con esta herramienta, se puede verificar que quien realice la auditoría cubra todos los puntos descritos en su planeación de auditoría. Inclusive, de acuerdo con el diseño de esta lista de chequeo, también puede auditar todos los aspectos que repercuten en la prestación de los servicios outsourcing informáticos y en la ayuda en línea.*

- *El uso de las técnicas de* **muestreo** (sección 9.6), *debido a que sería casi imposible, a la vez que inoperante, revisar todas las actividades que se llevan a cabo para el cumplimiento de las funciones, tareas y operaciones de la prestación/recepción del servicio outsourcing y la ayuda en línea, más si éstos se realizan mediante una red de servicios, y ésta es WAN o Internet. Por esta razón, al practicar el levantamiento de información, el auditor tiene que utilizar muestras representativas para evaluar el cumplimiento de las necesidades de los usuarios del servicio outsourcing informático, de acuerdo con las necesidades y características de la prestación/recepción adoptadas en la empresa, sus componentes y la magnitud de servicios y en la transmisión en línea.*

El responsable de la auditoría puede utilizar la siguiente herramienta para evaluar las funciones de los ejecutivos, empleados y usuarios de sistemas, así como el desempeño de todo lo que está alrededor del funcionamiento de una red de cómputo utilizada para la prestación de servicios outsourcing informáticos:

- *La* **ponderación** (sección 11.2) *es una de las herramientas más útiles , ya que le permite evaluar el funcionamiento adecuado de cada una de las partes en que se dividió esta auditoría, dándole a cada una de esas partes un peso ponderado que, según su criterio, le corresponda. Por ejemplo: un peso x para evaluar al prestador del servicio, otro para el que recibe el servicio y otro más para la ayuda en línea. Estos pesos ponderados se asignan de acuerdo con un criterio de evaluación para hacer más equitativa la revisión de la actividad outsourcing. Debemos señalar que es potestad absoluta del auditor establecer la división que más convenga a sus requerimientos de evaluación.*
  Recordemos que con esta técnica es posible darle un peso específico a cada una de las partes en que se divide la actividad de las redes, y que la ponderación se tiene que adoptar de cada una de las subsecciones que conforman este subcapítulo.

Otras herramientas que pueden ser de mucha utilidad para evaluar el servicio outsourcing, tanto en las empresas que lo proporcionan como en las que lo reciben, son las siguientes:

- *Los* **modelos de simulación** (sección 11.3), *ya que con ellos es posible hacer simulacros sobre la prestación de los servicios outsourcing proporcionados a los usuarios de sistemas de la empresa que los contrata, en este caso mediante el desarrollo de pruebas simuladas, planeadas previamente, en las que el auditor hace mal uso del servicio outsourcing y de la ayuda en línea. Esto se evalúa a través de acciones premeditadas, donde el auditor realiza actividades concretas para analizar el funcionamiento de la actividad informática que se ofrece a los usuarios outsourcing, a la atención de sus necesidades informáticas o solicitudes de ayuda en línea; se pueden hacer tantas pruebas como sean necesarias;*

ya sea para mal usar la actividad outsourcing y de ayuda en línea*, para analizar su comportamiento y cumplimiento, o bien,* realizar todo tipo de simulaciones, *de acuerdo con las necesidades de evaluación y experiencia del auditor, lo cual le permitirá medir el grado de cumplimiento y satisfacción de las actividades informáticas para el servicio de los usuarios de la empresa.*

- *El* **análisis de la diagramación de sistemas** (sección 11.7), *el cual también puede ser una herramienta valiosa para el auditor, ya que le permite hacer el seguimiento de cualquier actividad de captura, procesamiento de información y emisión de resultados en los sistemas outsourcing y ayuda en línea, a fin de evaluar si el flujo de los servicios es acorde con las necesidades de los usuarios. También puede hacer el seguimiento de las rutinas de los programas de atención a los usuarios y la prestación de los servicios informáticos; incluso le sirve para evaluar que los flujos de comunicación que se utilizan en la transmisión/recepción de la información y de los servicios que integran la actividad outsourcing y ayuda en línea sean acordes con las actividades y funciones que contrató la empresa.*

El responsable de la auditoría debe tomar las sugerencias anteriores sobre los aspectos que se pueden evaluar mediante la auditoría outsourcing en los sistemas computacionales de acuerdo con sus necesidades específicas de evaluación, ya que es su facultad absoluta utilizarlas como están, adaptarlas e inclusive sustituirlas por aquellos puntos concretos que le ayuden a realizar mejor su auditoría. También debe utilizar las técnicas, métodos y procedimientos de auditoría que le agraden o que conozca más.

12.9 Auditoría ISO-9000 a los sistemas computacionales

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la revisión exhaustiva, sistemática y especializada que realizan únicamente los auditores especializados y certificados en las normas y procedimientos ISO-9000, aplicando en forma exclusiva los lineamientos, procedimientos e instrumentos establecidos por esta asociación. El propósito fundamental de esta revisión es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa se apegue a los requerimientos del ISO-9000.*

Es la evaluación de la calidad de los sistemas computacionales, de acuerdo con los estándares y requerimientos de las normas ISO-9000, a fin de obtener la certificación de los sistemas de la organización.

Por lo general, esta auditoría ISO-9000 es de carácter externo y tiene que ser practicada por algún despacho reconocido y autorizado para otorgar la certificación ISO-9001, ISO-9004 o la más reciente, que es la ISO-14000, aplicables según los criterios de certificación a los sistemas de cómputo. Cuando un auditor de sistemas que no es-

tá certificado como auditor ISO-9000 realiza la auditoría, entonces se considera como auditoría interna de sistemas y no tendrá validez para obtener alguna certificación de calidad. Para obtener su certificación de calidad es necesario recurrir a los auditores ISO-9000, certificados.*

Los fundamentos de la calidad ISO-9000 se pueden resumir en tres acciones fundamentales:

- *Documentar lo que se hace.*
- *Realizar lo que se está documentado.*
- *Revisar lo que se hace con lo documentado.*

Casi no existen normas específicas que se puedan aplicar expresamente a la certificación de los sistemas computacionales; tal es el caso de la norma ISO-9004, la cual se puede aplicar a los sistemas computacionales utilizando los ***elementos de administración*** y ***sistemas de calidad*** en sus cuatro partes:[4]

- *Parte 1. Guías*
- *Parte 2. Guías para servicios*
- *Parte 3. Guías para materiales procesados*
- *Parte 4. Guías para mejoramiento de la calidad*

Por otro lado, también se utiliza la norma ISO-9001, ya que se puede aplicar bajo el enfoque del modelo cliente-servidor en una fábrica de software a la medida, debido a que este modelo representa a cualquier empresa que ofrece sus productos (en este caso software) a sus clientes como resultado de todos los procesos que se siguen para realizar dicho software.[5]

Bajo este enfoque, se pueden aplicar las 20 secciones de esta norma, con sus características específicas de aplicación.

Para el enfoque de auditoría ISO-9000 que pretendemos mostrar en esta parte, aceptaremos como válidos ambos criterios, a fin aplicar esos elementos a la auditoría ISO-9000 a los sistemas computacionales; también debemos señalar que es responsabilidad del auditor vigilar que se cumpla con los puntos indicados en las guías establecidas en la norma ISO-9004 o con los criterios señalados en la norma ISO-9001.

Además, el cumplimiento tanto de las acciones como de los aspectos señalados en las guías de la norma ISO-9004 y en la norma ISO-9001, se verifica a través de los criterios de las normas fundamentales, las cuales se listan en la siguiente tabla; también se anotan las normas ISO-9002 e ISO 9003, para tener el panorama completo de estos criterios.

* El tratamiento de este punto se refiere exclusivamente a la calidad ISO-9000; sin embargo, los mismos conceptos, procedimientos, aplicaciones y sugerencias para realizar este tipo de auditoría, también pueden hacerse extensivos a las nuevas corrientes de certificación de calidad que se están exigiendo a las empresas de hoy. Algunos ejemplos: NOM (Normas Mexicanas de Calidad), TQS (Sistemas de Calidad Total).

Criterio de la norma ISO-9000*	ISO-9001	ISO-9002	ISO-9003	ISO-9004
• Responsabilidad administrativa	Sí	Sí	Sí	Sí
• Sistemas de calidad	Sí	Sí	Sí	Sí
• Revisión del contrato	Sí	Sí	Sí	
• Control de diseño de proyectos	Sí	Sí		
• Control de documentos e información	Sí	Sí	Sí	Sí
• Control de compras (adquisiciones)	Sí	Sí	Sí	
• Control de productos suministrados por el cliente	Sí	Sí	Sí	
• Identificación del producto y posibilidad de seguimiento	Sí	Sí	Sí	Sí
• Rastreabilidad	Sí	Sí	Sí	
• Control de procesos	Sí	Sí	Sí	
• Inspecciones y pruebas	Sí	Sí	Sí	Sí
• Control de inspecciones, equipos de mediciones y prueba	Sí	Sí	Sí	Sí
• Estado de inspección y prueba	Sí	Sí	Sí	Sí
• Control de productos que no llenan requisitos	Sí	Sí	Sí	Sí
• Acciones correctivas y preventivas	Sí	Sí	Sí	
• Manejo, almacenamiento, embalaje, preservación y envío	Sí	Sí	Sí	Sí
• Control de registros de calidad	Sí	Sí	Sí	Sí
• Auditorías internas de calidad	Sí	Sí	Sí	Sí
• Programas de capacitación	Sí	Sí	Sí	Sí
• Control de servicios al cliente	Sí	Sí	Sí	Sí
• Técnicas estadísticas	Sí	Sí	Sí	Sí
• Costo de la calidad	Sí			

El auditor de sistemas que aplica la auditoría de calidad ISO-9000 a los sistemas computacionales debe vigilar que se cumplan estos criterios; además debe verificar el cumplimiento de los puntos señalados en las guías de la norma ISO-9004 y los de la norma ISO-9901.

Cabe aclarar que la presentación de esta *auditoría de calidad ISO-9000 a los sistemas computacionales* no pretende sustituir ni modificar los lineamientos de la ***auditoría de certificación ISO-9000***, sino que el propósito es mostrar al auditor de sistemas los elementos que le ayudarán a complementar la práctica de una auditoría de sistemas

* Este articulista de Soluciones avanzadas. ISO-9000, *Eduardo Cadena Gómez*, , aporta 22 criterios, mientras que los demás autores del tema aportan sólo 20 de ellos, ya que muchos consideran que los puntos **9, Rastreabilidad,** y **10, Control de procesos**, son uno solo; además agrega el **22, Costo de la calidad.**

computacionales, a fin de hacer más completa la revisión, ya que en esta auditoría bien podría aplicar las Normas Mexicanas de Calidad, o también las normas señaladas por System Quality. En todos los casos, el propósito es ayudar a satisfacer los requisitos para la aplicación de esas normas de calidad; aunque en algunos casos, sí podría coadyuvar a la obtención de una certificación a los sistemas, bajo la auditoría específica de las normas ISO-9000 y la certificación de un auditor autorizado para ello.

En consideración a ello, se sugiere utilizar los siguientes puntos:

- *Evaluación del cumplimiento de los requisitos de la norma ISO-9004.**
  - *Analizar el grado de cumplimiento de los criterios de la norma ISO-9004, a fin de evaluar si el cumplimiento es acorde con los requisitos establecidos para obtener la certificación ISO-9000.*
  - *Analizar si las pruebas de certificación ISO-9000 se realizan conforme con los requisitos señalados en las guías de criterios de esas normas.*
  - *Analizar si se cumple con la documentación de las actividades de sistemas y cómo se acatan los elementos fundamentales de las normas ISO-9000 en ese renglón:*
    - *La existencia y actualización de la documentación de las actividades informáticas que se realizan en las áreas de sistemas de la organización.*
    - *Que estén documentados los desarrollos de sistemas que se han realizado dentro de la institución.*
    - *La existencia de la documentación completa y necesaria del software de desarrollo, de aplicación y utilerías adquiridos para el área de sistemas.*
    - *La existencia de manuales e instructivos de organización, operación, flujo de información y todos los demás documentos que señalen las actividades de sistemas en la empresa.*
    - *La existencia y uso de documentación de estándares y metodologías para el desarrollo de proyectos informáticos*
  - *Analizar si las actividades informáticas se cumplen conforme están establecidas en la documentación de actividades de sistemas, de acuerdo con los lineamientos fundamentales de las normas ISO-9000:*
    - *Comprobar que las acciones informáticas se estén realizando conforme se describe en la documentación de esas actividades.*
    - *Evaluar el grado de cumplimiento de las actividades, conforme a lo descrito en la documentación de actividades del centro de cómputo.*

* Para complementar esta auditoría, sería de mucha utilidad que el auditor utilizara los aspectos señalados en la **auditoría sin la computadora** (sección 12.2), la **auditoría a la gestión informática del área de sistemas** (sección 12.3) y la **auditoría alrededor de la computadora** (sección 12.5), ya que estas auditorías están muy relacionadas con lo que se busca evaluar con la auditoría ISO-9000.

- *Evaluar que los sistemas desarrollados o adquiridos para el área de sistemas cuenten con la documentación y manuales de usuarios, de operaciones, de flujo de actividades y demás documentación donde se pueda validar el cumplimiento de sus actividades.*

— *Analizar que se verifique el cumplimiento de las actividades de sistemas, conforme se documentaron en los manuales, instructivos y demás documentación relacionada con dichas actividades, y conforme a los señalamientos fundamentales de las normas ISO-9000.*

— *Verificar que se cumpla con las 20 secciones establecidas para las normas ISO-9000, de acuerdo con el criterio de certificación que se utilice, ya sea ISO-9001 o ISO-9004.*

— *Analizar que en la empresa se cuente con la infraestructura técnica, de servicios y de organización que soporten la implementación de los sistemas de calidad ISO-9000, a través del establecimiento de los siguientes aspectos en el área de sistemas:*

- *Verificar la existencia de los procedimientos, responsabilidades y recursos necesarios para que los sistemas computacionales de la empresa cumplan con estos sistemas de calidad.*
- *Verificar que se conozcan y se apliquen los objetivos y políticas de calidad ISO-9000 a los sistemas computacionales de la empresa.*
- *Verificar que existan los manuales de calidad ISO-9000, los procedimientos para la aplicación de la calidad y la capacitación necesaria para sujetarse a la precertificación de las normas ISO-9000.*
- *Verificar que existan las actividades necesarias, de directivos, ejecutivos y empleados de la empresa y del área de sistemas, a fin de cumplir con los requerimientos para el aseguramiento de la calidad en los sistemas computacionales.*
- *Verificar la existencia, aplicación y cumplimiento del plan de calidad para la certificación de los sistemas computacionales de la organización.*
- *Revisar que se cumpla con las normas, políticas, lineamientos y secuencia de actividades para la certificación de la calidad ISO-9000 de los sistemas computacionales de la empresa.*
- *Verificar la existencia y aprovechamiento de los recursos informáticos empleados para contribuir a la certificación de sistemas ISO-9000, tanto del personal del área de sistemas como del personal ajeno a ésta, y de los recursos no humanos necesarios para evaluar la calidad.*

• *Auditoría de los costos de certificación ISO-9000.**

* Aquí se recomienda realizar una auditoría de carácter contable, a fin de evaluar los gastos hechos para la certificación ISO-9000, o una auditoría a la gestión informática, con especial énfasis en dichos gastos.

- *Evaluación del seguimiento de la certificación ISO-9000.*
  - *Evaluar si los resultados de la certificación ISO-9000 son acordes con lo esperado, y su repercusión en el cumplimiento de las actividades informáticas de la empresa, así como su aprovechamiento en dichas actividades.*
  - *Analizar las acciones seguidas después de la certificación ISO-9000, y determinar si se obtuvieron mejoras en el servicio de cómputo para las áreas de la empresa.*
  - *Valorar las opiniones de los usuarios de sistemas respecto a la aprobación o desaprobación de la certificación ISO-9000 para los sistemas computacionales de la empresa, así como sus opiniones sobre la calidad de los sistemas.*
  - *Hacer el seguimiento de las actividades, actualizaciones y cambios que se presentan en el área de sistemas, a fin de evaluar su apego a los requisitos de la norma ISO-9000.*
  - *Analizar la custodia y almacenamiento de la documentación utilizada en la certificación ISO-9000, y si los usuarios utilizan dicha documentación después de obtenida la certificación.*

Auditoría para la certificación de calidad ISO-9000*

12.9.1 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría ISO-9000 a los sistemas computacionales

Esta auditoría tiene aspectos muy específicos que la hacen diferente de las demás auditorías de sistemas, debido a que cuenta con características peculiares de aplicación, todas ellas enfocadas a la certificación ISO-9000. Especialmente porque las personas que aplican la auditoría de certificación de calidad ya tienen definidas las herramientas, técnicas y procedimientos especiales, mismos que utilizan sin ninguna variación, porque ya están normados para la certificación de calidad.

En consideración a lo anterior, se omiten las herramientas, técnicas y procedimientos establecidos para la auditoría de certificación de calidad ISO-9000, y únicamente se ponen a consideración del lector las herramientas que se pueden utilizar para evaluar los demás aspectos señalados para este tipo de auditorías.

Por esa razón se recomienda al auditor que, siguiendo cada uno de los puntos anotados para la evaluación de todo lo que rodea a la auditoría ISO-9000 a los sistemas computacionales, utilice cualquiera de las herramientas señaladas en los capítulos 9, 10 y 11 de este libro.

* Solamente mencionaremos, de manera muy general, las normas, técnicas, procedimientos y herramientas de la auditoría para la certificación ISO-9000, debido a que dicha auditoría es muy especializada y sólo la pueden aplicar auditores certificados y autorizados para llevar a cabo este tipo de evaluaciones. Para conocer las normas y políticas para el uso de las herramientas de auditoría ISO-9000, le sugerimos contactar a los institutos de certificación de calidad ISO-9000.

- *El diseño de* **entrevistas** (sección 9.1) **cuestionarios** (sección 9.2) *y* **encuestas** (sección 9.3) *elaborados con preguntas para valorar el cumplimiento de los requisitos de calidad ISO-9000, y para valorar la aceptación, rechazo o indiferencia hacia la aplicación de las normas de calidad ISO-9000, así como para verificar que las actividades informáticas se realicen conforme están documentadas.*
  Estas herramientas se pueden utilizar también para conocer la opinión de los usuarios de sistemas respecto a la aplicabilidad y funcionamiento de esta certificación de calidad, así como sobre su aprovechamiento y sus ventajas y desventajas.

Además, quizá como una de las primeras acciones de evaluación de la calidad ISO-9000, el auditor de sistemas también puede utilizar la siguiente herramienta:

- *El levantamiento de* ***inventarios*** (sección 9.5), *a fin de hacer un recuento de los bienes informáticos destinados a la certificación ISO-9000 y de la documentación de actividades, sistemas y procedimientos para cumplir con la función informática de la organización.*
  - *Inventario de los componentes de las redes de servicio o sistemas individuales que puedan cumplir con la certificación de calidad ISO-9000; en este inventario se deben contemplar los servidores, terminales, cableados, componentes y demás bienes informáticos que integran la red, así como a los fabricantes, marcas, modelos procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo, etcétera.*
  - *Inventario de la documentación de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, a fin de valorar el cumplimiento de las normas ISO-9000.*
  - *Inventario de la documentación de normas, políticas, reglamentos, medidas preventivas y correctivas del área de sistemas, a fin de evaluar la satisfacción de los requisitos de las normas ISO-9000.*
  - *Otros inventarios relacionados con la documentación de actividades para la certificación de los servicios informáticos de la empresa.*

Debido a que se tiene que cumplir con un plan de certificación ISO-9000, es indispensable que el responsable de la auditoría tome en cuenta lo siguiente al elaborar su programa de auditoría:

- *La elaboración de una* **guía de evaluación** (sección 11.1), *a fin de planear específicamente cada uno de los aspectos importantes del funcionamiento de las actividades y secuencia de pasos de la auditoría ISO-9000. Para ello es recomendable que tome en cuenta los procedimientos, herramientas y técni-*

cas para la certificación de calidad, así como cada uno de los puntos indicados en el inicio de esta sección, adaptándolos a las necesidades específicas de la certificación de calidad a los sistemas computacionales de la empresa, e incluso modificándolos de acuerdo con sus necesidades de evaluación.

Otras herramientas que es recomendable utilizar en estas auditorías son las siguientes:

- *Las técnicas de* **observación** (sección 9.4) *a fin de verificar que los servicios de cómputo se otorguen conforme con lo documentado, así como para verificar que el desarrollo de las operaciones y actividades de servicios de cómputo sí satisfagan los requisitos demandados por la auditoría ISO-9000. Además, cuando el caso lo requiera, el auditor podrá realizar la observación oculta, participativa, el monitoreo y los demás tipos de observación descritos en esa sección.*
- *Las técnicas de* **revisión documental** *(*sección 10.5*) para revisar la documentación de los servicios y actividades y los demás documentos relacionados con la función informática de los sistemas de la empresa, así como para revisar el cumplimiento de los requisitos, normas, procedimientos relacionados con la certificación ISO-9000.*
- *La* **matriz de evaluación** (sección 10.7) *o la* **matriz DOFA** (sección 10.8), *según las preferencias y necesidades de revisión del auditor; con estas herramientas puede analizar las fortalezas y debilidades de la certificación de calidad ISO-9000, así como las áreas de oportunidad para fortalecer la calidad de los sistemas de la empresa. También puede evaluar las debilidades, fortalezas, amenazas y áreas de oportunidad de la actualización de esta certificación, de las nuevas tecnologías de servicio, así como las necesidades de las áreas de cómputo, los costos de la actividad informática, el avance de la tecnología de redes y la comunicación para evitar la fragilidad en la actualización de la actividad informática de la institución.*

Un elemento de control para el responsable de esta evaluación de la calidad es el siguiente:

- *El uso de la* **lista de chequeo** (sección 11.6), *ya que con esta herramienta puede verificar el cumplimiento de todos los criterios de evaluación contemplados para la planeación de la auditoría de las normas ISO-9000.* Además, esta herramienta le ayuda a verificar que quien realice la auditoría cubra todos los puntos descritos. Inclusive, de acuerdo con el diseño de esta lista de chequeo, puede evaluar todos los aspectos que repercuten en el cumplimiento de las actividades, requisitos y criterios de la calidad ISO-9000.*

* La tabla de criterios de las normas ISO-9000 es un claro ejemplo de la aplicación de la técnica de lista de chequeo; lo que tiene que hacer el auditor es verificar el cumplimiento de cada uno de los criterios ahí plasmados.

Otra herramienta que puede ser de mucha utilidad en esta evaluación es la siguiente:

- *Los* **modelos de simulación** (sección 11.3), *ya que con ellos es posible hacer las pruebas necesarias de la calidad, documentación y del cumplimiento en la empresa de los requerimientos de la norma ISO-9000 para los servicios de sistemas; en estas pruebas simuladas, planeadas previamente, el auditor, a través de acciones premeditadas, hace mal uso de las actividades documentadas, pudiendo hacer las pruebas tantas veces como sean necesarias con el fin de analizar su comportamiento y cumplimiento para medir, con la mayor veracidad posible, el grado de cumplimiento y satisfacción de los requisitos de la certificación de calidad ISO-9000.*

El responsable de la auditoría debe tomar las sugerencias anteriores sobre los aspectos que se pueden evaluar mediante la auditoría de calidad ISO-9000 a los sistemas computacionales, de acuerdo con sus necesidades específicas de evaluación, ya que es su facultad absoluta utilizar las normas ISO-9000, o bien utilizar estas sugerencias. También debe utilizar las técnicas, métodos y procedimientos de auditoría que le agraden o que conozca más.

12.10 Auditoría ergonómica de los centros de cómputo

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la revisión técnica, específica y especializada que se realiza para evaluar la calidad, eficiencia y utilidad del entorno, hombre, máquina y medio ambiente que rodean el uso de los sistemas computacionales en una empresa. Esta revisión se realiza también con el propósito de evaluar la adquisición y el uso correctos del mobiliario, equipo y sistemas, a fin de proporcionar el bienestar, confort y la comodidad que requieren los usuarios de los sistemas computacionales de la empresa, así como para evaluar la detección de los posibles problemas y sus repercusiones, y la determinación de las soluciones relacionadas con la salud física y el bienestar de los usuarios de los sistemas de la empresa.*

La ergonomía, palabra compuesta por ***ergon***, trabajo, y ***nomos***, leyes, es la ciencia que se encarga de estudiar el bienestar, confort, la comodidad y seguridad de los trabajadores dentro de su ambiente laboral, considerando en este estudio el entorno profesional y el impacto que tienen las herramientas y los instrumentos de trabajo en el desempeño de las actividades. También se analiza el impacto del trabajo en la salud física y emocional de los trabajadores, a fin de proponer medidas preventivas y correctivas que permitan desarrollar el trabajo en las mejores condiciones.

Esta ciencia se define de la siguiente manera:

La ergonomía, la ciencia del trabajo, es un campo de la tecnología que considera las limitaciones y capacidades humanas en el diseño de máquinas y objetos que usan las personas, los procesos de trabajo que deben de seguir y los ambientes en que operan.[6]

Aplicada al ámbito de las computadoras, la ergonomía es una ciencia moderna que se encarga de estudiar estudiar todo lo relacionado con la comodidad, bienestar y seguridad de los usuarios de los sistemas computacionales. Además permite analizar la influencia y repercusiones de dichos sistemas y del ambiente laboral en la salud de los usuarios, así como en su productividad.

Para iniciar el planteamiento de la auditoría ergonómica de los centros de cómputo, conviene tomar como punto de partida una división de los aspectos fundamentales de la ergonomía, esto es, el efecto del uso de computadoras en la salud del individuo, a fin de que el auditor capte los principales problemas que debe analizar en este renglón. Dicha división es la siguiente:

El sistema visual: el estudio de los efectos del trabajo en los ojos y la visión en general; asimismo, el estudio de la iluminación, las luminarias y los deslumbramientos.

El sistema muscular-esquelético: el estudio de la afectación del trabajo en el tronco, tórax, cuello, cabeza, columna vertebral, espalda, brazos, manos, dedos, piernas y pies del individuo, en las **posturas que adoptan los usuarios:** debido al mobiliario, las herramientas y la computadora.

El ambiente laboral del centro de cómputo; concretamente, el mobiliario, equipo, la iluminación, el aire acondicionado y los demás elementos del área de trabajo.

Se supone que los anteriores son los factores que más influyen en los problemas relacionados con la salud de los usuarios de sistemas computacionales. Por ello, el auditor de sistemas debe realizar el análisis a partir de esta división fundamental. En estos aspectos es donde se supone mayor incidencia de este tipo de problemática, por lo que es allí donde debe enfocar su auditoría. Por lo tanto, analizaremos el impacto en la salud de los usuarios tomando en cuenta los siguientes factores:

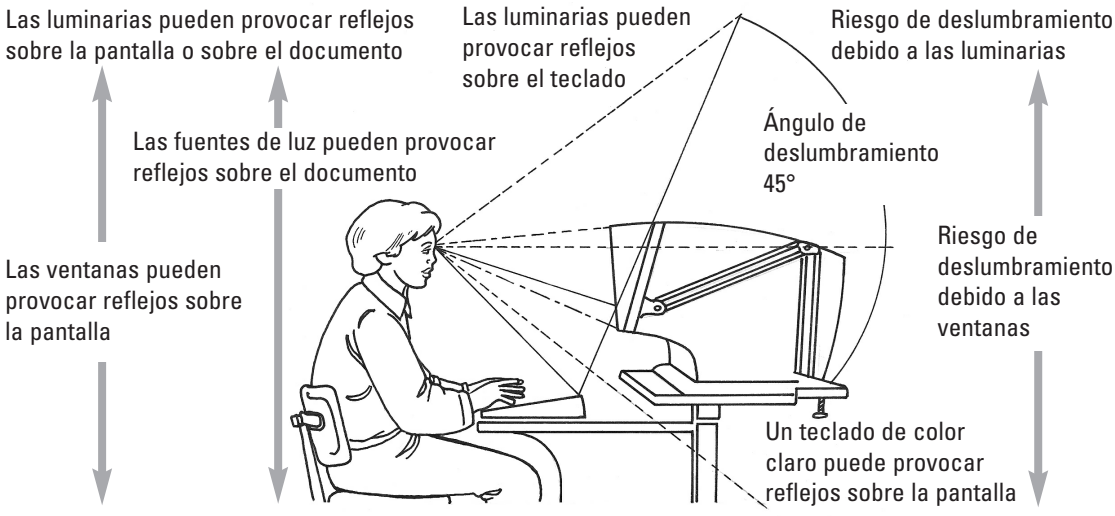
- *Las repercusiones de los sistemas en la salud visual de los usuarios.*
- *Las repercusiones en los músculos y huesos de brazos, manos y dedos.*
- *Las repercusiones en los músculos y huesos de la espalda, tronco, tórax, cuello, cabeza y columna vertebral.*
- *Las repercusiones del ambiente del área de sistemas en la salud del usuario.*
- *Las consecuencias del diseño e instalación del área de sistemas en la salud física y emocional de los usuarios, así como su impacto en la actividad informática de la organización.*

- *El impacto del diseño ergonómico (o de la falta de éste) en el desempeño del trabajo y en el bienestar de los usuarios, así como en su comodidad durante su estancia en el área de sistemas.*
- *La atención (o desatención) que los directivos, empleados y usuarios del área de sistemas de la empresa ponen para el estudio de esta problemática.*
- *La afectación de los estudios ergonómicos (o carencia de ellos) en el diseño de los centros de cómputo, en el mobiliario y equipo destinado a los usuarios.*

A continuación presentaremos gráficas relacionadas con estos puntos, las cuales se explican por sí mismas.

12.10.1 Auditoría de las repercusiones de los sistemas computacionales en la salud visual del usuario

Partiendo del análisis de la siguiente gráfica,[7] podemos observar la afectación de la vista del usuario de sistemas ya que, como se desprende del estudio, se registran ciertos problemas de reflexión o deslumbramiento, los cuales pueden influir en la salud visual de quienes utilizan computadoras como herramientas de trabajo.



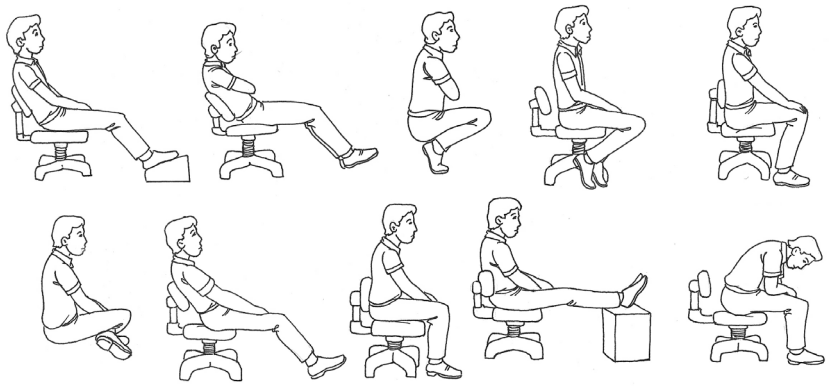
El auditor de sistemas debe tomar en cuenta los riesgos de deslumbramiento ocasionados por las luminarias y fuentes de iluminación que estén sobre la pantalla y los documentos, así como las fuentes de iluminación que emanan de la pantalla. Lo siguiente puede darnos una idea de las serias consecuencias que pueden tener estos aspectos de la iluminación en los usuarios de los sistemas.

- *Analizar si se tienen los estudios de Ergonomía en las actividades de sistemas y cómo se cumple con los elementos fundamentales en este renglón.*

- *Analizar si existen afectaciones en la salud visual de los usuarios de los sistemas computacionales, y determinar si existen medidas preventivas para evitarlas y medidas correctivas para solucionarlas.*
- *Analizar las repercusiones recientes y pasadas en la salud visual de estos usuarios, a fin de evaluar las acciones preventivas y si las soluciones a esas repercusiones son favorables para la salud de los usuarios.*
- *Analizar si se consideraron los siguientes aspectos en el estudio inicial, al adquirir, diseñar e instalar los sistemas computacionales en la organización:*
  - *Que se haya cumplido con los estudios relacionados con el efecto de los sistemas computacionales en la salud de los usuarios, y que dichos estudios estén documentados.*
  - *El análisis de el uso de la pantallas de las computadoras, de acuerdo con las características de las pantallas, sus componentes y demás características ergonómicas.*
  - *El análisis de la iluminación del área de trabajo, el color de las pantallas, paredes, hojas y demás aspectos relacionados con la iluminación del lugar de trabajo, a fin de hacerlo más seguro y cómodo.*
  - *El análisis del campo visual horizontal y vertical de los usuarios y de la distancia del usuario a la pantalla y sus ángulos visuales.*
  - *El estudio del impacto visual en los usuarios de los sistemas, antes de instalar el centro de cómputo.*

12.10.2 Evaluación de las repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, nuca, piernas y pies a causa de la posición que adoptan los usuarios

Mediante el análisis de esta gráfica podemos observar a los usuarios de sistemas y de cualquier otro mobiliario y equipo de oficina, cómo les afecta la posición que adoptan al sentarse; estas posturas pueden repercutir, en forma parcial o total, temporal o permanente, en la columna y la espalda, el tórax y tronco, piernas, pies, brazos y, en general, en todo el cuerpo del usuario.



En esta gráfica podemos observar diez posiciones que adoptan los usuarios al sentarse frente a la computadora y cuál es la afectación directa en la columna vertebral, de lo cual podemos: analizar e identificar estas posiciones en los usuarios de sistemas, la frecuencia con que las adoptan y si existen medidas preventivas para evitarlas.

- *Analizar si la constante incidencia de estas posiciones puede repercutir en la salud muscular-esquelética del usuario, ya sea en forma parcial o total, temporal o permanente y leve o grave.*
- *Analizar si se han tomado las medidas preventivas o correctivas para evitar estos vicios de postura.*
- *Analizar globalmente el problema de las posturas de los usuarios, para comprobar los siguientes factores:*
  - *¿Con qué frecuencia e intensidad repercute en la salud del usuario la posición que adopta frente a la computadora?*
  - *Si existen estudios médicos especializados sobre los efectos actuales y futuros en la salud de los usuarios.*
  - *Si, a partir de tales estudios, se han diseñado y se cumplen las medidas preventivas y correctivas para solucionar estos problemas.*
  - *Si existen investigaciones en la empresa sobre las causas de estos vicios de postura de los usuarios de sistemas, y si se definen acciones para crear conciencia sobre este riesgo.*
  - *Si existen muebles de diseño ergonómico para evitar estos vicios de postura.*
- *Verificar que existan estudios en las áreas de sistemas de la empresa sobre los efectos de los sistemas en la salud de los usuarios.*
- *Analizar si esta afectación de la salud muscular-esquelética es producto de las deficiencias del diseño del mobiliario que se utiliza en el centro de cómputo.*
- *Analizar si en el proyecto de un centro de cómputo existen los estudios antropométricos del usuario promedio nacional, que permitan identificar las posibles repercusiones en la salud muscular-esquelética de los usuarios.*
- *En caso de que no existan estudios de este tipo, investigar si se debe a que se desconoce la forma de realizarlos, o a que no se tomaron en cuenta esas necesidades al adquirir el mobiliario.*
- *Investigar con qué efectos y con qué frecuencia se presentan esas repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, cabeza, nuca, piernas y pies del usuario, ya sea por la posición que adopta al estar en contacto con las computadoras o por el diseño del mobiliario del centro de cómputo. Evaluar ambos casos.*
- *Analizar, como complemento de la evaluación de la existencia o carencia de los estudios antropométricos, la periodicidad de otros estudios médicos traumatológicos de las afectaciones sobre una población seleccionada de in-*

dividuos, con mobiliario y equipo diseñados en forma ideal, a fin de comparar esa población con otra población de individuos que seguirán trabajando en la forma actual, sin ninguna mejora en las condiciones de muebles y equipos para el uso de computadoras.

- *Evaluar si existen los siguientes elementos:*
  - *La recopilación de información entre los usuarios que siempre han utilizado la computadora con deficiencias en el mobiliario y equipo y con vicios de postura.*
  - *La comprobación de las repercusiones que han tenido los sistemas en la salud de estos usuarios; precisar si se debe al uso del mobiliario y equipo que se utiliza y a la posición que se adopta. Con esta base es fácil plantear el siguiente punto.*
  - *Evaluar en forma global si la posición que adopta el usuario ante la computadora se debe a defectos en el diseño del mobiliario, esto es, de la silla y la mesa, o por deficiencias y vicios del usuario.*

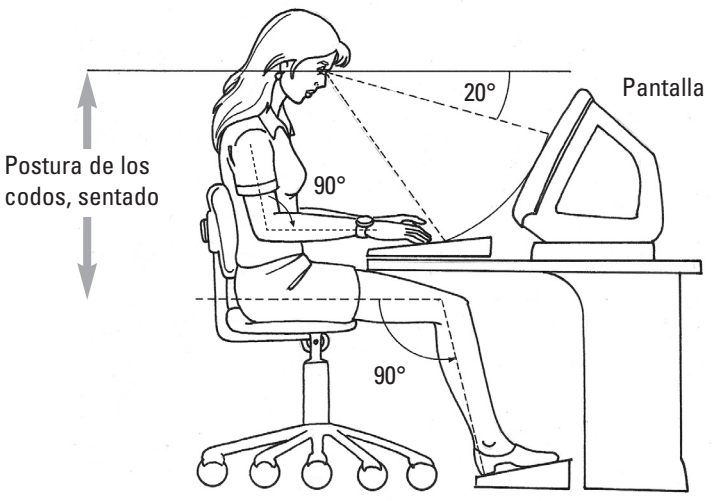
12.10.3 Evaluación de las repercusiones musculares-esqueléticas de manos, muñecas, dedos y brazos del usuario

El diseño actual de los sistemas computacionales, en cuanto al uso del teclado y del ratón, difícilmente puede satisfacer las necesidades de comodidad y bienestar de los usuarios. Esto se debe a que el teclado no permite tener una distancia igual entre los dedos y las líneas de teclas, lo cual hace que se adopte una posición incómoda de las manos. Además, los teclados se colocan en lugares con cierta inclinación, los cuales no son muy adecuados para la posición de manos y brazos. Esto, aunado a su constante uso, llega a repercutir en la salud muscular-esquelética de manos y brazos del usuario. Para comprobar esto, basta con poner las manos abiertas sobre el teclado y darnos cuenta de la separación y distancia de nuestros dedos en cada una de las líneas de teclas. Lo mismo ocurre con la inclinación del teclado. Después de este breve análisis, sólo basta calcular la prolongada adopción de esta postura para deducir cuál será el efecto en manos y dedos, como se ilustra en la figura.

Sin embargo, éstos no son todos los aspectos que se pueden tomar en cuenta al analizar la problemática del uso del teclado, ya que también es posible analizar la postura del antebrazo y de las manos en la altura a la que se encuentra el teclado; lo mismo ocurre con el ratón. En la gráfica se muestra la forma ideal de poner los brazos y manos para manejar teclado. Aunque hay que aclarar que esto depende de la altura de la mesa, la forma y altura del teclado y la distancia de las manos con respecto de la mesa.

En esa gráfica se observa la postura correcta de los brazos, manos y muñecas en relación con el teclado y la mesa. Pero aun así se puede notar una separación importante entre la muñeca, los dedos y el teclado. Esto es lo que repercute en el puente carpiano, lo cual afectaba principalmente a las secretarias y mecanógrafas, y ahora también a los usuarios de sistemas. Para lo cual podemos evaluar:

- *Analizar si existen afectaciones en muñecas, manos, dedos y brazos de los usuarios, debido al uso del ratón y del teclado de la computadora.*
- *Analizar las distintas formas de teclado y ratón, con el fin de identificar el tipo de lesiones, repercusiones y grado de afectación que pudieran llegar a tener estas herramientas en los usuarios.*
- *Analizar la repercusión global que puede tener en el usuario el contacto con estos sistemas; en concreto, evaluar la posición, la distancia y las características de sillas, mesas y otro mobiliario y equipo, así como las características del teclado y del ratón.*



Como complemento de esta parte de la auditoría ergonómica a este renglón, en la gráfica se presenta un análisis global más completo sobre este problema:

- *Investigar si se analizaron las repercusiones del teclado y del ratón en la salud muscular-esquelética de los usuarios al diseñar el centro de cómputo.*
- *Evaluar en forma global si las posturas que se adoptan al usar el teclado y el ratón se deben a defectos en el diseño del mobiliario, por vicios de los usuarios o por deficiencias del diseño de los fabricantes de teclados y ratones.*
- *Recopilar la opinión de los usuarios que siempre han utilizado estos teclados y ratones sobre las deficiencias de fabricación del mobiliario y equipo y sobre los vicios de postura.*
- *Evaluar las repercusiones que tiene en la salud de los usuarios el ambiente donde se utilizan los sistemas computacionales.*

Actualmente, los centros de cómputo de todas las instituciones son lugares donde se concentra la mayoría de los usuarios y, precisamente por estar concentrados los

equipos, debe haber algunas medidas de carácter ergonómico que contribuyan a la comodidad y bienestar de los usuarios. Sin embargo, aunque existan dichas medidas, éstas no siempre son las ideales ni las más deseables para desempeñar el trabajo en forma óptima. Sobre todo cuando se sospecha la carencia de estudios relacionados con el impacto ergonómico en los usuarios de estos sistemas.

También existen usuarios que utilizan la computadora en forma personal, en su casa, oficina o cualquier lugar que, muchas veces, carece de las condiciones mínimas para el uso de sistemas, y su ambiente es muy limitado. Estas condiciones también se deben evaluar, ya que pueden llegar a repercutir en la salud del usuario.

- *Analizar todo lo relacionado con el ambiente que rodea al área de sistemas, por ejemplo:*
  - *La distribución, el uso y los efectos del aire acondicionado en los usuarios.*
  - *La afectación del ruido en el desarrollo del trabajo de sistemas.*
  - *La presencia de humedad, calor, cambios de temperatura y otros fenómenos climáticos en la arquitectura del lugar, con el fin evaluar el desempeño de las actividades de sistemas.*
  - *El acomodo del mobiliario y de todos los demás factores de higiene y seguridad que influyen de alguna manera en la realización de los trabajos del área de sistemas.*
  - *La iluminación, el mobiliario y muchos otros aspectos del centro de cómputo que influyen en la realización de las actividades del centro de cómputo.*
- *Analizar en forma global si existe alguna repercusión en la salud del usuario a causa del ruido, el aire acondicionado, la humedad, la arquitectura, la higiene, la seguridad y otros aspectos del ambiente donde están instalados los sistemas.*
- *Evaluar si estos análisis están apoyados por un estudio inicial de la ergonomía, aplicada exclusivamente al ambiente de trabajo del usuario de los sistemas, de los componentes, el mobiliario y equipo.*
- *Determinar si existe algún estudio ergonómico enfocado exclusivamente a la salud física de los usuarios, sin considerar otros aspectos que estudia la ergonomía, ya que no sería conveniente incluir dichos aspectos debido a lo especializado de su tratamiento.*
- *Realizar un análisis global del problema de los efectos de la computadora en la salud de los usuarios, así como de los efectos de los componentes de cómputo, el mobiliario y equipo, el ambiente, la iluminación del local, el ruido, los sistemas de aire acondicionado, etcétera.*
- *Analizar el efecto que tienen en la vista de los usuarios las pantallas, la iluminación y demás reflejos.*
- *Analizar las posiciones y posturas que adoptan los usuarios frente a la computadora y que repercuten en su columna vertebral, tórax, cuello, nuca y que les producen cansancio y afectaciones ortopédicas.*

- *Analizar las demás afectaciones físicas del ambiente, la iluminación, los sistemas de aire acondicionado, las instalaciones, el mobiliario y los demás medios que rodean el uso de sistemas.*
- *Evaluar el impacto que tienen estos sistemas en el desempeño y la productividad del personal que esté relacionado con ellos.*
- *Evaluar todos los aspectos relacionados con el bienestar, la comodidad y la seguridad que proporciona el ambiente del centro de cómputo al usuario, la repercusión que tiene dicho centro en la salud física y emocional de los usuarios, las medidas preventivas y correctivas para disminuir dichas repercusiones, y el diseño de espacios de trabajo adecuados.*
- *Evaluar la existencia y aplicación de los estudios relacionados con el bienestar, la comodidad y la seguridad de los directivos, empleados y usuarios de los sistemas de la organización.*
- *Evaluar la existencia, actualización y aprovechamiento de los estudios sobre el impacto de los sistemas en la salud física de los directivos, empleados y usuarios de la empresa, en especial en sus repercusiones en vista, tórax, cuello, nuca, columna vertebral, brazos, manos y dedos, para la productividad de la empresa.*
- *Evaluar los estudios y propuestas para el diseño del mobiliario, equipos y ambiente del trabajo de sistemas que permitan a directivos, empleados y usuarios desarrollar su trabajo con seguridad, comodidad y bienestar.*
- *Evaluar la aplicación y seguimiento de los estudios ergonómicos realizados en las áreas de sistemas de la empresa, así como de las medidas preventivas y correctivas derivadas de los mismos, a fin de mantener la seguridad, comodidad y bienestar de los usuarios de sistemas.*

12.10.4 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría ergonómica de los centros de cómputo

En la práctica, esta auditoría casi no se lleva a cabo, ya sea porque aún no se considera importante en los centros de cómputo, o por que tiene aspectos muy específicos, los cuales la vuelven muy diferente de los demás tipos de auditoría. Además, no existen estudios específicos en los que se pueda apoyar el responsable de la auditoría para llevarla a cabo.

Cada una de las partes que hemos analizado tiene aplicaciones concretas, muy específicas y aún no desarrolladas en su totalidad. Lo mismo ocurre con las metodologías de análisis de esta problemática y con los procedimientos y técnicas necesarios para realizar los estudios ergonómicos.

Ante este panorama, el responsable de una auditoría de sistemas también se encuentra sin fundamentos para realizar la evaluación. Por estas razones, en el presente punto no sugerimos ninguna técnica, herramienta o procedimiento aplicable a este ti-

po de auditoría. Sin embargo, recomendamos repasar lo señalado para las auditorías de la gestión informática, alrededor de la computadora, sin la computadora y seguridad de los sistemas computacionales. Esto sin restarles importancia a las técnicas, procedimientos y herramientas de las otras auditorías analizadas en este capítulo.

Además, para realizar evaluaciones ergonómicas, el auditor de sistemas debe apoyarse en los conocimientos de los especialistas en esta rama, a fin de obtener su opinión sobre los puntos concretos que tenga que auditar en un centro de cómputo. De esta manera, también puede obtener o diseñar los procedimientos, técnicas y herramientas específicas para evaluar este tipo de problemática ergonómica.

12.11 Auditoría integral a los centros de cómputo

Podemos definir este tipo de auditoría de la siguiente manera:

> *Es la revisión exhaustiva, sistemática y global de todas las actividades y operaciones de un centro de sistematización, realizada por un equipo multidisciplinario de auditores, a fin de evaluar, en forma integral, el uso adecuado de sus sistemas computacionales, periféricos y equipos de apoyo para el procesamiento de información de la empresa, así como el desarrollo correcto de las funciones de sus áreas, personal y usuarios. Es también la revisión de la administración del sistema, del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, de la adquisición del hardware y software institucionales, de la integración y uso adecuado de sus recursos informáticos y de la existencia y cumplimiento de las normas, políticas, estándares y procedimientos que regulan el uso del sistema y la actuación del personal y usuarios del centro de cómputo.*

Este tipo de auditorías es propiamente el uso conjunto de todos los arquetipos de evaluación, ya que con esta aplicación global se busca hacer una revisión total del sistema computacional de la empresa, no sólo del equipo procesador y sus equipos periféricos asociados, del manejo y control de los sistemas, lenguajes, programa y paqueterías de procesamiento de información, de la administración de los recursos informáticas, la información, el personal y los usuarios del sistema y de las variadas formas de evaluación aisladas que ya hemos señalamos a lo largo de este capítulo; por el contrario, lo que se pretende con dicha auditoría es conjuntar todos esos métodos, aplicaciones y procedimientos en una sola metodología, de una forma integral que permita hacer una evaluación de un centro de cómputo más eficiente y más completa.

En la realización de esta auditoría integral le deben exigir, al auditor la existencia de planteamientos globales, la definición de objetivos comunes y la aplicación de métodos, técnicas y procedimientos estándares de evaluación, los cuales pueden ser diseñados con el apoyo de los sistemas de información y con las herramientas tradi-

cionales de la auditoría; siempre que entre ambos casos se definan herramientas de aplicación uniforme para hacer una evaluación sistemática y completa de todas las actividades y funciones del sistema del centro de cómputo, de sus aplicaciones, su información y de su personal.

Todo esto se puede realizar con el control de todas las actividades del personal que participará en dicha evaluación. Además se tiene que contar con la participación de un equipo multidisciplinario de auditores, quienes tienen que manejar en forma adecuada y conjunta los aspectos relacionados con el ámbito de sistemas y al mismo tiempo las técnicas de auditoría.

Antes de continuar con el tratamiento del tema, debemos establecer que la auditoría integral al centro de cómputo es la revisión global de todos los procedimientos, áreas, sistemas, métodos y los demás aspectos que intervienen en dicho centro; sin embargo, esa revisión se debe hacer de acuerdo con las características y requerimientos propios de cada centro de cómputo.

12.11.1 Tipos de auditoría integral de sistemas

Aunque no existe ninguna clasificación formal de este tipo de auditorías, a continuación presentamos dos formas para realizar una auditoría integral de sistemas; por un lado, la auditoría externa y por otro lado la auditoría interna:

Auditoría externa de sistemas.
Auditoría interna de sistemas.

Antes de seguir con este análisis, conviene aclarar que podemos aplicar los mismos criterios señalados en la sección 2.4 del capítulo 2, tanto para la auditoría integral de carácter externo, realizada por personal ajeno a la empresa como para la de tipo interno, realizada por personal de la propia empresa.

Por esa razón, a continuación presentaremos los aspectos más relevantes que se deben tomar en cuenta al realizar esta auditoría, con la aclaración de que los puntos que estudiaremos a continuación se presentan únicamente a escala conceptual, ya que su aplicación real se deberá adaptar a las características y requerimientos específicos del centro de cómputo a auditar:

- Objetivos de la auditoría integral al centro de cómputo.
- Áreas, sistemas, funciones y elementos que serán auditados.
- Responsabilidades a cumplir en la auditoría integral al centro de cómputo.
- Obligaciones profesionales del auditor que realiza la auditoría integral al centro de cómputo.
- Métodos, técnicas y procedimientos de la auditoría integral al centro de cómputo.
- Estructura de organización de la auditoría integral, según el tamaño del área de sistemas.

A continuación analizaremos detalladamente los puntos anteriores.

12.11.1.1 Auditoría externa de sistemas computacionales

La auditoría externa de sistemas computacionales es aquella que realiza un auditor o un grupo de auditores que son ajenos a la operación normal de la organización en donde se llevará a cabo la revisión del sistema. La principal característica de esta auditoría es que los profesionales que participan en estos trabajos tienen absoluta libertad en la aplicación de sus métodos, técnicas y procedimientos de evaluación, sin que ningún funcionario o empleado del centro de cómputo de la empresa interfiera en su trabajo. Por lo tanto, su dictamen es de carácter independiente.

Para continuar con el análisis de estos puntos, a continuación presentamos los aspectos básicos que se deben tomar en cuenta para el estudio de la auditoría externa de sistemas:

- Los objetivos de la auditoría externa de sistemas son:
  - *Realizar la auditoría con personal ajeno a la empresa, a fin de hacer una evaluación y emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de sistemas.*
  - *Evaluar el aspecto financiero, el uso de los recursos del centro de cómputo y el aprovechamiento del sistema computacional, del mobiliario y de los equipos periféricos e instalaciones.*
  - *Evaluar el aprovechamiento de los sistemas de procesamiento, de los sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.*
  - *Evaluar el cumplimiento de estándares, políticas, normas y lineamientos que regulan las funciones y actividades de los sistemas de procesamiento de información, así como del personal y de los usuarios del centro de cómputo.*
- Áreas, factores y elementos que se deben auditar
  - *Objetivos, planes, programas y presupuestos del área de sistemas.*
  - *Estructura organizacional, funciones y puestos del área de sistemas.*
  - *Administración del sistema de procesamiento, periféricos, instalación, lenguajes, programas e información del centro de computación.*
  - *Administración de los recursos asignados al centro de cómputo.*
  - *Administración del personal y usuarios del área de sistemas, así como las prestaciones y obligaciones de dicho personal.*
  - *Normas, políticas, métodos y procedimientos de operación.*
  - Auditoría a la gestión administrativa del sistema y del centro de cómputo.
    - Auditoría a la estructura de organización, funciones y actividades del área de sistemas.
    - Evaluación del desarrollo de sistemas.
    - Evaluación de la operación del sistema de procesamiento de información.

- Auditoría de los sistemas, lenguajes, programas y paqueterías de aplicación y desarrollo de sistemas.
- Auditoría de los procesadores, periféricos, equipos e instalaciones del centro de cómputo.
- Auditoría de los sistemas de seguridad y de prevención de contingencias.
- Auditoría de otros aspectos de sistemas.
  - Auditoría externa integral de sistemas.
  - Auditoría interna integral de sistemas.

— Aspectos a evaluar con la auditoría integral de sistemas

- *Auditoría de la gestión administrativa del sistema y del área de informática.*
- *Auditoría de la estructura de organización, funciones y actividades del sistema.*
- *Auditoría del desarrollo de sistemas.*
- *Auditoría de la operación del sistema de procesamiento de información.*
- *Auditoría a los sistemas, lenguajes, programas y paqueterías de aplicación y desarrollo de sistemas.*
- *Auditoría a los procesadores, periféricos, equipos e instalaciones que hay en el área de sistemas.*
- *Auditoría de los sistemas de seguridad y prevención de contingencias.*
- *Auditoría de otros aspectos de sistemas.*
- *Programas de aplicaciones y explotación del software.*
- *Metodologías para el análisis y desarrollo de sistemas.*
- *Métodos de acceso, seguridad y operación del sistema.*
- *Configuración.*
- *Evaluación del diseño físico del sistema, en cuanto a:*
- *Configuración del sistema, equipos e instalaciones físicas.*
- *Componentes físicos del sistema, periféricos, mobiliario y equipos.*
- *Características del sistema e instalaciones del centro de cómputo.*
- *Instalaciones eléctricas, de comunicación y del medio ambiente del sistema.*
- *Métodos de acceso, seguridad y protección física del sistema.*
- *Distribución del mobiliario, equipo y sistemas.*
- *Evaluación del control de accesos y salidas de datos, en relación con:*
  - *Estándares y métodos de entradas de datos y salidas de Información.*
- *Especificaciones de acceso y uso de los datos e información del sistema, así como de los procesos y operación del sistema.*

- *Especificaciones sobre las normas, políticas y procedimientos para el acceso de datos, el procesamiento de los mismos y la salida de información del sistema computacional.*
- *Administración y control de los niveles de accesos de administradores, operadores y usuarios del sistema, así como del uso y explotación de dichos niveles de accesos.*
- *Evaluación del control del procesamiento de datos, en cuanto a:*
- *Estándares para la operación y manipulación de datos del sistema.*
- *Identificación, accesos, almacenamiento y custodia de información, archivos y programas.*
- *Formas de procesamiento y procesos de datos en línea o lote y sus justificaciones.*
- *Administración de la frecuencia y volumen de la operación del sistema.*
- *Evaluación de los controles de almacenamiento, en relación con:*
- *Diseño de archivos, bases de datos y almacenamiento de información.*
- *Administración de archivos, programas e información.*
- *Planes y programas de prevención contra contingencias y para la custodia de la información.*
- *Administración del respaldo de información y de los programas institucionales, así como del manejo de los archivos del centro de cómputo.*
- *Evaluación de controles de seguridad.*
- *Sistemas de seguridad y protección del sistema, programas, información, instalaciones, empleados y usuarios del sistema computacional.*
- *Sistemas de control de accesos lógicos al sistema y a las bases de datos.*
- *Sistemas de control de accesos físicos al centro de cómputo.*
- *Procedimientos de acceso al procesador, terminales, programas e información.*
- *Evaluación de controles adicionales para la operación del sistema, en relación con:*
  - *Manuales e instructivos de operación, para usuarios y de procedimientos*
  - *Metodologías y estándares para el desarrollo de sistemas.*
  - *Estándares de programación y documentación.*
  - *Estandarización de lenguajes, programas y paqueterías de uso institucional.*
- *Evaluación de la administración del área de sistemas, en relación con:*
  - *Diseño de la estructura de organización del sistema, áreas de trabajo, funciones y líneas de autoridad y responsabilidad.*

- *Administración centralizada de sistemas, archivos y procesamiento de información.*
- *Administración desconcentrada de sistemas, archivos y procesamiento de información.*

■ *Administración y control de los recursos informáticos.*

- *Estándares para la evaluación y adquisición del hardware, software, mobiliarios, instalaciones y artículos de consumo para el área de sistemas.*
- *Estándares para la selección, capacitación y desarrollo del personal y usuarios del área de sistemas.*
- *Supervisión, coordinación y control de funciones y actividades de funcionarios, personal del área de sistemas y usuarios de los sistemas computacionales.*
- *Supervisión, coordinación y control de la operación del sistema, equipos y periféricos.*

■ *Evaluación de los aspectos técnicos del sistema.*

- *Administración y control del sistema operativo del procesador.*
- *Administración y control de lenguajes de operación, desarrollo y programación.*
- *Administración y control de sistemas de red, multiusuarios y microcómputo.*
- *Administración y control de sistemas de telecomunicación y teleprocesamiento.*
- *Prevención y control de la contaminación informática.*

■ *Actualización permanente de a cuerdo con los cambios computacionales.*

■ *Diseño e implementación de estándares de operación, adquisición, capacitación, desarrollo de sistemas, accesos al sistema, procesamiento de datos y de los demás estándares relacionados con la administración y control del centro de cómputo.*

• Auditoría a la administración interna del área de sistemas

— *Evaluación de la función del personal informático.*

■ *Inventario del personal informático y usuarios del sistema.*

■ *Análisis del perfil de puestos.*

■ *Sueldos, salarios y prestaciones.*

■ *Análisis de los planes y programas de capacitación y adiestramiento.*

■ *Análisis de los índices de rotación y ausentismo laboral del personal del área de sistemas.*

■ *Análisis de la organización del trabajo.*

■ *Análisis de las condiciones de trabajo.*

- *Análisis del estilo de dirección.*

— *Evaluación de la administración de los recursos físicos.*
- *Inventario de sistemas computacionales.*
- *Inventario de mobiliario y equipo de oficina.*
- *Inventario de dispositivos periféricos.*

— *Evaluación de la administración de los recursos informáticos.*
- *Inventario de sistemas operativos.*
- *Inventario de lenguajes, programas y paquetes de desarrollo.*
- *Inventario de programas y paquetes de aplicación.*
- *Inventario de utilerías, librerías y bibliotecas.*
- *Inventario de software institucional.*
- *Inventario de licencias y permisos de uso del software institucional.*

— *Evaluación de la administración de la planeación de proyectos.*
- *Metodologías para el desarrollo de sistemas.*
- *Estándares para el desarrollo de sistemas.*
- *Seguimiento del desarrollo de nuevos proyectos informáticos.*
- *Análisis de la utilidad, compatibilidad y seguimiento de los nuevos proyectos de sistemas.*

— *Evaluación de los reportes de actividades de funcionarios, personal y usuarios del sistema.*
- *Análisis de los reportes de incidencias del personal.*
- *Evaluación del cumplimiento del personal.*
- *Informes.*

— *Evaluación la administración y Control de los gastos corrientes del área de sistemas.*
- *Evaluación de la automatización interna.*

— Administración del área de sistemas
- *Desempeño del personal.*
- *Desarrollo de proyectos.*
- *Gastos de área.*
- *Asignación de recursos.*

— Centros de procesamiento de datos.
- *Hardware.*
- *Software.*
- *Seguridad.*

- *Planes contra contingencias.*
- *Planes de modernización.*

— Desarrollo de sistemas.
- *Metodología.*
- *Planeación y control de proyectos.*
- *Bases de datos.*
- *Control de calidad.*

— Sistemas de producción.
- *Análisis de producción.*
- *Respaldos.*
- *Seguridad en sistemas de producción.*
- *Mantenimiento.*

— Software de trabajo.
- *Adquisición.*
- *Bitácora.*
- *Instalación.*
- *Aplicación.*
- *Control y seguridad.*

12.11.2 Sugerencias de herramientas, técnicas y procedimientos aplicables en la auditoría integral a los centros de cómputo

Esta auditoría viene a ser la concentración de todos los tipos anteriores, sólo que aquí se enfoca en una revisión global del lugar donde se supone se concentran todas las actividades informáticas de una empresa. Se pretende que esta auditoría abarque todos los aspectos de sistemas, en una forma profunda, completa y amplia, a fin de evaluar en forma integral todos los aspectos que intervienen en el ámbito de sistemas. Claro está, la auditoría integral siempre se realizará de acuerdo con el alcance e intención que se le quiera dar a la evaluación, así como con la disponibilidad de recursos y tiempo para realizarla.

La auditoría integral a los centros de cómputo tiene aspectos muy específicos, los cuales hacen que cada una sea muy diferente de otra. Se encuentran notables diferencias entre una auditoría practicada a una empresa con un pequeño centro de cómputo, y a otra cuyo centro sea de mayor envergadura. Aunque ambas auditorías sean integrales y muy similares en algunos alcances, intenciones e incluso en los puntos que abarquen, las herramientas, los procedimientos, las técnicas y los métodos de evaluación son totalmente diferentes. Lo mismo ocurre con centros de cómputo de diferente plataforma, así como entre áreas de sistemas que administran redes LAN o WAN y las

que manejan PCs individuales o sistemas de equipos mayores. En todos los casos las necesidades de evaluación son distintas.

Tampoco es lo mismo auditar integralmente un centro de cómputo donde se utiliza COBOL como lenguaje de desarrollo, en el que todas las bases de datos y actividades están orientadas a ese lenguaje, que un centro de cómputo, de similares características, pero que maneje su información en DB2, cuyas aplicaciones y bases de datos tienen diferentes sentidos y características. Cada cual tiene aplicaciones, metodologías, procedimientos y técnicas diferentes entre sí.

Por todas estas razones, en este punto no presentamos sugerencias de técnicas, herramientas y procedimientos aplicables a este tipo de auditoría. Sin embargo, sí recomendamos que el responsable de la auditoría repase todo lo señalado para los tipos de auditorías anteriores y de ahí obtenga lo que a su parecer sea lo mejor y que se adapte más a sus necesidades de evaluación. Así, conjuntando todos estos elementos podrá determinar los que requiera para su auditoría integral. Claro, sin menoscabo de los propios procedimientos, técnicas y herramientas específicos que su experiencia le dicte para llevar a cabo de una mejor forma este tipo de auditoría de sistemas.

Apéndice

A

Lista de verificación para una auditoría a la gestión informática

Auditoría a la planeación estratégica en la empresa y en el área de sistemas

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La misión de la actividad informática.				
La visión de la actividad informática.				
Los objetivos generales y específicos de la actividad informática.				
Las estrategias para el funcionamiento de la actividad informática.				
Las funciones fundamentales para proporcionar el servicio informático a las áreas de la empresa.				
Las políticas, normas y lineamientos que regulen la actividad informática en la empresa y en el área de sistemas.				
Los procedimientos generales para proporcionar la actividad informática.				
La existencia, difusión, seguimiento y control de la misión, visión, objetivo, políticas, normas, lineamientos y procedimientos para la actividad informática de la empresa.				

Auditoría a la estructura de organización del área de sistemas

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La división funcional (u otro criterio) para el área de sistemas.				
La estructura de puestos del área de sistemas.				
Las funciones de los puestos del área de sistemas.				
Los canales formales e informales de comunicación en el área de sistemas.				
Los niveles de autoridad y responsabilidad de los puestos del área de sistemas.				
La reestructuración y/o actualización de puestos.				
Los perfiles de puestos.				
Las estructuras para el desarrollo de proyectos, atención a usuarios y operación de las actividades informáticas de la empresa.				
Los manuales de organización, procedimientos, operación y demás documentación normativa del área de sistemas.				
Otros aspectos de la gestión administrativa en el área de sistemas.				

Auditoría al cumplimiento de las funciones, tareas y operaciones de la actividad informática en la empresa y en el área de sistemas

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La existencia, difusión y cumplimiento de las funciones, tareas y operaciones de la actividad informática en el área de sistemas.				
El seguimiento de los manuales e instructivos del área de sistemas.				
Los métodos y procedimientos para la actividad informática en la empresa y en el área de sistemas.				
El cumplimiento de los fundamentos y principios administrativos aplicables al área de sistemas de la empresa.				

Auditoría a la dirección del área de sistemas

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
El ambiente laboral en el área de sistemas.				
El estilo de liderazgo y ejercicio de autoridad en el área de sistemas.				
Las jerarquías de autoridad y responsabilidad en el área de sistemas.				
La coordinación del personal y usuarios del área de sistemas.				
La coordinación de los recursos informáticos utilizados para la actividad informática en el área de sistemas y en la empresa.				
Las relaciones de trabajo jefe-subordinado e iguales.				
El ejercicio y control de la toma de decisiones en el área de sistemas.				
La integración de grupos de trabajo en el área de sistemas.				
Las relaciones de comunicación formal (comunicación escrita, verbal, correo electrónico u otras formas de comunicación) en el área de sistemas.				

Auditoría a la administración del factor humano en el área de sistemas

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
La coordinación de las funciones, actividades, tareas y operaciones del personal informático del área de sistemas.				
La división funcional de las funciones, actividades y operaciones del factor humano del área de sistemas.				
Los planes y programas de capacitación, adiestramiento y promoción del personal y usuarios del área de sistemas.				

La rotación y movilidad del personal del área de sistemas.				
La motivación para el personal y usuarios del área de sistemas.				
Los procesos de selección de personal para el área de sistemas.				
La remuneración y prestaciones para el personal del área de sistemas.				
Integración de grupos de trabajo.				
La evaluación del cumplimiento de las funciones y actividades del personal, del perfil de puestos y la asignación de actividades en el área de sistemas.				
Los estudios ergonómicos para el personal y usuarios del área de sistemas.				
La gestión directiva de funcionarios, empleados y usuarios.				

Auditoría a la administración de los recursos informáticos no humanos del área de sistemas

Calificar el grado de cumplimiento de:	**100%**	**75%**	**50%**	**25%**
La administración de los sistemas computacionales (*hardware*) del área de sistemas y de los sistemas de las demás áreas de la empresa.				
La administración del sistema computacional (*software*) del área de sistemas y del sistema de las demás áreas de la empresa.				
La administración de las instalaciones del sistema computacional del área de sistemas y de las instalaciones de las demás áreas de la empresa que cuenten con sistemas.				
La administración de las telecomunicaciones del sistema computacional del área de sistemas y de las telecomunicaciones de las demás áreas de la empresa que cuenten con sistemas.				
La administración de las bases de datos e información del área de sistemas y de las bases de datos de las demás áreas de la empresa que cuenten con sistemas.				
La administración del mobiliario y equipo asignados al área de sistemas y del mobiliario de las demás áreas de la empresa que cuenten con sistemas.				
La administración de los bienes materiales, consumibles y materiales de oficina utilizados en el área de sistemas, y de los materiales de las demás áreas de la empresa que cuenten con sistemas.				

La administración de las adquisiciones de sistemas computacionales, *hardware*, *software*, componentes, periféricos, mobiliario, equipos, consumibles y demás implementos para el funcionamiento de los sistemas de la empresa.				
La administración de los bienes informáticos y activos del área de sistemas y de los bienes informáticos de las demás áreas de la empresa que cuenten con sistemas.				
Los planes, programas y presupuestos que afectan al área de sistemas.				
La gestión financiera y contable de los recursos del área de sistemas.				

Auditoría a los controles informáticos del área de sistemas

Calificar el grado de cumplimiento de:	**100%**	**75%**	**50%**	**25%**
Los controles internos sobre la organización del área de sistemas.				
Los controles internos sobre el desarrollo de sistemas.				
Los controles internos sobre la operación del sistema.				
Los controles sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados.				
Los controles internos sobre la seguridad en el área de sistemas.				

Evaluación de la existencia, establecimiento y uso de los estándares de sistemas

Calificar el grado de cumplimiento de:	**100%**	**75%**	**50%**	**25%**
Las metodologías del análisis y diseño de sistemas.				
El uso de software, lenguajes y programas de desarrollo para la programación y codificación de sistemas.				
La elaboración y seguimiento de pruebas y simulaciones de sistemas, programas y lenguajes de cómputo nuevos, así como para erradicar virus informáticos.				
La liberación e implantación de nuevos sistemas.				
La capacitación y el adiestramiento del personal y usuarios del área de sistemas.				
La documentación de sistemas.				
Las adquisiciones de sistemas computacionales, así como de sus materiales y demás componentes y consumibles.				
Los demás estándares que regulen el desempeño de la función informática en la empresa.				

Auditoría a la documentación de los sistemas en el área de informática y a la documentación de las demás áreas de la empresa que cuenten con servicios informáticos

Calificar el grado de cumplimiento de:	100%	75%	50%	25%
Los manuales de usuarios.				
Los manuales técnicos del sistema.				
Los manuales de capacitación.				
Los manuales de operación.				
Las bitácoras de proyectos nuevos.				
La documentación de pruebas y simulaciones de sistemas.				
La actualización de manuales.				
La existencia, difusión, préstamo y uso de los manuales e instructivos de sistemas computacionales.				

Apéndice

B

Lista de verificación para una auditoría a la seguridad informática

Seguridad en los sistemas computacionales y dispositivos periféricos.

Seguridad en la información institucional y bases de datos.

Seguridad en los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional.

Seguridad en los activos informáticos del área de sistemas.

Seguridad para el personal informático y los usuarios del sistema.

Seguridad en la protección y conservación de locales, instalaciones, mobiliario y equipos.

Seguridad en los accesos a las áreas de sistemas, así como a sus sistemas computacionales, información y software.

Seguridad en la arquitectura de las telecomunicaciones.

Seguridad en los sistemas de redes, sistemas mayores y PCs.

Seguridad contra la piratería informática.

Seguridad contra los virus informáticos.

- Auditoría de la seguridad en las condiciones e instalaciones físicas del área de sistemas
- Protección contra los riesgos y contingencias de origen natural relacionados con el ambiente de trabajo.
  - Las condiciones generales de trabajo de los sistemas computacionales, para el bienestar y comodidad de los empleados y usuarios del sistema.
  - Protección contra la humedad del ambiente.
  - Medidas para prevenir que los sistemas computacionales y las instalaciones eléctricas, telefónicas y de datos tengan contacto con el agua.
  - Protección contra las partículas de polvo y deshechos volátiles de cualquier tipo en el ambiente, a fin de evitar desperfectos en los sistemas computacionales y medios de almacenamiento, así como el deterioro de los activos informáticos del área de sistemas.
  - Protección contra la estática e imantación producidas por fibras sintéticas, metales, algunos plásticos y por el cabello humano y animal que pueden repercutir en el funcionamiento de los sistemas computacionales de la empresa.
  - Análisis de los sistemas de acondicionamiento y pisos falsos.
  - Análisis de la regulación de temperatura y aire acondicionado.
  - Análisis de los suministros de energía, comunicaciones y procesamiento de datos.
  - Análisis de la limpieza del área de sistemas.

- Protección contra riesgos y contingencias relacionados con el ambiente de trabajo en las áreas de sistemas de la empresa.
  - La iluminación artificial del área de sistemas y la iluminación por medio de luz solar.
  - Las instalaciones eléctricas, de datos y de comunicación.
  - Los accesos y salidas en las áreas de sistemas.
  - La repercusión de los aspectos de carácter ergonómico.
  - Las adaptaciones de los equipos de cómputo.
  - Las condiciones de trabajo con computadora.
  - Protección contra contingencias causadas por la temperatura del sistema de aire acondicionado.
  - La ventilación natural de las áreas y espacios.
- Protección contra riesgos y contingencias causados por factores meteorológicos, atmosféricos y desastres naturales incontrolables.
  - Por precipitación pluvial, de nieve, de granizo y otras precipitaciones.
  - Por vientos, huracanes, ciclones y fenómenos atmosféricos.
  - Por terremotos y temblores.
  - Por inundaciones, marejadas, maremotos y fenómenos marítimos.
  - Por tormentas eléctricas.
  - Por incendios accidentales.
  - Otros fenómenos de origen natural que afectan a las áreas de sistemas y a los propios sistemas computacionales.
- Protección contra riesgos y contingencias derivados del suministro de la energía eléctrica.
  - Prevención de interrupciones y falta permanente del suministro de energía eléctrica para el funcionamiento de los sistemas computacionales.
  - Continuidad del suministro de la energía eléctrica, por medio de la red pública o plantas de emergencia, fuentes ininterrumpidas de poder y no-breaks.
  - Previsión en la funcionalidad, distribución adecuada y seguridad de las instalaciones eléctricas del área de sistemas.
  - Prevención de fallas y deficiencias de la red pública de suministro de electricidad.
  - Protección contra las variaciones de voltaje, así como el uso de reguladores de corriente, contactos supresores de picos y sistemas de no-breaks.
  - El análisis del cableado público de las instalaciones eléctricas que están fuera de la empresa.
  - El análisis del cableado, construcciones y adaptaciones eléctricas, contactos, tierra física y demás instalaciones eléctricas internas del área de sistemas.
- Protección y seguridad de los espacios físicos de las instalaciones de cómputo.

- En los sistemas de vigilancia de las áreas de sistemas.
- En los accesos a las instalaciones de las áreas de cómputo.
- En las áreas restringidas y de accesos exclusivos.
- En las áreas de trabajo de sistemas, almacenamiento, cintotecas (bóvedas) y otros espacios de sistemas.
- En la administración y control de los medios de seguridad, y de la observación y vigilancia de los sistemas computacionales.
- En la vigilancia del mobiliario, equipo y activos informáticos de las áreas de sistemas.
- En la vigilancia del almacenamiento de información, datos y software institucional en las áreas de cómputo.
- En la vigilancia de accesos a los sistemas computacionales en las áreas ajenas al centro de cómputo.
- En la seguridad, salvaguarda y protección de las cintas, disquetes y otros medios magnéticos utilizados en el área de sistemas.
- En la seguridad y protección de manuales, instructivos, datos, información y reportes del área de sistemas.
- En la totalidad, veracidad y confiabilidad de la captura de información.

- El análisis de los planes de contingencias informáticas.
  - Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias de sistemas.
  - Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.
  - Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.

- Auditoría de la seguridad y protección en el diseño de las instalaciones del área de sistemas de la empresa y/o empresas de cómputo.
  - En el análisis de los estudios de localización de planta para instalar el área de sistemas.
  - En el análisis para la localización de instalaciones físicas del área de sistemas.
  - En el análisis de los estudios de la densidad de población.
  - En el análisis de la infraestructura pública de servicios.
  - En el análisis de los medios de comunicación pública, y de los medios de transporte de pasajeros.
  - En el análisis de los estudios de composición del suelo para prevenir desastres naturales.
  - En el análisis del cableado telefónico interno para el funcionamiento del área de sistemas.
  - En el análisis del cableado externo y redes públicas del servicio telefónico, así como de telecomunicación para el funcionamiento del área de sistemas.

- Auditoría de la seguridad en los sistemas computacionales.
  - Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.
  - Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización.
  - Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos del área de sistemas.
  - Evaluar el rendimiento, la aplicación y la utilidad del equipo de cómputo, mobiliario y demás equipos.
  - Evaluar la seguridad en el procesamiento de información.
  - Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.
- Auditoría de la seguridad del hardware
  - Realizar inventarios de hardware, equipos y periféricos asociados.
  - Evaluar la configuración del equipo de cómputo (hardware).
  - Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.
  - Evaluar el estado físico del hardware, periféricos y equipos asociados.
- Auditoría de la seguridad del software
  - Realizar inventarios de software, paqueterías y desarrollos empresariales.
  - Evaluar las licencias, permisos y usos de los sistemas computacionales.
  - Evaluar el rendimiento y uso del software de los sistemas computacionales.
  - Verificar que la instalación de software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta última.
- Auditoría para verificar la captura, procesamiento de datos y emisión de resultados
  - Evaluar la totalidad, veracidad y confiabilidad de la captura de información.
  - Evaluar la existencia, difusión, aplicación y uso del plan contra contingencias en los sistemas.
  - Evaluar la aplicación de simulacros, así como del plan contra contingencias durante la ocurrencia de siniestros en los sistemas.
  - Evaluar la confiabilidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.
- Auditoría de la prevención de actos premeditados que afecten el funcionamiento de los sistemas computacionales
- Protección contra los actos ilegales en contra de los sistemas, activos informáticos e información.
  - Contra sabotajes.
  - Por extorsión.

  - — Por alteración o destrucción de datos.
  - — Por fraudes.

- Protección contra el mal uso de la información.
  - — Por invasión de privacidad.
  - — Para mal uso de la confiabilidad.
  - — Por uso inadecuado de los datos.

- Protección contra la piratería y robo de información.
  - — Con medidas preventivas.
  - — Con la protección de archivos.
  - — Con limitación de accesos.
  - — Con protección contra robos.
  - — Con protección ante copias ilegales.

- Protección para el almacenamiento de la información.
  - — Respaldos de programas e información.
  - — Almacenamiento y custodia de cintas, disquetes, etcétera.
  - — Lugares adecuados, como cintotecas (bóvedas), discotecas, etcétera.
  - — El control y uso de información, programas y paquetes.

- Protección contra actos no intencionales.
  - — Por negligencia y descuido.
  - — Por fallas del equipo y del sistema.
  - — Por fallas de carácter externo.

- Protección contra virus informático.
  - — Medidas preventivas y correctivas.
  - — Uso de vacunas y buscadores de virus.
  - — Protección de archivos, programas e información.

- Protección y seguridad para el desarrollo de programas y proyectos de sistemas.
  - — Desarrollo de programas y nuevos proyectos de sistemas.
  - — Protección contra deficiencias de programas y lenguajes.
  - — Prevención de fallas del sistema operativo.
  - — Protección en el establecimiento de estándares de proyectos.

- Protección y seguridad para los accesos al sistema computacional y a la información.
  - — En el uso de contraseñas.
    - ■ Establecimiento de niveles de acceso y uso de archivos.
    - ■ Para el uso de sistemas de encriptación.
  - — Para el uso de estándares de seguridad y protección.

- Protección y seguridad del hardware, componentes del sistema, periféricos y equipos asociados.
  - Protección a la CPU.
- Mantenimiento preventivo y correctivo a la CPU.
  - Medidas de seguridad y protección.
  - Rutinas internas para el inicio del sistema.
  - Rutinas internas de auditoría y verificación de componentes.
- Mantenimiento preventivo y correctivo al sistema.
  - Rutinas internas de auditoría y verificación de conexiones.
  - Con el uso de manuales e instructivos de operación.
- Mantenimiento preventivo y correctivo a los periféricos.
  - Rutinas internas de auditoría y verificación de periféricos.
  - Para el uso adecuado de los periféricos.
- Mantenimiento preventivo y correctivo al equipo adicional.
  - Rutinas internas de auditoría y verificación de equipos.
- Resultados de auditorías de sistemas.
- Seguridad ante fenómenos sociales
  - Protección contra mítines, revueltas, etc.
    - Prevención de huelgas.
    - Prevención ante cambios sociales, económicos, legales, etc.

Prevención ante cambios tecnológicos.

El levantamiento de inventarios (sección 9.5), a fin de hacer un recuento de los bienes informáticos del área de sistemas cuya seguridad se tenga que evaluar; para llevar a cabo esto, es recomendable realizar los siguientes inventarios:

- Inventarios de los equipos de cómputo, contemplando la seguridad, protección y salvaguarda de los bienes informáticos y sistemas computacionales, sus marcas, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con el inventario de la seguridad de estos equipos.
- Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas, a fin de valorar su protección y custodia.

- Inventario del personal informático y usuarios del sistema, a fin de evaluar la protección de este importante recurso.
- Inventario de las medidas de seguridad y protección para los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo sus licencias, resguardos y copias de seguridad.
- Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, a fin de valorar su protección y uso adecuados.
- Inventario de los accesos a los sistemas de redes o sistemas mayores, dependiendo del diseñado del sistema, así como del acceso a la información y a los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o sistemas mayores.
- Inventario de las instalaciones físicas, a fin de evaluar la vigilancia y los accesos establecidos para la protección y seguridad de los bienes informáticos del área de sistemas.
- Inventario de las normas, políticas, reglamentos y medidas preventivas y correctivas del área de sistemas, a fin de evaluar la seguridad establecida para satisfacer las necesidades de protección en la función informática.
- Otros inventarios relacionados con la seguridad, protección y salvaguarda de los bienes informáticos del área de sistemas.

Apéndice C

Listado de verificación de auditoría de redes

Gestión administrativa de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Los objetivos de la red de cómputo.					
Las características de la red de cómputo.					
Los componentes físicos de la red de cómputo.					
La conectividad y las comunicaciones de la red de cómputo.					
Los servicios que proporciona la red de cómputo.					
Los sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas de la red de cómputo.					
Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.					
Los protocolos de comunicación interna de la red.					
La administración de la red de cómputo.					
La seguridad de las redes de cómputo.					

Evaluación del análisis de la red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de redes de cómputo.					
Análisis de la definición de la problemática y solución para instalar redes de cómputo en la empresa.					
Análisis del cumplimiento de los objetivos fundamentales de la organización para instalar una red de cómputo, evaluando en cada caso:					
La forma de compartir los recursos informáticos de la organización, especialmente la información y los activos.					

La cobertura de los servicios informáticos para la captura, el procesamiento y la emisión de información en la organización.					
La cobertura de los servicios de comunicación.					
La frecuencia con que los usuarios recurren a los recursos de la red.					
La confiabilidad y seguridad en el uso de la información institucional.					
La centralización, administración, operación, asignación y el control de los recursos informáticos de la organización.					
La distribución equitativa de los costos de adquisición y operación de los recursos informáticos de la organización.					
La escalabilidad y migración de los recursos computacionales de la organización.					
La satisfacción de las necesidades de poder computacional de la organización, sea con redes, cliente/servidor o mainframe.					
La solución a los problemas de comunicación de información y datos en las áreas de la organización.					

Análisis de la delimitación de los proyectos de red, a fin de evaluar la manera en que se cumplen:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La delimitación temporal, por el tiempo en que se instalará la red.					
La delimitación espacial, por las dimensiones físicas y lógicas del proyecto de red.					
La delimitación conceptual, por el análisis específico de las necesidades que se deben satisfacer con la red de cómputo.					
La delimitación tecnológica, por los requerimientos y conocimientos informáticos específicos en sistemas de red.					

Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
El estudio de factibilidad tecnológica.					
El estudio de factibilidad económica.					
El estudio de factibilidad administrativa.					
El estudio de factibilidad operativa.					
Otros estudios de factibilidad que repercuten en el diseño e instalación de la red en la organización.					

Análisis de la escalabilidad y el aprovechamiento de los recursos informáticos de la empresa para instalar una red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la tolerancia de las posibles fallas de la red.					
Análisis de la transparencia del trabajo para los usuarios de la red.					

Evaluación del diseño e implementación de la red según el ámbito de cobertura

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de las redes de multicomputadoras.					
Evaluar el funcionamiento de la cobertura de punto a punto.					
Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas.					
Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes.					

Análisis de la red de área local (LAN)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 10 metros a 10 kilómetros.					
Evaluar el uso adecuado y confiable de la tecnología utilizada internamente					

para la transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas, en todas las computadoras conectadas a la LAN.					
Evaluar la restricción adoptada para establecer el tamaño de la red.					
Evaluar el tiempo promedio de transmisión de la red (entre el peor caso y el mejor caso de transmisiones conocidas de datos).					
Evaluar que las velocidades utilizadas normalmente en su transmisión estén en el rango de 10 a 100 Mbps.					

Análisis de la red de área metropolitana (MAN)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 10 a 100 kilómetros.					
Evaluar los criterios adoptados para establecer el tamaño y la cobertura de la red.					
Evaluar el funcionamiento de la tecnología utilizada internamente en la transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas, en todas las máquinas conectadas en la red LAN.					
Evaluar el tiempo promedio de transmisión de la red.					
Evaluar las velocidades utilizadas normalmente en la transmisión.					

Análisis de la red de área amplia (WAN)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 100 a 1,000 kilómetros.					
Evaluar el funcionamiento de la composición, consistente en la colección de hosts (computadoras					

interconectadas) o LANs de hosts conectados por medio de subredes.					
Evaluar la forma de enviar los paquetes de un enrutador a otro, según las características de envío de la red.					
Evaluar el uso adecuado y confiable de la tecnología (interna y externa) de transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas, en todas las máquinas conectadas a las LANs y a la WAN.					
Evaluar la conveniencia del tiempo promedio de transmisión de la red entre LANs y entre subredes.					
Evaluar que las velocidades utilizadas normalmente en la transmisión cumplan con los rangos establecidos para este tipo de redes.					

Análisis de las redes públicas (también conocidas como Internet)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar su cobertura de 10,000 a 100,00 kilómetros.					
Evaluar la composición de esta red, consistente en la integración de la red Internet a la vinculación con puertas de enlace (gateways), computadoras que pueden traducir entre formatos incompatibles.					
Evaluar el uso adecuado y confiable de la tecnología y sistemas de interconexión utilizados (interna y externamente) en la transmisión de datos, como el cable coaxial, cable de par trenzado, fibra óptica o sistemas de transmisión satelital o de microondas.					
Evaluar las velocidades utilizadas normalmente en la transmisión.					

Análisis de las redes inalámbricas

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar el uso adecuado de este tipo de red según sus características.					
Evaluar el uso adecuado y confiable del radio, microondas, satélites, infrarrojo o cualquier otro mecanismo de comunicación sin cable.					
Evaluar la posibilidad de combinar las redes inalámbricas con otras computadoras móviles y/u otras redes.					
Evaluar las posibilidades de integrar Internet o su vinculación con puertas de enlace u otros sistemas de computadoras que pueden traducir entre formatos incompatibles.					

Evaluación del diseño e instalación de la red según su configuración básica

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Red(es) establecida(s) en la empresa:					
Análisis del diseño e implementación del tipo de red basada en el concepto de servidor único.					
Análisis del diseño e implementación del tipo de red basada en el concepto cliente/servidor.					
Análisis del diseño e implementación del tipo de red de punto a punto (uno a uno).					
Análisis del diseño e implementación del tipo de redes de multipunto (uno a muchos, muchos a muchos).					
Análisis del diseño e implementación del tipo de red lógica basada en el concepto de conexión entre terminales sin cables.					
Análisis del diseño e implementación del tipo de red virtual basada en el concepto de tecnología y comunicación vía Internet.					

Análisis del diseño e implementación de la topología de cobertura de la red, en cuanto a:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Estudio de las necesidades de cobertura con la topología física de la red.					
Estudio de las necesidades de cobertura con la topología lógica de la red.					

Análisis del diseño de los modelos de comunicación ISO de la red de la empresa, en cuanto al funcionamiento de las siguientes capas:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Capas físicas.					
Capas de enlace.					
Capas de red.					
Capas de transporte.					
Capa de sesión.					
Capa de presentación.					
Capa de aplicación.					

Análisis de los estándares adoptados para el funcionamiento de las redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
EtherNet (norma IEEE 802.3).					
Token ring (norma IEEE 802-5).					
ARCnet (Attached Resource Computer Network).					
IPX (Internetwork Packet Exchange).					

Evaluación del diseño e implementación de las características de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la confiabilidad en el funcionamiento de los medios de transmisión y del medio físico que utiliza la red para la comunicación entre las computadoras que la integran.					
Cableado.					

Transmisión por radio, microondas, satelital, infrarrojo y cualquier otro tipo de comunicación sin cable.					
Combinación de los medios de transmisión.					

Análisis de las técnicas de transmisión que determinan cómo se utilizan los medios físicos para la comunicación entre las computadoras de la red, estudiando el funcionamiento de:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La transmisión síncrona.					
La transmisión asíncrona.					
La transmisión analógica.					
La transmisión digital.					
La codificación de datos en señales analógicas.					
La transmisión en paralelo.					
La transmisión en serie.					
Los códigos de comunicación de datos.					

Análisis del funcionamiento y la confiabilidad de los dispositivos para conectar las redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Repetidores. Sirven para amplificar o regenerar las señales, con lo cual pueden utilizarse cables más largos.					
Puentes. Son los dispositivos para guardar y reenviar los datos en la red; operan en el nivel de enlace y pueden cambiar los campos de las tramas.					
Enrutadores de protocolos múltiples. Son como los puentes que funcionan en el nivel de red y que permiten la conexión de redes con distintos protocolos.					
Puertas de enlace de transporte. Conectan las redes en nivel de transporte.					
Puertas de enlace de aplicación. Conectan dos partes de una aplicación, aunque éstas utilicen formatos distintos.					

Análisis del funcionamiento de las técnicas de transferencia de datos

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Simplex. Solamente en un sentido.					
Semidúplex. En ambos sentidos, pero uno a la vez.					
Dúplex total. En ambos sentidos a l a vez.					

Análisis de los tipos de topologías utilizados en el diseño de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Topología de bus.					
Topología de estrella.					
Topología de anillo.					
Topología de malla.					
Topología de doble anillo.					
Análisis de los métodos de acceso al medio y de la manera en que se conectan los dispositivos de la red para utilizar la transmisión por el medio físico.					
Evaluación del diseño e implementación de los componentes de la red de cómputo.					
Análisis del diseño e implementación del tipo de servidor principal establecido para la red.					
Análisis del diseño e implementación de los servidores dedicados.					
Análisis del diseño e implementación de los servidores no dedicados.					
Análisis del diseño e implementación de los servidores de apoyo.					
Servidores de archivos (distribuidos, dedicados y no dedicados).					
Servidores de discos (dedicados y no dedicados).					
Análisis del diseño e implementación de los servidores de impresión.					
Análisis del diseño e implementación de los servidores de comunicación.					

Análisis del diseño e implementación de los concentradores.					
Análisis del diseño e implementación de los otros tipos de servidores.					

Análisis del diseño e implementación de las estaciones de trabajo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Características y componentes de la terminal o estación de trabajo.					
Número de terminales o estaciones de trabajo.					
Aplicaciones de la terminal o estación de trabajo.					
Privilegios, información y uso de la terminal o estación de trabajo.					

Análisis del funcionamiento y la confiabilidad de los elementos de enlace físico de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del diseño e implementación de los nodos de la red.					
Análisis del uso de las tarjetas de la red.					
Tarjetas de interfaz de red.					
Adaptador de 2Mbps (este adaptador soporta longitudes de hasta 500 metros de cable de par trenzado sin blindaje o UTP.					
Adaptador EtherNet AE-1/t de bajo costo y número limitado por número de puertos hub, y velocidad de transferencia de 10Mbps.					
Adaptador EtherNet AE-2; es un adaptador inteligente con autoconfiguración de selección de parámetros óptimos de funcionamiento.					
Adaptador EtherNet AE-2/t para conexiones de cables UTP y coaxial.					
Adaptador EtherNet AE-3 para soportar tres tipos de cable: UTP, coaxial grueso y coaxial delgado.					

Cable de par trenzado de amplio rango, sin blindaje y UTP.					
Cable coaxial.					
Cable de banda base para un solo canal con un solo mensaje a la vez y velocidades de 10 a 80 Mbps.					
Cable de banda ancha; este cable maneja varias bandas a la vez y en diferentes frecuencias de manera simultánea, con sistema dual de cable o un solo cable y amplificadores bidireccionales.					
Cable de fibra óptica.					

Análisis de la confiabilidad y el funcionamiento correcto de los elementos establecidos para la expansión de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Repetidores, para recibir y retransmitir datos, compensando las pérdidas de señal.					
Puentes y dispositivos para la capa de enlace OSI, para manejar datos de origen y destino.					
Puentes/enrutadores y dispositivo de interconexión de la red.					
Enrutadores relacionados directamente con los protocolos de comunicación.					
Puertas de enlace, dispositivos para la conexión de minicomputadoras y mainframes.					
Evaluación del diseño e implementación de los protocolos de comunicación de la red.					

Análisis de la adopción de jerarquías de protocolos en la red de la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
El software para controlar las redes y las estructuras para manejar la complejidad.					
La organización en la mayoría de las redes en una pila de niveles.					

Los niveles que ofrecen ciertos servicios a los niveles superiores y la implementación de estos servicios en el nivel inferior siguiente para implementar sus servicios.					
El nivel de comunicación "n" de una computadora con el nivel "n" de otra computadora.					
Las reglas y convenciones que controlan la conversación entre las computadoras, según el nivel "n" de los protocolos.					
Las entidades en niveles correspondientes de comunicación entre computadoras distintas.					
La transferencia de los datos directamente del nivel "n" de otro nivel, a fin de pasar la información hacia abajo de un nivel a otro hasta que llegue al nivel del medio físico.					
Los niveles donde están las interfaces permiten cambios en la implementación de un nivel sin afectar el nivel superior.					
El nivel que tiene que transmitir un paquete a otra computadora para que ésta pueda agregar un encabezamiento al paquete y pueda identificar el mensaje y el destino al nivel de la mayoría de las redes para imponer el límite en el tamaño de los paquetes.					

Análisis del funcionamiento del modelo OSI para la red, estudiando el comportamiento de los siguientes niveles:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Nivel físico. Para las relaciones de los voltajes, la duración de un bit, el establecimiento de una conexión, el número de polos de enchufe y demás aspectos técnicos de este nivel.					
Nivel de enlace. Para convertir el medio de transmisión crudo en uno que esté libre de errores de transmisión en cuanto al remitente de los datos de entrada, el procesamiento de los de					

acuse y el manejo de las tramas perdidas, dañadas, o duplicadas, y en cuanto a la regulación de la velocidad del tráfico.					
Nivel de red. Para determinar el enrutamiento de los paquetes desde sus fuentes hasta sus destinos, manejando la congestión a la vez y su incorporación a la función de contabilidad.					
Nivel de transporte. Es el primer nivel de comunicación directa de su par en el destino (los anteriores niveles son de computadora a computadora). Este nivel suministra varios tipos de servicio, como abrir conexiones múltiples de red para proveer capacidad alta. Se puede utilizar el encabezamiento de transporte para distinguir entre los mensajes de conexiones múltiples que entran en una máquina y abastecer el control de flujo entre los hosts.					
Nivel de sesión. Parecido al nivel de transporte, pero provee servicios adicionales, ya que puede manejar token (objetos abstractos y únicos) para controlar las acciones de los participantes, o puede hacer checkpoints (puntos de inspección) en las transferencias de datos.					
Nivel de presentación. Provee funciones comunes a muchas aplicaciones, como traducciones entre juegos de caracteres, códigos de números, etc.					
Nivel de aplicación. Define los protocolos usados por las aplicaciones individuales de la red. Entre estas aplicaciones tenemos el correo electrónico y Telnet, entre otros.					

Análisis del funcionamiento adecuado de los protocolos X.25 para la red, estudiando el comportamiento de las siguientes capas:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Capa física.					
Capa de bloque.					
Capa de paquetes.					

Análisis del funcionamiento adecuado de los protocolos TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet)

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar el cumplimiento de los objetivos, la conexión de redes múltiples y la capacidad de mantener conexiones aun cuando una parte de la subred esté perdida.					
Evaluar la aplicación de red packet-switched, basada en un nivel de Internet sin conexiones.					
Evaluar la aplicación y el funcionamiento de los niveles físico y de enlace (nivel de hosts a red) y su definición (si la hay) en esta arquitectura.					
Evaluar el funcionamiento del nivel de Internet, en el que los hosts introducen paquetes en la red, los cuales viajan independientemente del destino, pero sin garantías de entrega ni de orden.					
Evaluar la definición que provee el enrutamiento y control de congestión en el nivel del IP.					
Evaluar el funcionamiento del nivel de transporte. Esto permite que los pares en los hosts de fuente y destino puedan conversar en sus dos protocolos: TCP (Protocolo de Control de Transmisión), el cual permite que dos computadoras conectadas a Internet establezcan una conexión confiable para la entrega sin errores de un flujo de bytes; también maneja el control de flujo. Y el UDP (Protocolo de Datagrama de Usuario).					

Este protocolo es menos confiable que el TCP y no intenta establecer una conexión con una computadora remota para la entrega de mensajes discretos o para la entrega rápida, cuando ésta es más importante que la entrega garantizada.					
Evaluar el funcionamiento del nivel de aplicación. Como en OSI. No usa los niveles de sesión o presentación.					
Evaluar el funcionamiento del protocolo Telnet para terminales virtuales.					
Evaluar el funcionamiento del SMTP (Protocolo Simple de Transporte de Correo)					
Evaluar el funcionamiento del FTP (Protocolo de Transferencia de Archivos)					
Evaluar el funcionamiento del SNMP (Protocolo Simple de Administración de Red)					

Análisis del funcionamiento de los protocolos kernel

Evaluar y calificar el cumplimiento de los siguientes aspectos	**Excelente**	**Bueno**	**Regular**	**Mínimo**	**No cumple**
IP.					
ICPM (Protocolo de Mensajes de Control en Internet).					
TCP.					
UDP.					
FTP.					
SMTP.					
SNMP.					
DNS (Servicio de Nombres de Dominio).					
Telnet.					
Análisis de otros protocolos de transmisión de una red.					
Análisis del funcionamiento del método de transmisión de datos CSMA/CD (Acceso Múltiple por Percepción de Portadora con Detección de Colisiones).					

Evaluación de la instalación física de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del diseño arquitectónico de las instalaciones de la red.					
Análisis de los elementos de enlace y cableado de la red.					
Análisis del mantenimiento físico, correctivo y preventivo de los foros donde están las instalaciones de la red.					
Análisis de la instalación, el funcionamiento y mantenimiento de las tarjetas que configuran la red.					
Análisis de la instalación, el funcionamiento y mantenimiento de los servidores y terminales de la red de la empresa.					

Evaluación de los elementos de expansión de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de los aspectos técnicos de la red de cómputo.					
Análisis de los estándares de redes locales, según la referencia y formatos que se utilicen para el funcionamiento de la red de la empresa.					
Modelo de Referencia OSI.					
Norma IEEE 802.					
Métodos de acceso CSMA/CD.					
IPX.					
SPX (Secuenced Packet Exchange)					
Análisis del funcionamiento técnico de los sistemas operativos de la red.					

Evaluación de la administración y el control de la red de cómputo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del acceso a la información institucional por áreas, privilegios y niveles de operación de los datos.					
Análisis de los sistemas y software.					

Análisis del cambio periódico de niveles, privilegios y contraseñas de acceso al sistema.					
Análisis de los reportes de incidencias, contingencias y circunstancias que afecten el funcionamiento de la red, de su información o software.					
Análisis de la atención y rapidez de respuesta para satisfacer las necesidades informáticas de los usuarios del sistema.					
Análisis de la existencia, acatamiento y actualización de las políticas y reglamentos de uso de los sistemas computacionales de la red.					
Análisis del cumplimiento de la actividad informática de los servidores, terminales, sistemas y programas de cómputo utilizados para satisfacer las necesidades de los usuarios del sistema.					

Análisis de la atención y solución de algunas diferencias en la operación entre redes

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
La clase de servicio. Evaluando su orientación permanente a la conexión y/o no conexión de las terminales de servicio, de acuerdo con las políticas del área de sistemas.					
El funcionamiento adecuado de los protocolos de la red.					
El funcionamiento correcto de direcciones, ya sean por un nivel o jerárquicas.					
El manejo de los tamaños de paquetes que se manejan en la red, según su máximo.					
El control de errores para la entrega confiable y en orden o sin orden de la información que se transmite en la red.					
Control del flujo y de velocidad de transmisión de los datos de la red.					

Control de la congestión del manejo de la información, transmisión y protocolos de la red.					
Administración y control de la problemática de seguridad de la red, la información, los usuarios, los sistemas computacionales y de las instalaciones físicas.					
Contabilidad de los tiempos de uso del sistema, ya sea por conexión de las terminales, por paquete, por byte, por proceso o por cualquier otra actividad que se realice en los sistemas de la red.					
Evaluación de la seguridad y protección de la red y de los activos informáticos de la empresa.					
Análisis del funcionamiento de los mecanismos de control de acceso a las instalaciones, información y software institucionales.					
Análisis de la prevención de accesos múltiples, sin permisos, dolosos y de todas aquellas acciones para ingresar al sistema sin la autorización correspondiente.					
Análisis del procesamiento de información en los sistemas de red.					
Análisis de la administración y el control de la asignación de los niveles de acceso, privilegios y contraseñas para los usuarios para ingresar al sistema y tener acceso a la información.					
Análisis del monitoreo de las actividades de los usuarios.					
Análisis de las medidas correctivas y preventivas para evitar la piratería de información, software, activos informáticos y consumibles del área de sistemas.					
Análisis de la realización, actualización y custodia de los respaldos de sistemas e información que se procesan en la red.					
Análisis de las auditorías periódicas del funcionamiento de la red.					

Análisis de las medidas preventivas y correctivas para erradicar los virus informáticos de la red.					
Análisis del establecimiento de las barreras físicas y lógicas para proteger los accesos de intrusos, piratas y hackers informáticos y cualquier otra intromisión, accidental o dolosa.					

Evaluación del uso y funcionamiento adecuado del software de la red

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de los sistemas operativos para el funcionamiento de la red.					
Análisis de los lenguajes y programas de desarrollo de la red.					
Análisis de los programas y paquetes de aplicación de la red.					
Análisis a las utilerías y bibliotecas de la red.					
Análisis de la disponibilidad de licencias y permisos de instalación del software de la red.					
Análisis de la actualización informática y de los proveedores de sistemas de la red.					
Análisis del diseño de nuevos proyectos informáticos para el funcionamiento de la red.					
Análisis de la actualización tecnológica del software desarrollado en la empresa y del que se encuentra en el mercado.					
Análisis de la administración y el control de las utilerías y bibliotecas para el funcionamiento adecuado de la red.					
Análisis de las utilerías para el funcionamiento del software y juegos no autorizados (piratas).					
Evaluación del mantenimiento de la red.					

Análisis de los reportes y servicios de mantenimiento correctivo y preventivo de la red.					
Análisis de las bitácoras y estadísticas de incidencias de la red.					
Análisis de las estadísticas de incidencias, descomposturas, caídas del sistema, colisiones, pérdidas de información y demás detalles que repercuten en la operación de la red.					

Levantamiento de inventarios a fin de hacer un recuento de los bienes informáticos destinados al funcionamiento de la red y del área de sistemas

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Inventarios de los componentes de las redes de cómputo de la empresa, contemplando servidores, terminales, cableados, componentes y demás bienes informáticos que integran la red, así como los fabricantes, marcas, modelos, procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables del resguardo y todos los demás aspectos relacionados con el inventario de la seguridad de estos equipos.					
Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, así como de las licencias, resguardos, originales, copias autorizadas y copias pirata, a fin de valorar la protección y custodia de dichos sistemas.					
Inventario de la seguridad y protección de la información y de los datos del sistema de red.					
Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, a fin de valorar su protección y uso.					
Inventario de los accesos a los sistemas de redes, así como del					

acceso a la información que se maneja en ellos y los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o de equipos mayores en red.					
Inventario de las instalaciones físicas de las redes, a fin de evaluar los accesos establecidos para la protección de los bienes informáticos del área de sistemas, así como su uso.					
Inventario de configuraciones, protocolos, tarjetas y demás características técnicas del funcionamiento de los sistemas de red.					
Inventario de las normas, políticas, reglamentos y medidas preventivas y correctivas del área de sistemas, a fin de evaluar la seguridad establecida para satisfacer las necesidades de protección de la función informática.					
Otros inventarios relacionados con la seguridad, protección y salvaguarda de los bienes informáticos del área de sistemas.					

Apéndice D

Lista de verificación para el hardware de la computadora

Tarjeta madre del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, tipo, versión del BIOS, configuración y componentes.					
Arquitectura, componentes y características de la tarjeta madre.					
Conjunto de chips.					
Ranuras de expansión para bus.					
Ranuras de expansión tipo PCI.					
Ranuras de expansión tipo ISA.					
Capacidad máxima en RAM.					
Ranuras de expansión de memoria (SIMM y DIMM).					
Puertos paralelos, seriales y para ratón.					
Socket para multiprocesadores.					
Bahías para unidades accesibles en parte frontal e interna.					
Capacidad del voltaje de la fuente de energía.					
Capacidad máxima en ROM, EROM y EPROM.					
Conexiones periféricas.					

Procesador

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, marca, tipo, configuración y características.					
Velocidad de procesamiento en MHz.					
Máxima memoria en RAM del sistema.					
Memoria caché y RAM externa.					
Coprocesador matemático.					
Conjunto de chips (fabricante, modelo, capacidad y características).					
Administrador de memoria.					

Unidades adicionales, características, interfaz y capacidad

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Unidades de discos flexibles.					
Discos duros (fabricante, capacidad, características y número).					
Unidades de CD-ROM, DVD, CD-R (modelo y velocidad).					
Unidades de cinta.					
Dispositivos multimedia: sonido, tarjetas, bocinas, tarjeta multimedia y sintetizador, bocinas, micrófono y vídeo.					
Fax-módem (marca, modelo, velocidad en Kbps).					
Soporte para gráficos (fabricante, capacidad en RAM e interfaz).					
Monitor (fabricante, modelo, tamaño y características).					
Teclado, ratón, joystick.					

Tarjetas adicionales al sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Tarjeta aceleradora de gráficos.					
Tarjetas para red.					
Tarjeta para multimedia.					
Tarjeta para fax-módem.					
Tarjetas para vídeo.					
Otras tarjetas a través de extensiones del sistema.					

Periféricos externos asociados al sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Impresoras (fabricante, modelo, tamaño y características).					
Sistemas de videoconferencia (fabricante, modelo, alcance, nitidez y características).					
Escáner y dictador de textos.					

Aprovechamiento y utilidad de cada uno de los componentes internos y periféricos del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Monitor, teclado, ratón y unidad de disco flexible.					
CD-ROM, CD-RW, DVD y disco duro.					
Conexiones de periféricos, de conectividad y de comunicación.					

Aprovechamiento y utilidad del sistema computacional

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Capacidad para el crecimiento del sistema.					
Calidad de los componentes del sistema (fabricante, marca y características).					
Obsolescencia y durabilidad del equipo (sistema y componentes).					
Garantía y soporte del fabricante.					

Mantenimiento básico para los sistemas

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Mantenimiento preventivo y correctivo (frecuencia y resultados).					
Sistemas reguladores de corriente y no-breaks.					
Instalaciones y conexiones eléctricas y de tierra.					
Protección del medio ambiente contra humedad, polvo y estática.					

Lista de verificación para las características del software

Evaluación al sistema operativo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricante, características y operabilidad.					
Plataforma y ambientes de aplicación.					
Licencias y permisos.					
Versión, actualizaciones, cambios e innovaciones.					
Manuales e instructivos técnicos, de operación, de programación y demás documentación relacionada con el funcionamiento del lenguaje.					
Facilidad para la administración del sistema operativo.					
Sistemas, rutinas y programas para la seguridad y protección de los datos y del sistema operativo.					
Tecnología de aprovechamiento.					
Compatibilidad y escalabilidad con otros sistemas operativos.					
Ventajas y desventajas.					

Evaluación de los lenguajes de desarrollo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad del lenguaje.					
Plataforma y ambientes de aplicación y desarrollo.					
Versión, actualización y utilidad para el sistema.					
Facilidad de compilación y traducción al lenguaje de máquina.					
Uso y generación de códigos y programas fuente, seudocódigos, programas objeto y programas ejecutables.					
Bibliotecas, herramientas y utilerías para programación.					
Facilidad de programación y desarrollo.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.					
Administración del lenguaje.					
Sistemas para la seguridad y protección de los datos y del propio lenguaje.					
Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otras plataformas y lenguajes.					
Ventajas y desventajas.					
Requerimientos de capacitación y especialización.					

Evaluación de los programas de desarrollo

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad.					
Plataforma y ambientes de aplicación y explotación.					
Versión, actualización y utilidad para el sistema.					
Licencias y permisos.					
Facilidad de traducción, comunicación y compilación con lenguaje de máquina.					
Bibliotecas, herramientas y utilerías para programación.					
Programas para bases de datos.					

Facilidad de programación (visual y de codificación).					
Uso y generación de programas fuente, programas objeto, programas gráficos y programas ejecutables.					
Compatibilidad, exportabilidad y escalabilidad con otros lenguajes y programas.					
Sistemas para la seguridad y protección de los datos y del propio programa.					
Administración del programa de aplicación.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.					
Requerimientos de capacitación y especialización.					
Facilidad de programación, compatibilidad, escalabilidad y desarrollo con otros sistemas, plataformas, lenguajes y programas.					
Ventajas y desventajas.					

Evaluación de los programas y paquetería de aplicación y explotación

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Fabricantes, características y operabilidad de programa.					
Ambiente de aplicación y uso.					
Versión, actualización y utilidad para el usuario.					
Licencias y permisos.					
Bibliotecas y utilerías de apoyo.					
Compatibilidad, exportabilidad y escalabilidad con otros programas y paqueterías de aplicación, de desarrollo o con el sistema operativo.					
Requerimientos de capacitación y especialización.					
Paqueterías y programas desarrollados internamente.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento del programa.					
Ventajas y desventajas de los programas y paqueterías de aplicación.					

Evaluación de la administración del software para aplicaciones

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Paqueterías y programas integrados (Office y SmartSuite, por ejemplo).					
Programas y paqueterías para aplicaciones de escritorio (hojas de cálculo, bases de datos, procesadores de texto, agendas y presentaciones).					
Programas y paqueterías para gráficos, diseño, presentaciones, publicaciones, autoedición y multimedia.					
Programas y paqueterías de negocios y productividad.					
Programas y paqueterías para comunicación y red.					
Aplicaciones y utilerías para Internet.					
Aplicaciones para la administración de redes, cliente/servidor y sistemas mayores.					
Manuales e instructivos de instalación, operación, técnicos, de programación y demás documentación para el funcionamiento y uso del programa.					
Otro software para aplicaciones y productividad.					

Evaluación de las utilerías para el funcionamiento del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Utilerías para el archivo de información.					
Utilerías para la compresión de datos.					
Utilerías para la administración del sistema.					
Utilerías para la administración del sistema Windows.					
Utilerías y bibliotecas para el manejo de redes					
Utilerías para Internet y telecomunicaciones.					
Otras utilerías para el manejo del sistema.					

Lista de verificación para el diseño lógico del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Evaluación de los componentes lógicos del sistema operativo, de desarrollo, de comunicaciones, bases de datos y de los programas de aplicación.					
Características lógicas del funcionamiento del hardware, software, periféricos, instalaciones y componentes asociados al sistema.					
Evaluación de los procesos lógicos para la captura y procesamiento de datos y elaboración de informes.					
Evaluación de la arquitectura y configuración lógicas (internas y externas) del sistema, así como de sus periféricos y archivos.					
Evaluación del funcionamiento de las capas OSI y de los protocolos de comunicación de datos del sistema.					
Evaluación de los componentes lógicos del sistema para las capas y protocolos de comunicación entre datos y archivos.					
Evaluación de las aplicaciones lógicas para el desarrollo y la programación de nuevos sistemas.					
Evaluación de las aplicaciones lógicas para los métodos de accesos, consulta y operación del sistema.					
Evaluación de la administración y control de los niveles lógicos de acceso para los administradores, operadores y usuarios del sistema, así como de su uso y explotación.					
Evaluación de los métodos y sistemas lógicos para la seguridad y protección de lenguajes, programas, paqueterías, utilerías y demás software institucional.					
Evaluación de las aplicaciones de los esquemas de seguridad lógica para protección de accesos, privilegios y manejo de las bases de datos y respaldos de información.					

Lista de verificación para el diseño físico del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Evaluación de la arquitectura interna y configuración física del sistema computacional, así como de sus equipos periféricos, componentes e instalaciones.					
Evaluación de la arquitectura externa del área de sistemas y de la configuración física del sistema computacional, mobiliario, equipos e instalaciones.					
Evaluación de los componentes físicos del sistema, así como de sus periféricos y equipos complementarios que permiten su funcionamiento adecuado.					
Evaluación del diseño físico de los circuitos, compuertas y cableado interno y externo del sistema computacional.					
Evaluación de las instalaciones eléctricas, de comunicación de datos y de comunicación telefónica del sistema computacional.					
Evaluación de la administración y control de los métodos de acceso, seguridad y protección física del área de sistemas, así como de la seguridad de los administradores, operadores y usuarios del sistema, de la información y del propio sistema computacional.					
Evaluación de la distribución física del mobiliario, equipo y sistemas.					

Evaluación de los periféricos más comunes del sistema

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Teclado y ratón del sistema: marca, modelo, ergonomía, utilidad, durabilidad y demás características.					
Monitores: marca, modelo, características, aceleradores de gráficos, tarjetas de expansión y funcionamiento.					
Impresoras: marca, modelo, características, velocidad de impresión, búferes, compatibilidad, manejo de papel y tamaño/peso.					
CD-ROM: velocidad de lectura/acceso, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad de sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI y software para respaldo.					

CR-RW: velocidad de lectura/grabación, velocidad de lectura/acceso, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad con sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI, tecnología para grabación de copia, software para funcionamiento, compatibilidad y multimedia.					
DVD: velocidad de lectura/grabación, velocidad de acceso/lectura, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad con sonido, imágenes y datos, soporte multimedia, compatibilidad DVD/CD-ROM e interfaz IDE/SCSI.					
Fax-módem: velocidad de acceso (Mbps), software de soporte, compatibilidad y protocolos de comunicación.					
Otros periféricos.					

Lista de verificación para la administración de accesos

Evaluar y calificar los siguientes aspectos:	**Excelente**	**Bueno**	**Regular**	**Deficiente**	**No cumple**
Evaluación de los estándares e instrucciones de operación y manipulación para el procesamiento de datos, de acuerdo con el propio sistema y su software.					
Evaluación de la estandarización del uso de sistemas operativos, lenguajes, programas y paqueterías para el procesamiento de información en el sistema.					
Evaluación de los procesos lógicos y físicos para el procesamiento de datos.					
Evaluación de los procesos en línea, en lote, multiprocesamiento y procesos compartidos en el sistema.					
Evaluación de la administración y control de la frecuencia, volumen, repetitividad e incidencias en los procesamientos de datos y operaciones lógico-matemáticas de las actividades que se realizan en el sistema.					
Evaluación de la administración centralizada y descentralizada de sistemas para el procesamiento de información.					

Lista de verificación para la administración y los controles de almacenamiento.					
Evaluación del diseño de archivos, bases de datos y medios establecidos para el almacenamiento de información de la empresa.					
Evaluación de la administración y control de archivos de información del área de sistemas y de la empresa.					
Evaluación de los planes y programas de prevención de contingencias relacionadas con el manejo de la información en el área de sistemas.					
Evaluación de la administración y control de respaldos de información y de datos del sistema, así como de los programas institucionales para el manejo de los archivos del centro de cómputo.					
Evaluación de la administración y control de la seguridad y protección de respaldos de información y de datos.					
Evaluación de las normas, políticas y procedimientos para el almacenamiento, custodia, protección y seguridad de la información del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales.					

Lista de verificación para la administración de los controles de seguridad del sistema computacional

Evaluar y calificar los siguientes aspectos:	Excelente	Bueno	Regular	Deficiente	No cumple
Evaluación de los métodos, rutinas de programación, procedimientos y medidas de seguridad y protección de los sistemas operativos, lenguajes, programas, paquetes, utilerías y demás software del sistema computacional.					
Evaluación de los métodos, rutinas de programación, procedimientos y medidas de seguridad y protección de los componentes físicos (internos y externos) del sistema computacional, como son los periféricos, dispositivos asociados y demás componentes físicos.					
Evaluación de las rutinas de programación, procedimientos y medidas de seguridad y protección de la información que se procesa en el sistema computacional.					

Evaluación a los métodos, procedimientos y sistemas de administración y control para los accesos (lógicos y físicos), uso, consulta, captura de datos y modificación de información del sistema computacional del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.					
Evaluación de los métodos, procedimientos y sistemas de administración y control para los accesos (lógicos y físicos) al procesador, terminales, programas e información del sistema computacional.					
Evaluación de la administración y control de los niveles de acceso, privilegios, permisos y contraseñas para los administradores, operadores, usuarios, fabricantes, proveedores y desarrolladores ajenos al área de sistemas.					
Evaluación de los métodos, procedimientos y sistemas de administración y control para los accesos remotos al sistema computacional, al procesador, a las terminales y a los programas e información del área de sistemas por medio de redes, Internet, intranet, fax-módem, redes virtuales y demás comunicación externa.					
Evaluación de los métodos, procedimientos y sistemas de administración y control para la protección contra virus informáticos, hackers y personas ajenas al sistema computacional de la empresa.					
Lista de verificación para la administración de los controles de seguridad del sistema computacional.					
Evaluación de la existencia, difusión, acceso y uso de manuales e instructivos del usuario, de operación, técnicos, de procedimientos, de elaboración de proyectos informáticos, de programación y los demás manuales e instructivos para el manejo de los sistemas de la organización.					
Evaluación de la difusión y uso de metodologías y estándares para el desarrollo de nuevos sistemas en la organización.					
Evaluación de la existencia, difusión y uso de estándares para el uso y programación de sistemas operativos, lenguajes, programas y paqueterías de desarrollo y aplicación de la empresa.					

Apéndice

E

Lista de verificación de auditoría alrededor de la computadora

Evaluación de la administración del software de la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Lenguajes y programas de desarrollo, aplicaciones y explotación del software institucional del área de sistemas y del software de las demás áreas de la empresa que cuenten con sistemas.					
Especificaciones de acceso y uso de los datos e información del sistema, así como de los procesos y operación del propio sistema.					
Estándares y métodos de entradas de datos y salidas de información.					
Estándares para la operación y manipulación de datos del sistema.					
Formas de procesamiento de información y procesos de datos en línea o lote.					
Administración de archivos, programas e información institucional.					
Medidas para evitar la piratería de software, así como la instalación de programas ilegales en el área de sistemas y en las demás áreas de la empresa que cuenten con sistemas.					
Administración y control de las licencias, resguardos y custodia del software institucional.					
Manuales e instructivos de operación, técnicos, de procedimientos, así como de las instalaciones y demás documentación relacionada con el funcionamiento del sistema.					
Metodologías y estándares para el desarrollo de nuevos sistemas.					
Estándares de programación y documentación de sistemas.					
Adquisición, desarrollo e instalación de nuevos sistemas computacionales.					
Mantenimiento preventivo y correctivo del sistema computacional, del hardware, software, de la información y demás componentes de los sistemas de la empresa.					

Evaluación de la configuración física del área de sistemas de la empresa

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Configuración, ubicación y adecuación de las áreas físicas del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas, en relación con el aire acondicionado, pisos falsos, iluminación, instalaciones y demás componentes físicos para el bienestar y comodidad de los usuarios de sistemas.					
Configuración del sistema computacional, redes, procesadores, periféricos, componentes e instalaciones físicas internas y externas del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas computacionales.					
Configuración y características físicas de locales, instalaciones, mobiliario y equipos.					
Distribución de los equipos, componentes y configuración física del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas.					
Instalaciones eléctricas (tipos de cableados y conexiones, tierra física, no-breaks, reguladores de corriente, etc.), de comunicación y de datos del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.					
Medio ambiente físico del área de sistemas (sistemas de calefacción, polvo, ruido, estática, aire acondicionado, etc.) y los demás elementos ambientales que pueden influir en el desarrollo adecuado de la función informática en la empresa.					
Sistemas de acceso, seguridad y protección físicos del área de sistemas, así como la seguridad de sus activos informáticos, personal y usuarios.					
Distribución del mobiliario, equipo y sistemas.					
Usuarios de los sistemas de red, PCs individuales, de correo electrónico, grupales y de cualquier otro sistema.					
Componentes externos del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.					

Evaluación de los métodos de acceso, seguridad y salvaguarda de los activos informáticos del área de sistemas.

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Planes y programas de prevención contra contingencias en el funcionamiento de los sistemas, en la información y datos de la empresa y en los demás bienes informáticos del centro de cómputo y de las demás áreas de la empresa que cuenten con sistemas.					
Identificación de accesos, almacenamiento y custodia de la información, sistemas operativos, lenguajes, archivos y programas institucionales.					
Evaluación de controles y sistemas de seguridad, protección y salvaguarda de los activos, del personal, instalaciones, información, mobiliario y equipo del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.					
Planes contra contingencia para seguridad y protección de los programas, información, instalaciones, empleados y usuarios del sistema computacional.					
Sistemas de control de accesos lógicos al sistema y a las bases de datos.					
Sistemas de control de accesos físicos al centro de cómputo.					
Prevención y erradicación de virus informáticos.					
Sistemas de protección y de supresión de sistemas piratas y juegos en los sistemas computacionales de la empresa.					

Evaluación de la administración del área de sistemas

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Diseño de la estructura de organización del sistema, de las áreas de trabajo y de las funciones y líneas de autoridad y responsabilidad de funcionarios, empleados y usuarios del área de sistemas.					
Administración centralizada de sistemas, archivos y procesamiento de información.					
Administración desconcentrada de sistemas, archivos y procesamiento de información.					

Administración y control de los recursos informáticos, personal, instalaciones, mobiliario y equipo del área de sistemas y de las demás áreas de la empresa que cuenten con sistemas.					
Estándares, normas y políticas para la evaluación y adquisición del hardware, software, periféricos, mobiliarios, equipos, instalaciones y artículos de consumo para el área de sistemas.					
Estándares para la selección, capacitación y desarrollo del personal y usuarios del centro de cómputo.					
Supervisión, coordinación y control de funciones y actividades de funcionarios, personal y usuarios del área de sistemas computacionales.					
Supervisión, coordinación y control de la operación de los sistemas, equipos, periféricos e información del área de sistemas.					
Evaluación de los aspectos técnicos del sistema, en cuanto a características, configuración, procesamiento de información, componentes y demás peculiaridades de la función informática en la empresa.					
Administración y control del sistema operativo, de los lenguajes, programas y paqueterías institucionales utilizados en el sistema computacional del procesador.					
Administración y control de los sistemas de red, cliente/servidor, multiusuarios y microcómputo de la empresa.					
Administración y control de sistemas de telecomunicación de datos y teleprocesamiento de información.					
Prevención y control de la contaminación informática.					
Actualización permanente de acuerdo con los cambios computacionales y tecnologías informáticas de vanguardia.					
Diseño e implantación de estándares de operación, adquisición, capacitación, desarrollo de sistemas, accesos al sistema, procesamiento de datos y demás estándares relacionados con la administración y control del centro de cómputo.					

Evaluación de los aspectos técnicos del sistema

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Administración y control de la configuración de servidores, terminales y PCs de la empresa, en cuanto a procesadores, tarjetas madres, cableado interno y externo, componentes del sistema computacional y demás peculiaridades de los sistemas de la empresa.					
Administración y control de los sistemas operativos, lenguajes de operación, desarrollo y aplicación para la programación y explotación del sistema.					
Administración y control de los sistemas de red (LAN, MAN o WAN), sistemas mayores, cliente/servidor, multiusuarios y de PC personal.					
Determinación y aplicación de normas y estándares para la instalación de sistemas computacionales en la empresa, relacionados con los procesadores, tarjetas madre, velocidades de procesos, memorias, medios de almacenamiento secundario y demás componentes de los sistemas de la empresa.					
Administración y control de las bibliotecas del sistema, sean maestras, fuente, de parámetros, de procedimientos, de carga, de objetivos y demás, según los sistemas operativos, lenguajes y programas de dicho sistema					
Administración y control de los archivos del sistema, de los usuarios y específicos de producción, pruebas de sistemas, operación de pruebas, nuevos proyectos y resguardos de la información institucional.					
Administración y control de las bases de datos del sistema y de los usuarios, en relación con su estructura, configuración, características, lenguajes y programas, resguardos, custodia interna y externa y demás formas de administración de las bases de datos.					
Administración y control de la arquitectura de comunicación, de los sistemas de telecomunicación, teleprocesamiento, transmisión, retransmisión, interconexión y de los sistemas utilizados para la transmisión vía módem, cableado o satelital.					
Prevención, control y erradicación de la contaminación informática, piratería y virus informáticos.					

Actualización permanente de acuerdo con los cambios computacionales y tecnológicos que impactan la función informática en la empresa.					
Administración y control de los estándares, velocidades, procesadores, memorias y demás características de los sistemas computacionales de la empresa.					

Evaluación de la administración del sistema

Evaluar y calificar el cumplimiento de los siguientes aspectos:	**Excelente**	**Bueno**	**Regular**	**Mínimo**	**No cumple**
Administración estratégica de la función informática, visión, misión y objetivos del área de sistemas, así como de los planes y programas, normas, políticas, lineamientos y procedimientos para regular la actividad de sistemas en la empresa.					
Los planes, programas y presupuestos financieros que afectan la administración del centro de cómputo.					
La estructura de organización, puestos, funciones, niveles de autoridad y canales de comunicación del centro de cómputo, según su tamaño, características y sistemas de procesamiento.					
La selección, capacitación, formación, adiestramiento y contratación de funcionarios, personal y usuarios del área de sistemas.					
El establecimiento y uso de los sistemas y métodos de control para el acceso a los sistemas e información institucionales.					
La aplicación de las técnicas y métodos de dirección, supervisión, toma de decisiones, coordinación y de motivación del personal y usuarios del centro de cómputo.					
Administración de proyectos de sistemas informáticos de la empresa, así como de la adquisición, adecuación o desarrollo interno de sistemas.					
Existencia, difusión, actualización y uso de la documentación técnica y administrativa del área de sistemas, manuales de usuarios, de operación del sistema, manuales de organización, de procedimientos y de operación administrativa del área de sistemas.					
Existencia, difusión y actualización de resguardos de sistemas computacionales, licencias de lenguajes, programas y paquetes del sistema.					

Administración y control de los materiales y consumibles del área de sistemas.					
Evaluación de los perfiles de puestos del área de sistemas y cumplimiento de los requisitos del puesto.					
Análisis del entorno de los sistemas, en relación con la comunicación de las áreas de la empresa y la atención a usuarios.					
Cumplimiento de las funciones administrativas de los funcionarios del área de sistemas, en lo referente a la planeación, organización, dirección y control de las funciones informáticas de la empresa.					

El levantamiento de inventarios a fin de hacer un recuento de los bienes informáticos del área de sistemas

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Inventarios de los equipos de cómputo, contemplando las marcas, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con estos equipos.					
Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias piratas.					
Inventario del personal informático y usuarios del sistema, a fin de evaluar sus perfiles de puestos, conocimientos, características y preparación para el uso de los sistemas computacionales de la empresa.					
Inventario de bienes muebles, inmuebles, materiales y consumibles del área de sistemas.					
Inventario de los sistemas de redes, cuando el sistema esté diseñado de esta manera.					
Inventario de instalaciones físicas, protecciones, características y funcionalidad de las áreas de sistemas, contemplando su medio ambiente de trabajo, iluminación, aire acondicionado, ruidos, temperatura, estática y demás peculiaridades de su funcionamiento.					
Otros inventarios acordes a las necesidades de la auditoría.					
El diseño físico del área de sistemas y de las áreas de la empresa que cuenten con sistemas computacionales.					

El análisis y aprobación de las propuestas para la adquisición del software, hardware, periféricos, equipos adicionales, bienes muebles, consumibles y materiales diversos que permiten el funcionamiento del sistema.					
El medio ambiente de trabajo en el que se realiza la función informática de la empresa.					
La gestión administrativa de la función informática de la empresa.					
El diseño de proyectos de nuevos sistemas computacionales en el área de sistemas.					
El diseño de formatos, formas y métodos para la recopilación de información que será procesada en el sistema.					
La administración y control de los sistemas de seguridad y salvaguarda de los activos informáticos, la información, el personal y los usuarios del sistema.					
La administración y control de accesos a las instalaciones del área de cómputo, a los sistemas, a la información y los bienes informáticos del área.					
Todos aquellos aspectos especiales que intervienen de alguna manera en el aprovechamiento y explotación del sistema computacional y en la gestión administrativa del centro de cómputo. Con la condición indiscutible de no interferir directamente en el uso del equipo de cómputo.					

Apéndice

F

Lista de verificación de auditoría ergonómica

El sistema visual: *el estudio de los efectos del trabajo en los ojos y la visión en general; asimismo, el estudio de la iluminación, las luminarias y los deslumbramientos.*

El sistema muscular-esquelético: *el estudio de la afectación del trabajo en el tronco, tórax, cuello, cabeza, columna vertebral, espalda, brazos, manos, dedos, piernas y pies, a causa de las posturas que adoptan los usuarios, debido al mobiliario, las herramientas y la computadora.*

El ambiente laboral del centro de cómputo: *concretamente, el mobiliario, equipo, la iluminación, el aire acondicionado y los demás elementos del área de trabajo.*

Se supone que los anteriores son los factores que más influyen en los problemas relacionados con la salud de los usuarios de sistemas computacionales. Por ello, el auditor de sistemas debe realizar el análisis a partir de esta división fundamental. En estos aspectos es donde se supone mayor incidencia de este tipo de problemática, por lo que es ahí donde se debe enfocar la auditoría. Por lo tanto, analizaremos el impacto en la salud de los usuarios tomando en cuenta los siguientes factores:

- Las repercusiones de los sistemas en la salud visual de los usuarios.
- Las repercusiones en los músculos y huesos de la espalda, tronco, tórax, cuello, cabeza y columna vertebral.
- Las repercusiones en los músculos y huesos de brazos, manos y dedos.
- Las repercusiones del ambiente del área de sistemas en la salud del usuario.
- Las consecuencias del diseño e instalación del área de sistemas en la salud física y emocional de los usuarios, así como su impacto en la actividad informática de la organización.
- El impacto del diseño ergonómico (o de la falta de éste) en el desempeño del trabajo y en el bienestar de los usuarios, así como en su comodidad durante su estancia en el área de sistemas.
- La atención (o desatención) que los directivos, empleados y usuarios del área de sistemas de la empresa ponen en el estudio de esta problemática.
- La afectación de los estudios ergonómicos (o de la carencia de ellos) en el diseño de los centros de cómputo, en el mobiliario y equipo destinado a los usuarios.

A continuación presentaremos gráficas relacionadas con estos puntos, las cuales se explican por sí mismas:

Auditoría de las repercusiones de los sistemas computacionales en la salud visual del usuario

Partiendo del análisis de la figura de la página 670, podemos observar la afectación de la vista del usuario de sistemas ya que, como se desprende del estudio, se registran

ciertos problemas de reflexión o deslumbramiento, los cuales pueden influir en la salud visual de quienes utilizan computadoras como herramientas de trabajo.

El auditor de sistemas debe tomar en cuenta los riesgos de deslumbramiento ocasionados por las luminarias y fuentes de iluminación que estén sobre la pantalla y los documentos, así como las fuentes de iluminación que emanan de la pantalla. Lo siguiente puede darnos una idea de las serias consecuencias que pueden tener estos aspectos de la iluminación en los usuarios de los sistemas.

- Analizar si se cumple con la documentación de las actividades de sistemas y cómo se acatan los elementos fundamentales de las normas ISO-9000 en ese renglón.
- Analizar si existen afectaciones en la salud visual de los usuarios de los sistemas computacionales, y determinar si existen medidas preventivas para evitarlas y medidas correctivas para solucionarlas.
- Analizar las repercusiones recientes y pasadas en la salud visual de los usuarios, a fin de evaluar las acciones preventivas y si las soluciones a esas repercusiones son favorables para la salud de los usuarios.
- Analizar si se consideraron los siguientes aspectos en el estudio inicial, al adquirir, diseñar e instalar los sistemas computacionales en la organización:
  - Que se haya cumplido con los estudios relacionados con el efecto de los sistemas computacionales en la salud de los usuarios, y que dichos estudios estén documentados.
  - El análisis del uso de las pantallas de las computadoras, de acuerdo con las características de las pantallas, sus componentes y demás características ergonómicas.
  - El análisis de la iluminación del área de trabajo, el color de las pantallas, paredes, hojas y demás aspectos relacionados con la iluminación del lugar de trabajo, a fin de hacerlo más seguro y cómodo.
  - El análisis del campo visual horizontal y vertical de los usuarios y de la distancia del usuario a la pantalla y sus ángulos visuales.
  - El estudio del impacto visual en los usuarios de los sistemas, antes de instalar el centro de cómputo.

Evaluación de las repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, nuca, piernas y pies a causa de la posición que adoptan los usuarios

Mediante el análisis de esta gráfica podemos observar cómo afectan a los usuarios de sistemas, y de cualquier otro mobiliario y equipo de oficina, las posiciones que adoptan al sentarse. Estas posturas pueden repercutir, en forma parcial o total, temporal o permanente, en la columna y la espalda, el tórax y tronco, piernas, pies, brazos y, en general, en todo el cuerpo del usuario.

- En la figura de la página 671, podemos observar 10 posiciones que adoptan los usuarios al sentarse frente a la computadora y cuál es la afectación directa en la columna vertebral. Asimismo, podemos analizar e identificar estas posiciones que adoptan los usuarios de sistemas, la frecuencia con que las adoptan y si existen medidas preventivas para evitarlas
- Analizar si la constante incidencia de estas posiciones puede repercutir en la salud muscular-esquelética del usuario, ya sea en forma parcial o total, temporal o permanente y leve o grave.
- Analizar si se han tomado las medidas preventivas o correctivas para evitar estos vicios de postura.
- Analizar globalmente el problema de las posturas de los usuarios, para comprobar los siguientes factores:

  — ¿Con qué frecuencia e intensidad repercute en la salud del usuario la posición que adopta frente a la computadora?
  — Si existen estudios médicos especializados sobre los efectos actuales y futuros en la salud de los usuarios.
  — Si, a partir de tales estudios, se han diseñado y se cumplen las medidas preventivas y correctivas para solucionar estos problemas.
  — Si existen investigaciones en la empresa sobre las causas de estos vicios de postura de los usuarios de sistemas, y si se definen acciones para crear conciencia sobre este riesgo.
  — Si existen muebles de diseño ergonómico para evitar estos vicios de postura.

- Verificar que existan estudios en las áreas de sistemas de la empresa sobre los efectos de los sistemas en la salud de los usuarios.
- Analizar si esta afectación de la salud muscular-esquelética es producto de las deficiencias del diseño del mobiliario que se utiliza en el centro de cómputo.
- Analizar si en el proyecto de un centro de cómputo existen los estudios antropométricos del usuario promedio nacional, que permitan identificar las posibles repercusiones en la salud muscular-esquelética de los usuarios.
- En caso de que no existan estudios de este tipo, investigar si se debe a que se desconoce la forma de realizarlos, o a que no se tomaron en cuenta esas necesidades al adquirir el mobiliario.
- Investigar con qué efectos y con qué frecuencia se presentan esas repercusiones en la salud de la espalda, columna vertebral, tórax, cuello, cabeza, nuca, piernas y pies del usuario, ya sea por la posición que adopta al estar en contacto con las computadoras o por el diseño del mobiliario del centro de cómputo. Evaluar ambos casos.
- Analizar, como complemento de la evaluación de la existencia o carencia de los estudios antropométricos, la periodicidad de otros estudios médicos traumatológicos de las afectaciones sobre una población seleccionada de individuos, con mobilia-

rio y equipo diseñado en forma ideal, a fin de comparar esa población con otra población de individuos que seguirán trabajando en la forma actual, sin ninguna mejora en las condiciones de muebles y equipos para el uso de computadoras.

- Evaluar si existen los siguientes elementos:
  - — La recopilación de información entre los usuarios que siempre han utilizado la computadora con deficiencias en el mobiliario y equipo y con vicios de postura.
  - — La comprobación de las repercusiones que han tenido los sistemas en la salud de estos usuarios; precisar si se debe al uso del mobiliario y equipo que se utiliza y a la posición que se adopta. Con esta base es fácil plantear el siguiente punto.
  - — Evaluar en forma global si la posición que adopta el usuario ante la computadora se debe a defectos en el diseño del mobiliario, esto es, de la silla y la mesa, o por deficiencias y vicios del usuario.

Evaluación de las repercusiones musculares-esqueléticas de manos, muñecas, dedos y brazos del usuario

El diseño actual de los sistemas computacionales, en cuanto al uso del teclado y del ratón, difícilmente puede satisfacer las necesidades de comodidad y bienestar de los usuarios. Esto se debe a que el teclado no permite tener una distancia igual entre los dedos y las líneas de teclas, lo cual hace que las manos estén en una posición incómoda. Además, los teclados se colocan en lugares con cierta inclinación, los cuales no son muy adecuados para la posición de manos y brazos. Esto, aunado a su constante uso, llega a repercutir en la salud muscular-esquelética de manos y brazos del usuario. Para comprobar esto, basta con poner las manos abiertas sobre el teclado y darnos cuenta de la separación y distancia de nuestros dedos en cada una de las líneas de teclas. Lo mismo ocurre con la inclinación del teclado. Después de este breve análisis, sólo basta calcular la prolongada adopción de esta postura para deducir cuál será el efecto en manos y dedos, como se ilustra en la figura de la página 674.

Sin embargo, éstos no son todos los aspectos que se pueden tomar en cuenta al analizar la problemática del uso del teclado, ya que también es posible analizar la postura del antebrazo y de las manos en la altura a la que se encuentra el teclado; lo mismo ocurre con el ratón. En la figura se muestra la forma ideal de poner los brazos y manos para manejar teclado. Aunque hay que aclarar que esto depende de la altura de la mesa, la forma y altura del teclado y la distancia de las manos con respecto de la mesa.

En esa figura se observa la postura correcta de los brazos, manos y muñecas en relación con el teclado y la mesa. Pero aun así se puede notar una separación importante entre la muñeca, los dedos y el teclado. Esto es lo que repercute en el puente carpiano, lo cual afectaba principalmente a las secretarias y mecanógrafas, y ahora también a los usuarios de sistemas. Para lo cual podemos:

- Analizar si existen afectaciones en muñecas, manos, dedos y brazos de los usuarios, debido al uso del ratón y del teclado de la computadora.
- Analizar las distintas formas de teclado y ratón, con el fin de identificar el tipo de lesiones, las repercusiones y el grado de afectación que pudieran llegar a tener estas herramientas en los usuarios.
- Analizar la repercusión global que puede tener en el usuario el contacto con estos sistemas; en concreto, evaluar la posición, la distancia y las características de sillas, mesas y otro mobiliario y equipo, así como las características del teclado y del ratón.

Como complemento de esta parte de la auditoría ergonómica a este renglón, en la gráfica se presenta un análisis global más completo sobre este problema:

- Investigar si se analizaron las repercusiones del teclado y del ratón en la salud muscular-esquelética de los usuarios al diseñar el centro de cómputo.
- Evaluar en forma global si las posturas que se adoptan al usar el teclado y el ratón se deben a defectos en el diseño del mobiliario, por vicios de los usuarios o por deficiencias del diseño de los fabricantes de teclados y ratones.
- Recopilar la opinión de los usuarios que siempre han utilizado estos teclados y ratones sobre las deficiencias de fabricación del mobiliario y equipo y sobre los vicios de postura.
- Evaluar las repercusiones que tiene en la salud de los usuarios el ambiente donde se utilizan los sistemas computacionales.

Actualmente, los centros de cómputo de todas las instituciones son lugares donde se concentra la mayoría de los usuarios y, precisamente por estar concentrados los equipos, debe haber algunas medidas de carácter ergonómico que contribuyan a la comodidad y bienestar de los usuarios. Sin embargo, aunque existan dichas medidas, no siempre son las ideales ni las más deseables para desempeñar el trabajo en forma óptima. Sobre todo cuando se sospecha la carencia de estudios relacionados con el impacto ergonómico en los usuarios de estos sistemas.

También existen usuarios que utilizan la computadora en forma personal, en su casa, oficina o cualquier lugar que, muchas veces, carece de las condiciones mínimas para el uso de sistemas, y su ambiente es muy limitado. Estas condiciones también se deben evaluar, ya que pueden llegar a repercutir en la salud del usuario.

- Analizar todo lo relacionado con el ambiente que rodea al área de sistemas, por ejemplo:
  - La distribución, el uso y los efectos del aire acondicionado en los usuarios.
  - La afectación del ruido en el desarrollo del trabajo de sistemas.
  - La presencia de humedad, calor, cambios de temperatura y otros fenómenos climáticos en la arquitectura del lugar, con el fin evaluar el desempeño de las actividades de sistemas.

— La colocación del mobiliario y de todos los demás factores de higiene y seguridad que influyen de alguna manera en la realización de los trabajos del área de sistemas.
— La iluminación, el mobiliario y muchos otros aspectos del centro de cómputo que influyen en la realización de las actividades en éste.

- Analizar en forma global si existe alguna repercusión en la salud del usuario a causa del ruido, el aire acondicionado, la humedad, la arquitectura, la higiene, la seguridad y otros aspectos del ambiente donde están instalados los sistemas.
- Evaluar si estos análisis están apoyados por un estudio inicial de la ergonomía, aplicada exclusivamente al ambiente de trabajo del usuario de los sistemas, de los componentes, el mobiliario y equipo.
- Determinar si existe algún estudio ergonómico enfocado exclusivamente a la salud física de los usuarios, sin considerar otros aspectos que estudia la ergonomía, ya que no sería conveniente incluir dichos aspectos debido a lo especializado de su tratamiento.
- Realizar un análisis global del problema de los efectos de la computadora en la salud de los usuarios, así como de los efectos de los componentes de cómputo, el mobiliario y equipo, el ambiente, la iluminación del local, el ruido, los sistemas de aire acondicionado, etcétera.
- Analizar el efecto que tienen en la vista de los usuarios las pantallas, la iluminación y demás reflejos.
- Analizar las posiciones y posturas que adoptan los usuarios frente a la computadora y que repercuten en su columna vertebral, tórax, cuello, nuca y que les producen cansancio y afectaciones ortopédicas.
- Analizar las demás afectaciones físicas del ambiente, la iluminación, los sistemas de aire acondicionado, las instalaciones, el mobiliario y los demás medios que rodean el uso de sistemas.
- Evaluar el impacto que tienen estos sistemas en el desempeño y la productividad del personal que los utiliza.
- Evaluar todos los aspectos relacionados con el bienestar, la comodidad y la seguridad que proporciona el ambiente del centro de cómputo al usuario, las repercusiones que tiene dicho centro en la salud física y emocional de los usuarios, las medidas preventivas y correctivas para disminuir dichas repercusiones, y el diseño de espacios de trabajo adecuados.
- Evaluar la existencia y aplicación de los estudios relacionados con el bienestar, la comodidad y la seguridad de los directivos, empleados y usuarios de los sistemas de la organización.

Apéndice

G

Lista de verificación de auditoría ISO-9000

Evaluación del cumplimiento de los requisitos de la norma ISO-9004*

- Analizar el grado de cumplimiento de los criterios de la norma ISO-9004, a fin de evaluar si se cumple con los requisitos establecidos para obtener la certificación ISO-9000.
- Analizar si las pruebas de certificación ISO-9000 se realizan conforme a los requisitos señalados en las guías de criterios de esas normas.
- Analizar si se cumple con la documentación de las actividades de sistemas y cómo se acatan los elementos fundamentales de las normas ISO-9000 en ese renglón:
  - — La existencia y actualización de la documentación de las actividades informáticas que se realizan en las áreas de sistemas de la organización.
  - — Que estén documentados los sistemas que se han desarrollado dentro de la institución.
  - — La existencia de la documentación completa y necesaria del software de desarrollo, de aplicación y utilerías adquiridos para el área de sistemas.
  - — La existencia de manuales e instructivos de organización, operación, flujo de información y todos los demás documentos que señalen las actividades de sistemas en la empresa.
  - — La existencia y uso de documentación de estándares y metodologías para el desarrollo de proyectos informáticos.
- Analizar si las actividades informáticas se cumplen conforme están establecidas en la documentación de actividades de sistemas, de acuerdo con los lineamientos fundamentales de las normas ISO-9000:
  - — Comprobar que las acciones informáticas se estén realizando conforme se describe en la documentación de esas actividades.
  - — Evaluar el grado de cumplimiento de las actividades, conforme a lo descrito en la documentación de actividades del centro de cómputo.
  - — Evaluar que los sistemas desarrollados o adquiridos para el área de sistemas cuenten con la documentación y manuales de usuarios, de operaciones, de flujo de actividades y demás documentación en la que se pueda validar el cumplimiento de sus actividades.

* Para complementar esta auditoría, sería de mucha utilidad que el auditor utilizara los aspectos señalados en la auditoría sin la computadora (sección 12.2), la auditoría a la gestión informática del área de sistemas (sección 12.3) y la auditoría alrededor de la computadora (sección 12.5), ya que estas auditorías están muy relacionadas con lo que se busca evaluar con la auditoría ISO-9000.

- Analizar que se verifique que las actividades de sistemas se cumplan conforme se documentaron en los manuales, instructivos y demás documentación relacionada con dichas actividades, y conforme a los señalamientos fundamentales de las normas ISO-9000.
- Verificar que se cumpla con las 20 secciones establecidas para las normas ISO-9000, de acuerdo con el criterio de certificación que se utilice, ya sea ISO-9001 o ISO-9004.
- Verificar los siguientes aspectos del área de sistemas para comprobar que en la empresa se cuente con la estructura que soporte la implantación de los sistemas de calidad ISO-9000:

  — Verificar la existencia de los procedimientos, responsabilidades y recursos necesarios para que los sistemas computacionales de la empresa cumplan con estos sistemas de calidad.
  — Verificar que se conozcan y se apliquen los objetivos y políticas de calidad ISO-9000 a los sistemas computacionales de la empresa.
  — Verificar que existan los manuales de calidad ISO-9000, los procedimientos para la aplicación de la calidad y la capacitación necesaria para sujetarse a la precertificación de las normas ISO-9000.
  — Verificar que existan las actividades necesarias de directivos, ejecutivos y empleados de la empresa y del área de sistemas, a fin de cumplir con los requerimientos para el aseguramiento de la calidad en los sistemas computacionales.
  — Verificar la existencia, aplicación y cumplimiento del plan de calidad para la certificación de los sistemas computacionales de la organización.
  — Revisar que se cumpla con las normas, políticas, lineamientos y secuencia de actividades para la certificación de la calidad ISO-9000 de los sistemas computacionales de la empresa.
  — Verificar la existencia y aprovechamiento de los recursos informáticos empleados para contribuir a la certificación de sistemas ISO-9000, tanto del personal del área de sistemas como del personal ajeno a ésta, y de los recursos no humanos necesarios para evaluar la calidad.

Auditoría de los costos de certificación ISO-9000*

Evaluación del seguimiento de la certificación ISO-9000

- Evaluar si los resultados de la certificación ISO-9000 son acordes a lo esperado, así como su repercusión en el cumplimiento de las actividades informáticas de la empresa, y su aprovechamiento en dichas actividades.

* Aquí se recomienda realizar una auditoría de carácter contable, a fin de evaluar los gastos hechos para la certificación ISO-9000, o una auditoría a la gestión informática, con especial énfasis en dichos gastos.

- Analizar las acciones seguidas después de la certificación ISO-9000, y determinar si se obtuvieron mejoras en el servicio de cómputo para las áreas de la empresa.
- Valorar las opiniones de los usuarios de sistemas respecto a la aprobación o desaprobación de la certificación ISO-9000 para los sistemas computacionales de la empresa, así como sus opiniones sobre la calidad de los sistemas.
- Hacer el seguimiento de las actividades, actualizaciones y cambios que se presentan en el área de sistemas, a fin de evaluar su apego a los requisitos de la norma ISO-9000.
- Analizar la custodia y almacenamiento de la documentación utilizada en la certificación ISO-9000, y si los usuarios utilizan dicha documentación después de obtenida la certificación.
- El levantamiento de inventarios (inciso 9.5), a fin de hacer un recuento de los bienes informáticos destinados a la certificación ISO-9000 y de la documentación de actividades, sistemas y procedimientos para cumplir con la función informática de la organización.

  — Inventario de los componentes de las redes de servicio o sistemas individuales que puedan cumplir con la certificación de calidad ISO-9000; en este inventario se deben contemplar los servidores, terminales, cableados, componentes y demás bienes informáticos que integran la red, así como a los fabricantes, marcas, modelos procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo, etcétera.
  — Inventario de la documentación de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, a fin de valorar el cumplimiento de las normas ISO-9000
  — Inventario de la documentación de normas, políticas, reglamentos, medidas preventivas y correctivas del área de sistemas, a fin de evaluar el cumplimiento de los requisitos de las normas ISO-9000.

- Otros inventarios relacionados con la documentación de actividades para la certificación de los servicios informáticos de la empresa.

Apéndice H

Lista de verificación de auditoría outsourcing

Evaluación de los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios outsourcing

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
La infraestructura informática para la prestación de los servicios outsourcing.					
La administración adecuada y el control en la prestación del servicio de outsourcing informático.					
La eficiencia y eficacia de los sistemas de comunicación entre prestador y contratante de los servicios informáticos.					
La confiabilidad, veracidad, integridad, oportunidad, suficiencia y calidad con las que se procesa la información de la empresa que contrata los servicios.					
La configuración, composición e integración de los sistemas computacionales para evaluar la capacidad y suficiencia del prestador de los servicios de cómputo.					
El mantenimiento preventivo y correctivo de los servicios de cómputo, tanto del prestador como del que los contrata.					

Evaluación de la prestación de los servicios outsourcing informáticos

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Existencia del contrato de servicios outsourcing informáticos, contemplando las clausuras de servicio, seguridad, costos, tipo de servicios y todos los detalles inherentes a la prestación de la actividad informática.					
Análisis de la planeación estratégica del servicio outsourcing, en relación con:					

La administración de la prestación/recepción de servicios outsourcing informáticos

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
El cumplimiento de la misión, visión y objetivo de la actividad outsourcing informática, tanto del prestador de servicios como de quien los contrata.					
La existencia y aplicación de las estrategias, procedimientos y funciones sustantivas para proporcionar el servicio outsourcing informático.					

La existencia, aplicación y seguimiento de las políticas, normas y lineamientos que regulen la actividad informática en la empresa y en el área de sistemas.					
La existencia, difusión, seguimiento y control de la misión, visión, objetivo, políticas, normas, lineamientos y procedimientos para cumplir con la actividad y el servicio outsourcing informáticos en la organización.					

Evaluación de las estructuras de organización del área de sistemas del prestador de servicios y de la empresa receptora del servicio outsourcing informático, en cuanto a los siguientes aspectos:

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
División funcional (u otro criterio) para el servicio outsourcing informático, tanto del prestador como del receptor del servicio.					
Estructura de organización y perfiles de puestos para el servicio outsourcing informático, tanto del prestador como del receptor del servicio.					
Cumplimiento en las funciones, canales de comunicación (formales e informales), niveles de autoridad y responsabilidad de los puestos para el servicio outsourcing informático en el área de sistemas.					
Estructuras para el desarrollo de proyectos, atención a usuarios y operación de las actividades outsourcing informáticas.					

Evaluación de la administración de las funciones, actividades, tareas y operaciones del prestador del servicio para cumplir con la actividad outsourcing informática de la empresa contratante

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Existencia, difusión, cumplimiento y seguimiento de los compromisos, funciones, tareas y operaciones de la actividad outsourcing informática en el área de sistemas.					
Cumplimiento de los métodos, procedimientos, fundamentos y principios administrativos, así como de manuales e instructivos aplicables a la actividad outsourcing informática por parte del prestador de servicios.					
Evaluación de la dirección del área de prestación/ recepción de servicios outsourcing informáticos de la empresa contratante y de la empresa que presta el servicio.					

Análisis del ambiente laboral en la prestación/recepción del servicio outsourcing informático

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del estilo de liderazgo, relaciones de trabajo, jerarquías de autoridad y ejercicio de autoridad en la prestación/recepción del servicio outsourcing informático.					
Evaluación del cumplimiento de la responsabilidad en la recepción o en la prestación del servicio outsourcing informático.					
Análisis de la coordinación del personal, usuarios y recursos informáticos del área utilizados para la prestación/recepción del servicio outsourcing informático.					
Evaluación de la forma en que se ejerce y se controla la toma de decisiones para la prestación/recepción del servicio outsourcing informático.					
Análisis de la integración de grupos de trabajo para la prestación/recepción del servicio outsourcing informático, así como de las relaciones de comunicación formal (comunicación escrita, verbal, correo electrónico u otras formas de comunicación).					
Evaluación de la administración del factor humano del área de sistemas.					
Coordinación de las funciones, actividades, tareas y operaciones del personal informático destinado a la prestación/recepción del servicio outsourcing informático.					
Evaluación de la existencia y cumplimiento de los planes y programas de capacitación, adiestramiento y promoción del personal dedicado a la prestación/recepción del servicio outsourcing informático.					
Análisis de la rotación y movilidad en el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de los procesos de selección de personal para esta actividad.					
Análisis de la remuneración y prestaciones para el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de la motivación para que permanezca y progrese en esta actividad.					
Análisis de la integración de grupos de trabajo dedicados a la prestación/recepción del servicio outsourcing informático, así como de la gestión directiva de funcionarios, empleados y usuarios.					

Análisis de la asignación y cumplimiento de las funciones y actividades del personal dedicado a la prestación/recepción del servicio outsourcing informático, así como del perfil de puestos de dicho personal.					
Análisis de la existencia y aplicación de estudios ergonómicos para el personal y usuarios dedicados a la prestación/recepción del servicio outsourcing informático.					

Evaluación de la administración de los recursos informáticos no humanos del área de sistemas

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la administración del sistema computacional, en relación con el hardware, software y con las instalaciones dedicadas a la prestación/recepción del servicio outsourcing informático.					
Análisis de la administración de las telecomunicaciones, bases de datos e información del sistema computacional dedicado a la prestación/recepción del servicio outsourcing informático.					
Análisis de la administración del mobiliario, equipo, bienes materiales, consumibles y materiales de oficina utilizados en la prestación/recepción del servicio outsourcing informático, así como del manejo financiero de los bienes informáticos.					
Análisis de la administración de las adquisiciones de sistemas computacionales, hardware, software, periféricos, mobiliario, consumibles y demás implementos para la prestación/recepción del servicio outsourcing informático.					
Análisis de los planes, programas y presupuestos que afectan a la gestión financiera y contable de sus recursos dedicados a la prestación/recepción del servicio outsourcing informático.					

Evaluación de los controles informáticos del área de sistemas dedicada a la prestación/recepción del servicio outsourcing informático

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de la aplicación de los controles internos a los servicios outsourcing informáticos.					
Controles internos sobre la organización de la prestación/recepción del servicio outsourcing informáticos.					

Controles internos sobre el desarrollo de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Controles internos sobre la operación de los sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Controles sobre los procedimientos de entrada de datos, procesamiento de información y emisión de resultados con el servicio outsourcing informático.					
Controles internos sobre la seguridad en la prestación/recepción del servicio outsourcing informático.					
Evaluación de la existencia, establecimiento y uso de los estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					

Metodologías del análisis y diseño de sistemas dedicados a la prestación/recepción del servicio outsourcing informático

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis del uso de software, lenguajes y programas de desarrollo para la programación y codificación de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la elaboración y seguimiento de pruebas y simulaciones de sistemas, programas y lenguajes de cómputo dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la liberación e implementación de nuevos sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la capacitación y adiestramiento del personal y los usuarios del área de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la documentación de los sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de las adquisiciones de sistemas computacionales, componentes y periféricos dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la adquisición y consumo de materiales informáticos, componentes y materiales de oficina dedicados a la prestación/recepción del servicio outsourcing informático.					

Evaluación de la documentación y demás estándares de sistemas dedicados a la prestación/recepción del servicio outsourcing informático

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Existencia, difusión, préstamo y uso de los manuales de usuarios, manuales técnicos de los sistemas, de capacitación, de operación y bitácoras de nuevos proyectos.					
Análisis de la documentación de pruebas y simulaciones de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Análisis de la actualización de manuales e instructivos de sistemas computacionales, manuales de organización, de procedimientos, de operación y demás documentación normativa del área de sistemas dedicados a la prestación/recepción del servicio outsourcing informático.					
Evaluación de la forma en que la empresa contratante recibe el servicio outsourcing.					

Inventarios de la prestación de servicios outsourcing informáticos

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Inventarios de los componentes de las redes de cómputo o sistemas individuales de la empresa receptora de los servicios outsourcing informáticos, contemplando dentro de sus instalaciones.					
Inventario de los servidores, terminales, cableados, componentes, medios de comunicación y demás bienes informáticos que integran la red de prestación de servicios outsourcing informáticos instalada en la organización contratante.					
Inventario de la configuración de los sistemas individuales con los que se presta el servicio outsourcing informático en la empresa contratante, contemplando: fabricantes, marcas, modelos, procesadores, tarjetas madre, velocidad, configuración, componentes, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relativos al inventario de estos equipos para recibir el servicio outsourcing informático.					
Inventario del software de desarrollo y de aplicación que está a disponibilidad de los usuarios que reciben el servicio outsourcing informático, a fin de comprobar que se satisfagan las necesidades informáticas de la empresa receptora de dicho servicio.					

Inventario del personal destinado a la recepción de los servicios outsourcing informáticos en la organización receptora, así como del personal informático del prestador de los servicios.					

Evaluación de la recepción de los servicios outsourcing informáticos

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de la existencia y cumplimiento del contrato del servicio outsourcing informático, contemplando las clausuras de servicio, seguridad, costos, tipo de servicios y todos los detalles inherentes a la prestación de la actividad informática.					
Análisis de la administración estratégica de la prestación/recepción de los servicios outsourcing informáticos, en relación con:					
Objetivo general.					
Misión.					
Visión.					
Estrategias.					
Evaluación de la administración del factor humano del área de sistemas.					
Coordinación de las funciones, actividades, tareas y operaciones del personal informático destinado a la prestación/recepción del servicio outsourcing informático.					
Evaluación de la existencia y cumplimiento de los planes y programas de capacitación, adiestramiento y promoción del personal dedicado a la prestación/recepción del servicio outsourcing informático.					
Análisis de la rotación y movilidad en el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de los procesos de selección de personal para esta actividad.					
Análisis de la remuneración y prestaciones para el personal dedicado a la prestación/recepción del servicio outsourcing informático, así como de la motivación para que permanezca y progrese en esta actividad.					
Análisis de la integración de grupos de trabajo dedicados a la prestación/recepción del servicio outsourcing informático, así como de la gestión directiva de funcionarios, empleados y usuarios.					

Análisis de la asignación y cumplimiento de las funciones y actividades del personal dedicado a la prestación/recepción del servicio outsourcing informático, así como del perfil de puestos de dicho personal.					
Análisis de la existencia y aplicación de estudios ergonómicos para el personal y usuarios dedicados a la prestación/recepción del servicio outsourcing informático.					

Evaluación de los sistemas, personal informático, instalaciones, comunicación y demás aspectos relativos al prestador de los servicios HelpDesk

Evaluar y calificar el cumplimiento de los siguientes aspectos:	**Excelente**	**Bueno**	**Regular**	**Mínimo**	**No cumple**
Evaluación del soporte técnico, de la asistencia y capacitación a los usuarios, así como del mantenimiento de los sistemas y la detección de incidencias de problemáticas para la solución a los reportes de los usuarios					
Análisis de la oportunidad en la atención y solución de las problemáticas reportadas por los usuarios del sistema.					
Evaluación estadística de las incidencias de mayor problemática reportadas, y valoración de los tiempos de solución a esos reportes.					
Análisis de la capacidad de respuesta del personal especializado para solucionar las problemáticas que reportan los usuarios.					
Evaluación de la comunicación en línea entre los usuarios y el servicio HelpDesk, tanto de la comunicación telefónica como en red.					
Evaluación de la eficacia y eficiencia de las formas de comunicación, ya sea telefónica, escrita, vía fax, correo electrónico o cualquier otro medio, entre el prestador del servicio y el usuario solicitante de las ayudas.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar la calidad en la atención de solicitudes de servicios.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar La oportunidad, en días u horas promedio, en que se proporciona el servicio, desde que entra la llamada hasta su solución final.					

Análisis de las bitácoras de reportes y de servicios, a fin de evaluar la capacitación técnica y psicológica para la atención a los usuarios solicitantes de servicios, aun en caso de desconocimiento del manejo elemental de los sistemas computacionales.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar la frecuencia de las incidencias y problemáticas que reportan los usuarios, evaluando estadísticamente las mayores ocurrencias, sus soluciones y las medidas para evitar que se presenten.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar la confiabilidad en la solución a los problemas reportados, en grado de aceptación y porcentaje de soluciones.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar las acciones de capacitación para los usuarios, sobre la base de los reportes de incidencias, a fin de evitar la frecuencia de los reportes.					
Análisis de las bitácoras de reportes y de servicios, a fin de evaluar las actividades en línea para la solución de las problemáticas reportadas por los usuarios					

Evaluación de las actividades técnicas para proporcionar asistencia y mantenimiento a los sistemas computacionales

Evaluar y calificar el cumplimiento de los siguientes aspectos:	**Excelente**	**Bueno**	**Regular**	**Mínimo**	**No cumple**
Análisis de los objetivos, características, componentes, conectividad y comunicación de la red para la atención en línea HelpDesk y su aplicación en la solución de las problemáticas reportadas por los usuarios del sistema.					
Análisis de las características de configuración de la red, en cuanto a topologías, tipo de red, componentes, protocolos de comunicación, servidores, terminales, instalaciones de comunicación y demás aspectos de la red utilizada para proporcionar la ayuda en línea a los usuarios.					
Análisis de los componentes internos, externos y de la arquitectura física y lógica del sistema de red, a fin de verificar que cuente con los elementos técnicos necesarios para prestar la ayuda en línea a los usuarios del sistema.					

Análisis de la confiabilidad y funcionalidad de los medios de transmisión, medios físicos, instalaciones telefónicas, de datos y de energía eléctrica que se utilizan para mantener la comunicación entre el usuario demandante de auxilio y el prestador de la ayuda en línea.					
Análisis del diseño y funcionamiento de los servidores, estaciones de trabajo, componentes, periféricos, sistemas de instalaciones, protocolos de comunicación y enlace físico de la red, a fin de evaluar la eficiencia de las comunicaciones para la ayuda en línea de los usuarios.					
Análisis del diseño y aplicación del software especializado de atención, solución, desarrollo y aplicación para atender y solucionar las necesidades de cómputo de los usuarios del sistema.					
Análisis de las utilerías, bibliotecas y demás software que se utiliza en la red.					
Análisis de la protección, resguardo y respaldo de la información de los usuarios que solicitan ayuda en línea, evaluando la ayuda y capacitación proporcionadas a los usuarios para el manejo óptimo de su información.					
Análisis de la administración y control de la red de servicios en línea, evaluando el cumplimiento confiabilidad, privilegios, niveles de acceso y contraseñas para ingresar a la red.					
Análisis de la administración y control de la red de servicios en las terminales que solicitan ayuda en línea, a fin de mantener la integridad del sistema y proporcionar la atención solicitada en dicha red.					
Análisis de la administración y control de la red de servicios en relación con el funcionamiento técnico y operativo de los sistemas de red de ayuda en línea y del software especializado de atención a usuarios y mantenimiento físico.					
Análisis de la administración y control de la red de servicios en relación con la seguridad de la red y protección de los activos informáticos de la red de servicios y de los sistemas computacionales para la atención HelpDesk, a fin de mantenerlos en condiciones óptimas para la prestación de la ayuda en línea a los usuarios.					

Levantamiento de inventarios de los bienes informáticos destinados al funcionamiento de la red de servicios para atender las necesidades outsourcing y ayuda en línea de las áreas de la empresa contratante, así como de los bienes informáticos que se pueden analizar en el funcionamiento de los sistemas que conforman la red de servicios. Realizar los siguientes inventarios:

Evaluar y calificar el cumplimiento de los siguientes aspectos:	Excelente	Bueno	Regular	Mínimo	No cumple
Inventario de los componentes de las redes de servicio outsourcing o sistemas individuales que cumplan con la prestación de servicios informáticos en la organización, contemplando los servidores, terminales, cableados y demás bienes informáticos que integran la red, así como los fabricantes, marcas, procesadores, tarjetas madre, velocidad, configuración, memorias, sistemas de almacenamiento, tarjetas adicionales, números de serie, responsables de su resguardo y todos los demás aspectos relacionados con dicho inventario.					
Inventario de los sistemas operativos, lenguajes, programas, paqueterías, utilerías y demás software institucional, incluyendo licencias, resguardos, originales, copias autorizadas y copias pirata, a fin de valorar la prestación de los servicios informáticos y la ayuda en línea con estos sistemas.					
Inventario de la seguridad y protección de la información y datos del sistema de red de servicios, a fin de evaluar la confiabilidad en el manejo de los recursos informáticos de la empresa que presta los servicios informáticos y la ayuda en línea.					
Inventario de los bienes muebles, inmuebles, materiales y consumibles del área de sistemas, para valorar su protección y uso adecuados.					
Inventario de los medios, privilegios, niveles y métodos de acceso a los sistemas de los usuarios en línea, a fin de valorar la confiabilidad en el acceso a su información y a los sistemas operativos, lenguajes, programas y demás software institucional de esas redes o de los equipos mayores en red.					
Inventario de las instalaciones físicas de las áreas que reciben y proporcionan los servicios outsourcing y ayuda en línea, a fin de evaluar la calidad, confiabilidad, control y vigilancia del uso de los bienes informáticos en las actividades outsourcing informáticas y ayuda en línea.					
Inventario de las configuraciones, protocolos, tarjetas y demás tecnología utilizada para el funcionamiento de los sistemas de red de servicios outsourcing y ayuda en línea, así como de los sistemas individuales de servicios.					

Inventarios de las normas, políticas, reglamentos, medidas preventivas y correctivas del área de sistemas, a fin de evaluar la satisfacción de las necesidades de servicios outsourcing informáticos y ayuda en línea de la empresa.					
Otros inventarios relacionados con la prestación/ recepción de los servicios outsourcing informáticos y ayuda en línea (HelpDesk) para los usuarios de sistemas de la empresa.					

Apéndice

I

Lista de chequeo de auditoría integral

Los objetivos de la auditoría externa de sistemas son:

— Realizar la auditoría con personal ajeno a la empresa, a fin de hacer una valuación y emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de sistemas.
— Evaluar el aspecto financiero, el uso de los recursos del centro de cómputo y el aprovechamiento del sistema computacional, del mobiliario y de los equipos periféricos e instalaciones.
— Evaluar el cumplimiento de estándares, políticas, normas y lineamientos que regulan las funciones y actividades de los sistemas de procesamiento de información, así como del personal y de los usuarios del centro de cómputo.

Áreas, factores y elementos que se deben auditar

— Objetivos, planes, programas y presupuestos del área de sistemas.
— Estructura organizacional, funciones y puestos del área de sistemas.
— Administración del sistema de procesamiento, periféricos, instalación, lenguajes, programas e información del centro de computación.
— Administración de los recursos asignados al centro de cómputo.
— Administración del personal y usuarios del área de sistemas, así como de las prestaciones y obligaciones de dicho personal.
— Normas, políticas, métodos y procedimientos de operación.

- Auditoría a la gestión administrativa del sistema y del centro de cómputo.
- Auditoría a la estructura de organización, funciones y actividades del sistema.
- Evaluación del desarrollo de sistemas.
- Evaluación de la operación del sistema de procesamiento de información.
- Auditoría de los sistemas, lenguajes, programas y paqueterías de aplicación y desarrollo de sistemas.
- Auditoría de los procesadores, periféricos, equipos e instalaciones del centro de cómputo.
- Auditoría de los sistemas de seguridad y de prevención de contingencias.
- Auditoría de otros aspectos de sistemas.
  — Auditoría externa integral de sistemas
  — Auditoría interna integral de sistemas

Aspectos a evaluar con la auditoría integral de sistemas

- Auditoría de la gestión administrativa del sistema y del área de informática.
- Auditoría de la estructura de organización, funciones y actividades del sistema.
- Auditoría del desarrollo de sistemas.

- Auditoría de la operación del sistema de procesamiento de información.
- Auditoría de los sistemas, lenguajes, programas y paqueterías de aplicación y desarrollo de sistemas.
- Auditoría de los procesadores, periféricos, equipos e instalaciones que hay en el área de sistemas.
- Auditoría de los sistemas de seguridad y prevención de contingencias.
- Auditoría de otros aspectos de sistemas.
- Programas de aplicaciones y explotación del software.
- Metodologías para el análisis y desarrollo de sistemas.
- Métodos de acceso, seguridad y operación del sistema.
- Configuración.
- Evaluación del diseño físico del sistema, en cuanto a:
  — Configuración del sistema, equipos e instalaciones físicas.
  — Componentes físicos del sistema, periféricos, mobiliario y equipos.
  — Características del sistema e instalaciones del centro de cómputo.
  — Instalaciones eléctricas, de comunicación y del medio ambiente del sistema.
  — Métodos de acceso, seguridad y protección física del sistema.
  — Distribución del mobiliario, equipo y sistemas.
- Evaluación del control de accesos y salidas de datos, en relación con:
  — Estándares y métodos de entradas de datos y salidas de información.
  — Especificaciones de acceso y uso de los datos e información del sistema, así como de los procesos y operación del sistema.
  — Especificaciones sobre las normas, políticas y procedimientos para el acceso de datos, el procesamiento de los mismos y la salida de información del sistema computacional.
  — Administración y control de los niveles de accesos de administradores, operadores y usuarios del sistema, así como del uso y explotación de dichos niveles de accesos.
- Evaluación del control del procesamiento de datos, en cuanto a:
  — Estándares para la operación y manipulación de datos del sistema.
  — Identificación, accesos, almacenamiento y custodia de información, archivos y programas.
  — Formas de procesamiento y procesos de datos en línea o lote y sus justificaciones.
  — Administración de la frecuencia y volumen de la operación del sistema.
- Evaluación de los controles de almacenamiento, en relación con:
  — Diseño de archivos, bases de datos y almacenamiento de información.
  — Administración de archivos, programas e información.
  — Planes y programas de prevención contra contingencias y para la custodia de la información.

  - — Administración del respaldo de información y de los programas institucionales, así como del manejo de los archivos del centro de cómputo.
  - — Evaluación de controles de seguridad.
  - — Sistemas de seguridad y protección del sistema, programas, información, instalaciones, empleados y usuarios del sistema computacional.
  - — Sistemas de control de accesos lógicos al sistema y a las bases de datos.
  - — Sistemas de control de accesos físicos al centro de cómputo.
  - — Procedimientos de acceso al procesador, terminales, programas e información.
- Evaluación de controles adicionales para la operación del sistema, en relación con:
  - — Manuales e instructivos de operación, para usuarios y de procedimientos.
  - — Metodologías y estándares para el desarrollo de sistemas.
  - — Estándares de programación y documentación.
  - — Estandarización de lenguajes, programas y paqueterías de uso institucional.
- Evaluación de la administración del área de sistemas, en relación con:
  - — Diseño de la estructura de organización del sistema, áreas de trabajo, funciones y líneas de autoridad y responsabilidad.
  - — Administración centralizada de sistemas, archivos y procesamiento de información.
  - — Administración desconcentrada de sistemas, archivos y procesamiento de información.
  - — Administración y control de los recursos informáticos.
  - — Estándares para la evaluación y adquisición del hardware, software, mobiliarios, instalaciones y artículos de consumo para el área de sistemas.
  - — Estándares para la selección, capacitación y desarrollo del personal y usuarios del área de sistemas.
  - — Supervisión, coordinación y control de funciones y actividades de funcionarios, personal del área de sistemas y usuarios de los sistemas computacionales.
  - — Supervisión, coordinación y control de la operación del sistema, equipos y periféricos.
  - — Evaluación de los aspectos técnicos del sistema.
  - — Administración y control del sistema operativo del procesador.
  - — Administración y control de lenguajes de operación, de desarrollo y de programación.
  - — Administración y control de sistemas de red, multiusuarios y de microcómputo.
  - — Administración y control de sistemas de telecomunicación y de teleprocesamiento.
  - — Prevención y control de la contaminación informática.
  - — Actualización permanente de acuerdo con los cambios computacionales.

— Diseño e implementación de estándares de operación, adquisición, capacitación, desarrollo de sistemas, accesos al sistema, procesamiento de datos y de los demás estándares relacionados con la administración y control del centro de cómputo.

Auditoría de la administración interna del área de sistemas

- Evaluación de la función del personal informático.
  — Inventario del personal informático y usuarios del sistema.
  — Análisis del perfil de puestos.
  — Sueldos, salarios y prestaciones
  — Análisis de los planes y programas de capacitación y adiestramiento.
  — Análisis de los índices de rotación y ausentismo laboral del personal del área de sistemas.
  — Análisis de la organización del trabajo.
  — Análisis de las condiciones de trabajo.
  — Análisis del estilo de dirección.
- Evaluación de la administración de los recursos físicos.
  — Inventario de sistemas computacionales.
  — Inventario de mobiliario y equipo de oficina.
  — Inventario de dispositivos periféricos.
- Evaluación de la administración de los recursos informáticos.
  — Inventario de sistemas operativos.
  — Inventario de lenguajes, programas y paquetes de desarrollo.
  — Inventario de programas y paquetes de aplicación.
  — Inventario de utilerías y bibliotecas.
  — Inventario de software institucional.
- Inventario de licencias y permisos de uso del software institucional.
  — Evaluación de la administración de la planeación de proyectos.
  — Metodologías para el desarrollo de sistemas.
  — Estándares para el desarrollo de sistemas.
  — Seguimiento del desarrollo de nuevos proyectos informáticos.
  — Análisis de la utilidad, compatibilidad y seguimiento de los nuevos proyectos de sistemas.
- Evaluación de los reportes de actividades de funcionarios, personal y usuarios del sistema.
  — Análisis de los reportes de incidencias del personal.
  — Evaluación del cumplimiento del personal.
  — Informes.
- Evaluación del control de los gastos corrientes del área de sistemas.
- Evaluación de la automatización interna.

Administración del área de sistemas

- Desempeño del personal
- Desarrollo de proyectos
- Gastos de área
- Asignación de recursos

Centros de procesamiento de datos

- Hardware
- Software
- Seguridad
- Planes contra contingencias
- Planes de modernización

Desarrollo de sistemas

- Metodología
- Planeación y control de proyectos
- Bases de datos
- Control de calidad

Sistemas de producción

- Análisis de producción
- Respaldos
- Seguridad en sistemas de producción
- Mantenimiento

Software de trabajo

- Adquisición
- Bitácora
- Instalación
- Aplicación

Control y seguridad

Bibliografía

Capítulo 1

[1] *Diccionario Enciclopédico Universal SALVAT*, Ediciones Salvat. España, 1986. Tomo III, Pág. 130.
[2] *Gran Diccionario Enciclopédico Universal*. Director Luis Rodríguez Martínez. Asuri de Ediciones. España, 1988. Tomo III, Pág. 919.
[3] *Enciclopedia Universal Ilustrada Europeo–Americana*. ESPASA-CALPE. España, 1989. Tomo VI, Pág. 1007.
[4] *Auditoría de Sistemas en Redes de Área Local*. Tesis. UVM. Plantel Lomas Verdes, de la carrera L.S-.C.A. 1994. Georgina Fernández del Toro y Mario Romero Lara. Pág. 12.
[5] *Ídem*. Pág. 18.
[6] *Enciclopedia Interactiva Santillana*, CD-ROM. Santillana Publishing Co. Inc. And Chinon America Inc. 1995. Copyright 1991-1995.
[7] *Op. Cit. Gran Diccionario Enciclopédico Ilustrado ESPASA* [...]. Tomo III, Pág. 1007.
[8] *Gran Diccionario del Saber Humano.* Varios Autores*.* Director, Gonzalo Ang. Editorial Selecciones del Reader's Digest. México, 1992. Volumen I, Pág. 190.
[9] *Diccionario Inverso Ilustrado*. Varios Autores. Director, Gonzalo Ang. Editorial Selecciones del Reader's Digest. México, 1992. Pág. 72.
[10] *Pequeño Larousse Ilustrado*. Ramón García-Pelayo y Cross. Editorial Ediciones Larousse. México, 1984. Pág. 114.
[11] *Op. Cit. Enciclopedia Interactiva Santillana* [...].
[12] *Op. Cit. Enciclopedia Universal Ilustrada* [...]. Tomo VI, Pág. 1007.
[13] *Gran Diccionario Moderno Español/Inglés Larousse.* Ramón García-Pelayo y Cross y Micheline Durand. Editorial Ediciones Larousse. México, 1984. Pág. 758.
[14] *The Multimedia Encyclopedia CD-ROM*. Grolier Electrónico Editor. 1998.
[15] *Op. Cit. Gran Diccionario Enciclopédico Universal SALVAT* [...]. Tomo III, Pág. 131.

Capítulo 2

1 *AICPA (American Institute Certified Public Accounting*; Instituto Estadounidense de Contadores Públicos Certificados).
2 *Normas y procedimientos de auditoría*, boletín 1010. IMCPAC. Instituto Mexicano de Contadores Públicos, A.C. México, 1996. Pág. 10.
3 *Enciclopedia de la Auditoría*. William F. Messier. Capítulo III, Normas de auditoría. Grupo Editorial Océano. México, 1991. Pág. 39.

Capítulo 3

1 *Diccionario Etimológico*. Libros de consulta. Fernando Corripio Pérez. Editorial Bruguera. México, 1977. Pág. 187.
2 *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 763.
3 *Op. Cit*. *Pequeño Larousse Ilustrado*[...]. Pág. 444.
4 *Ídem*. Pág. 699.
5 *Op. Cit*. *Diccionario Inverso Ilustrado* [...]. Pág. 439.
6 *Ídem.* Pág. 627.
7 *Ética*. José Armando Estrada Parra. Editorial Publicaciones Cultural. México, 1992. Pág. 15.
8 *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 439.
9 *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 1047.
10 *Op. Cit*. *Diccionario Inverso Ilustrado* [...]. Pág. 344.
11 *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 375.
12 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 145 (citando a San Agustín. Sin referencia).
13 *Ética*. José Gutiérrez Sáenz. Editorial Porrúa. México, 1978. Pág.143.
14 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 153.
15 *Ídem*. Pág. 155.
16 *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1625.
17 *Ídem*. Pág. 136.
18 *Ídem*. Pág. 822.
19 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 166.
20 *Op. Cit*. *Ética*. Gutiérrez Sáenz [...]. Pág. 161 (citando a Engels y Konstantinov, ambos con fundamentos en la filosofía Marxista, Lenin: Materialismo y empiriocriticismo. Verneaux: Historia de la filosofía moderna).
21 *Ibídem* [...]. Pág. 163 (citando a Gálvez: el pensamiento de Carlos; Konstantinov y Marx: crítica de la filosofía hegeliana del derecho).
22 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 183.
23 *Ídem*. Pág. 186 (citando a José Ferrater Mora. *Diccionario de Filosofía*. México, 1944).
24 *Op. Cit*. *Diccionario Etimológico*. [...]. Pág. 372.
25 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 93.
26 *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 121.
27 *Ídem* [...]. Pág. 1048.
28 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 95.
29 *Op. Cit*. *Ética*. Gutiérrez Sáenz [...]. Pág. 183.

30 *Op. Cit*. *Ética*. Estrada Parra. Pág. 99.
31 *Op. Cit*. *Ética*. Gutiérrez Sáenz. Pág. 101.
32 *Ídem*. Pág. 98 (citando a De finance, *Ensayo sobre el obrar humano*. Pág. 392 y Sigs.).
33 *Ídem*. Pág. 184.
34 *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 199.
35 *Auditoría, un enfoque integral*. Alvin A. Arens y James K. Loebbecke. Editorial Prentice-Hall Hispanoamericana. México, 1996. Pág. 75.
36 Estas encuestas fueron realizadas por 40 alumnos de L.S.C.A., en la Universidad del Valle de México, Plantel San Rafael. Se siguió como metodología de recopilación de datos: la aplicación de un cuestionario piloto, un cuestionario final corregido y la elección de una muestra aleatoria de personas cercanas al encuestador (universo), para hacer una recopilación de 10 cuestionarios por cada alumno participante (muestra), en diversos puntos del D.F. (cercanos al domicilio del estudiante), y con diversas condiciones sociales y económicas de los encuestados. Total: 400 cuestionarios, aplicados de 1997 a 1998
37 *Normas y procedimientos de auditoría.* Instituto Mexicano de Contadores Públicos, A. C. Editorial IMCPAC. México, 1994. Pág. 17.
38 Colegio Nacional de Licenciados en Administración, A. C. México.
39 *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1824.
40 *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 951.
41 *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1822.
42 *Op. Cit*. *Enciclopedia Universal Ilustrada ESPASA* [...]. Vol. 50. Pág. 1113.
43 *Ídem*. Pág. 446.

Capítulo 4

1 *Auditoría e informática. Estructura en evolución*. Juan Manuel Lazcano y Enrique Rivas Zwy. Editorial del I.M.C.P.A.C. México, 1988. Pág. 83 (citando a Gómez Morfín).
2 *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 471.
3 *Introducción a la teoría general de la administración*. Adalberto Chiavenato. Traducción de *Introduçao a teoria geral da administraçao*. Editorial McGraw Hill do Brasil. 1981. Pág. 55.
4 *Ídem*. Pág. 556.
5 *Contabilidad de empresas*. Biblioteca para Dirección de Empresas. W.M. Harper. Editorial EDAF, Ediciones-Distribuciones. Madrid, 1982. Pág. 227.
6 *Administración en las organizaciones. Enfoque de sistemas y de contingencias*. Fremont E. Kast y James E. Rosenzweig. Editorial McGraw Hill. Cuarta edición. México, 1985. Pág. 536.
7 *Ídem*. Pág. 539.
8 *Op. Cit*. *Contabilidad de empresas* [...]. Pág. 227.
9 *Op. Cit*. *Administración*. Pág. 543.
10 *Op. Cit*. *Auditoría en informática* [...]. Pág. 5.
11 *Auditoría en centros de cómputo. "Una herramienta de apoyo para la gerencia".* Tesis de L.S.C.A. Universidad del Valle de México. Plantel Lomas Verdes. México, 1993. Pág. 22 (citando a *Auditoría, principios y procedimientos*. De Holmes. R. Arthur. Editorial UTHEA. 1987 (1994). Pág. 3).
12 *Administración de empresas*. Biblioteca para Dirección de Empresas. L. Hall. Editorial EDAF, Ediciones-Distribuciones. Madrid. Pág. 263.

[13] Sayma, consultores de gestión. http://www.sayma.es/auditor2.htm; septiembre.
[14] *Op. Cit*. *Auditoría de Sistemas* [...]. Pág. 10.
[15] Boletín E-02 del Instituto Mexicano de Contadores Públicos, A. C. México, 1994.
[16] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 654.
[17] *Ídem.* [...]. Pág. 655.
[18] *Ídem.* [...]. Pág. 1289.
[19] *Introducción a la administración con enfoque de sistemas.* Joaquín Rodríguez Valencia. Editorial EFACSA. México, 1998. Pág. 553.

Capítulo 5

[1] **Eficaz**. Del latín *efficax-acis*, de efficiere: Realizar, ejecutar [...]. Efectivo: [...] Que logra hacer efectivo un intento o propósito. **Eficiente**. Del latín *efficiens*: [...] Capaz de lograr un efecto [...]. Que tiene facultades para producir determinado efecto o realizar una determinada tarea. *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 160 y *Diccionario Inverso Ilustrado* [...]. Pág. 227.
[2] *Diccionario Etimológico*. Editorial Bruguera. Barcelona. 1973. Pág. 2045.
[3] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 2045.
[4] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 195.
[5] *Op. Cit*. *Diccionario Inverso Ilustrado* [...]. Pág. 266.

Capítulo 6

[1] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 679.
[2] *Op. Cit. Gran Diccionario del Saber Humano* [...] Pág. 1244.
[3] *Glosario de términos técnico-administrativos de uso frecuente en el IMSS.* Ediciones del I.M.S.S. México, 1980. Pág. 87.
[4] *Ídem.* Pág. 96.
[5] *Ídem.* Pág. 86.
[6] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 679.
[7] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1244.
[8] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. pág. 136.
[9] *Op. Cit*. *Administración en las organizaciones* [...]. Pág. 504.
[10] *Ídem*. Págs. 123 y 124.
[11] *Ídem*. Pág. 504.
[12] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. Pág. 93.
[13] *Op. Cit. Administración en las organizaciones* [...]. Pág. 504.
[14] *Op. Cit*. *Glosario de términos administrativos.* Presidencia de la República. Coordinación General de Estudios Administrativos. México, 1980. Pág. 182.
[15] *Glosario de términos de seguridad social*. I.M.S.S. México, 1983. Pág. 58.
[16] *Op. Cit*. *Glosario de términos administrativos de uso frecuente en el IMSS* [...]. Pág. 130.
[17] *Glosario de términos administrativos*. Secretaría de Educación Pública. SEP. México, 1982. Pág. 22.
[18] *Op. Cit. Glosario de términos administrativos.* Presidencia de la [...]. Pág. 128.
[19] *Ídem.* Pág. 199.
[20] *Ídem*. Pág. 63.

[21] *Ídem*. Pág. 28.
[22] *Op. Cit. Gran Diccionario del Saber Humano* [...]. Pág. 23.
[23] *Ídem*. Pág. 1915.
[24] *Op. Cit*. *Glosario de términos administrativos.* Presidencia de la [...]. Pág. 125.
[25] *Op. Cit*. *Glosario de términos de seguridad social.* I.M.S.S. Pág. 130 (citando a *Top Management Planning*,. McMillan Co. Nueva York, 1969. George Steiner).
[26] *Ídem.* Pág. 161.
[27] *Ídem.* Pág. 92.
[28] *Ídem*. Pág. 187.

Capítulo 8

[1] De Cantinflear: "*Hablar mucho y decir poco." Op. Cit*. *Pequeño Larousse Ilustrado*. Pág. 190.
[2] Dominguero: "*Que se usa o hace en domingo.[...]" . Ídem*. Pág. 370.
[3] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 455.
[4] *Cómo elaborar y asesorar una investigación de tesis.* Carlos Muñoz Razo. Editorial Pearson Educación. México, 1998.
[5] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 238.
[6] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 996.
[7] *Ídem*. Pág. 462.
[8] *ídem.* Pág. 1572.
[9] *Ídem.* Pág. 1016.
[10] "*Cuentista, que suele dar rollos. Persona pesada. Plúmbea (pesada como el plomo*)". Viene de rollo: [...] *"Discurso exposición, o charla larga y fastidiosa." Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1707.
[11] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 446.
[12] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 771.
[13] *Ídem*. Pág. 785.
[14] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 494.
[15] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 2038.

Capítulo 9

[1] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 732.
[2] *Metodología y técnicas de investigación en ciencias sociales*. Introducción elemental. Felipe Pardinas. Editorial Siglo XXI, 16ª edición, 1976. Pág. 47.
[3] *Ídem*. Pág. 732.
[4] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1374.
[5] *Introducción a la metodología de investigación en ciencias de la administración y del comportamiento*. Fernando Arias Galicia. Editorial Trillas. México, 1991. Pág. 92.
[6] *Op. Cit. Gran Diccionario del Saber Humano* [...]. Pág. 1031.
[7] *Dirección de producción*. Biblioteca para Dirección de empresas. H. A. Harding. EDAF, Ediciones-Distribuciones. España, 1982. Pág. 212.
[8] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1302.

[9] Boletín F-02 del Colegio Nacional de Contadores Públicos, A. C. México, 1994 (1995). Pág. 80.
[10] *Op. Cit. Metodología y técnicas de investigación* [...]. Pág. 68.
[11] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1302.
[12] *Estadística*. Taro Yamane. Traducción de Nuria Cortado. Editorial Harla. Tercera edición. México, 1974. Pág. 54.
[13] *Auditoría, un enfoque integral*. Alvin A. Arens y James K. Loebbecke. Editorial Pearson Educación. México, 1996.
[14] *Op. Cit*. *Metodología y técnicas de investigación* [...]. Pág. 67.
[15] *Op. Cit*. *Estadística*. Taro Yamane [...]. Pág. 54.
[16] *El proceso de la investigación científica.* Mario Tamayo y Tamayo. Editorial Limusa. México, 1986. Pág. 82.
[17] *Probabilidad y estadística*. Stephen S. Willowghby. Editorial Publicaciones Cultural. México, 1980. Pág. 123.
[18] *Op. Cit*. *Estadística*. Taro Yamane [...]. Pág. 54.
[19] *Ídem.* Pág. 86.
[20] *Ídem.* Pág. 55.
[21] *Ídem.* Pág. 55.

Capítulo 10

[1] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 771.
[2] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 447.
[3] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 771.
[4] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 448.
[5] *Ídem*. Pág. 849.
[6] *Op. Cit. Gran Diccionario del Saber Humano* [...]. Pág. 1593.
[7] *Ídem*. Pág. 1025.
[8] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 583.
[9] *Op. Cit*. Gran Diccionario del Saber Humano [...], Pág. 1025.
[10] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 583.
[11] *Ídem*. Pág. 260.
[12] *Ídem*. Pág. 260.
[13] *Gran Diccionario del Saber Humano* [...]. Pág. 456.
[14] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 260.
[15] *Ídem*. Pág. 260.
[16] *Diccionario Inverso Ilustrado* [...]. Pág. 155.
[17] La ley federal del trabajo establece como causas de rescisión de la relación laboral sin responsabilidad para el patrón, en su artículo 47, fracción décima, "Tener el trabajador más de tres faltas de asistencia en un periodo de 30 días, sin permiso del patrón o sin causa justificada". *Ley federal del trabajo 1999*, Pág. 29. Editores Mexicanos Unidos. México, 1999.
[18] *Especialidad en vinculación*. Doctor Adip Sabag Sabag. Universidad del Valle de México. Plantel Lomas Verdes. Febrero a diciembre de 1998.
[19] *Op. Cit*. *Ética*. Estrada Parra [...]. Pág. 93.

Capítulo 11

[1] *Pequeño Larousse Ilustrado* [...]. Pág. 525.
[2] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1124.
[3] *Ídem*. Pág. 769.
[4] *Ídem*. Pág. 769.
[5] *Op. Cit*. *Pequeño Larousse Ilustrado* [...]. Pág. 446.
[6] *Op. Cit*. *Diccionario Inverso Ilustrado* [...]. Pág. 262.
[7] *Pequeño Larousse Ilustrado* [...]. Pág. 1048.
[8] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 2011.
[9] *Ídem*. Pág. 2012.
[10] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 436.
[11] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág. 1814.
[12] *Ídem.* [...]. Pág. 1811.
[13] *Análisis y diseño de sistemas*. Kenneth E. Kendall y Julie E. Kendall. Editorial Pearson Educación. México, 1995. Tercera edición. Pág. 8 y Sigs.
[14] *Producción automática de software con herramientas CASE*. Antonio López-Fuensalida. Metodología de desarrollo. Editorial Macrobit. México, 1991. Pág. 15 y Sigs.
[15] *Ibídem.* [...]. Pág. 16.
[16] *Ibídem.* [...]. Pág. 119 y Sigs.
[17] *Ídem.* [...]. Pág. 138 y Sigs.
[18] *Sistemas digitales, principios y aplicaciones.* Ronald J. Tocci. Editorial Pearson Educación. México, 1981. Pág. 34.
[19] *Op. Cit*. *Glosario de terminología de seguridad social* [...] (citando a Cordera, Armando y Bobenriath, Manuel. *Administración de sistemas de salud*. A. Cordera Editor).
[20] *Ídem*. Pág. 44 (citando el Glosario de términos administrativos. Presidencia de la República; Coordinación General de Estudios Administrativos. 1980).
[21] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. Pág. 89.
[22] *Op. Cit*. *Glosario de términos de seguridad social* [...]. Pág. 30.
[23] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. Pág. 131.
[24] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 188.
[25] *Op. Cit*. *Gran Diccionario del Saber Humano* [...]. Pág.769.
[26] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. Pág. 81.
[27] *Op. Cit*. *Diccionario Etimológico* [...]. Pág. 2012.
[28] *Ídem*. Pág. 2011.
[29] *Op. Cit*. *Glosario de términos técnico-administrativos de uso frecuente en el IMSS* [...]. Pág. 106.
[30] *Controles Internos para sistemas de computación.* Jerry Fitzgerald. Editorial LIMUSA. México, 1981.
[31] *Op. Cit*. *Enciclopedia electrónica Grolier* [...].
[32] *Soluciones avanzadas*. Eduardo Cadena Gómez. Abril de 1996. Pág. 27 y Sigs.
[33] "La ISO-9000 (*International Standard Organization*) define un sistema de calidad consistente de la estructura organizacional, las responsabilidades, los procedimientos, los procesos y los recursos ne-

cesarios para implementar la administración de la calidad. Un registro de calidad es la evidencia de que una actividad de calidad requerida por la norma ISO-9001 [...]". Guillermo Rodríguez, Jorge González y Gladys Dávila. *Soluciones avanzadas*. Julio de 1998. Pág. 26.

[34] *Ibídem.* Pág. 28.

[35] *ISO-9000 Liderazgo virtual*. Tom Taormina. Editorial Pearson Educación. México, 1998. Pág. 66.

[36] *Op. Cit*. *Análisis y diseño de sistemas.* Kendall [...]. Pág. falta nº. de pág.

[37] PC Magazine en español. *Y2K, la cuenta regresiva hacia el 2000*. Volumen 19, número 4. Editorial TELEVISA. México, 1999. Pág. 65 y Sigs.

Capítulo 12

[1] *Ídem*. Pág. 90.

[2] *Personal Computing México*. Información comercial. Abril de 1998. Pág. 69. *Diagnôstik* es marca registrada de SOFTEL (Software & Technology Enterprise de México, S. A. de C. V).

[3] *Soluciones avanzadas*. Art. Outsourcing y telecomunicaciones. Marcelo Padua Díaz. Abril de 1996. Pág. 35.

[4] *Soluciones avanzadas*. ISO-9000, una visión global. Eduardo Cadena Gómez. México, Abril de 1996. Pág. 29.

[5] *Soluciones avanzadas*. La norma ISO-9001 en una fábrica de software a la medida. Guillermo Rodríguez, Jorge González y Gladys Dávila. Julio de 1998.

[6] *Enciclopedia Electrónica Grolier*; Grolier Electronic Publishing, Inc. CD-ROM.

[7] UVM. Diplomado en ergonomía. Plantel Lomas Verdes. México, 1994. Material de seminarios. Varios catedráticos.

ÍNDICE

B

C

D

E

F

G

H

I

J

L

M

R

S

T

U

V