AUDITORÍA INFORMÁTICA

Un enfoque práctico

2ª EDICIÓN AMPLIADA Y REVISADA

Mario G. Piattini
Emilio del Peso

Alfaomega Ra-Ma

Auditoría Informática

Un enfoque práctico

2.ª edición ampliada y revisada

Coordinadores

Mario Gerardo Piattini Velthuis
Universidad de Castilla-La Mancha

Emilio del Peso Navarro
IEE Informáticos Europeos Expertos

Alfaomega Ra-Ma

Auditoría Informática: Un enfoque práctico, 2a. edición ampliada y revisada

ISBN 84-7897-444-X, edición original publicada por RA-MA Editorial, MADRID, España.

Pitágoras 1139, Col. Del Valle, 03100 México, D.F.

Miembro de la Cámara Nacional de la Industria Editorial Mexicana
Registro No. 2317

Internet: **http://www.alfaomega.com.mx**
Email: **ventas1@alfaomega.com.mx**

ISBN: 970-15-0731-2

NOTA IMPORTANTE
La información contenida en esta obra tiene un fin exclusivamente didáctico y, por lo tanto, no está previsto su aprovechamiento a nivel profesional o industrial. Las indicaciones técnicas y programas incluidos, han sido elaborados con gran cuidado por el autor y reproducidos bajo estrictas normas de control. ALFAOMEGA GRUPO EDITOR, S.A. de C.V. no será jurídicamente responsable por: errores u omisiones; daños y perjuicios que se pudieran atribuir al uso de la información comprendida en este libro, ni por la utilización indebida que pudiera dársele.

Impresión:
Gente Nueva Editorial
Bogotá, D.C., Colombia

PREFACIO

Desde los inicios de la humanidad las distintas culturas han dado una importancia enorme a los temas de contabilidad, y por tanto también han necesitado de medios que permitieran verificar sus registros, es decir, de la auditoría. De hecho se piensa que la invención de la escritura surgió como respuesta a la necesidad de auditar, Flesher (1993); por lo que la de auditor sería una de las profesiones más antiguas.

Pero es realmente a partir de finales de 1800 cuando la auditoría financiera se extiende por el Reino Unido y Norteamérica, y se sientan las bases de las prácticas que conocemos en la actualidad.

A partir de 1950, la informática se convierte en una herramienta muy importante en las labores de auditoría financiera, ya que permite llevar a cabo de forma rápida y precisa, operaciones que manualmente consumirían demasiados recursos. Empieza la denominada **"auditoría con el computador"**, que no puede considerarse verdadera auditoría informática, sino que utiliza el computador como herramienta del auditor financiero.

Sin embargo, al convertirse los sistemas de información de la empresa cada vez más dependientes de los computadores, surge la necesidad de verificar que los sistemas informáticos funcionan correctamente, empezándose a finales de los años sesenta a descubrirse varios casos de fraude cometidos con ayuda del computador que hacen inviable seguir conformándose con la auditoría **"alrededor del computador"**. Surge así la necesidad de una nueva especialidad dentro de la auditoría, cuyo objetivo es precisamente verificar el funcionamiento correcto, eficaz y eficiente de la informática, en definitiva, la **"auditoría del computador"**.

En la actualidad nadie duda que la información se ha convertido en uno de los activos principales de las empresas, que representa su principal ventaja estratégica.

Las empresas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información que les ofrezcan la mayor productividad y calidad posibles. Es por eso que los temas relativos a la auditoría informática cobran cada vez más relevancia tanto a nivel internacional como nacional.

De esa importancia creciente de la información nace la necesidad de que ese bien jurídico sea protegido por el derecho y aparezca regulado en el ordenamiento jurídico.

La entrada en vigor de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal; la Ley Orgánica 10/1995 de 23 de noviembre que aprueba el nuevo Código Penal, y por último el Texto Refundido de la Ley de la Propiedad Intelectual aprobado por el Real Decreto Legislativo 1/1996 de 12 de abril así como una serie de normas específicas del sector establecen un marco jurídico de lo que se viene denominando Nuevas Tecnologías de la Información.

El establecimiento de ese marco jurídico incide de forma importante en la Auditoría Informática. Pues si antes comprobábamos que era imposible realizar una Auditoría de Cuentas si no se auditaba lo que contenían esas "cajas negras" que son los sistemas de información y que contienen todos los datos económicos de las organizaciones, ahora vemos que difícilmente se puede realizar una Auditoría Informática si no tenemos en cuenta el marco jurídico en que se sitúan esos sistemas informáticos.

Colaboran en el libro veintiocho autores, entre los que se encuentran profesores de universidad y profesionales de reconocido prestigio en el mundo de la auditoría informática, reuniendo algunos de ellos las dos cualidades, lo que aporta un gran valor añadido a la obra al ofrecer perspectivas y experiencias muy variadas sobre prácticamente todos los aspectos relacionados con la auditoría informática.

Los objetivos que nos hemos propuesto en esta obra son los siguientes:

- Presentar de forma clara y precisa los conceptos fundamentales sobre control interno y auditoría informática.
- Ofrecer un tratamiento sistemático de las técnicas y métodos del auditor informático.
- Dar a conocer los aspectos organizativos, jurídicos y deontológicos asociados a la auditoría informática.
- Exponer en profundidad las principales áreas de la auditoría informática: física, seguridad, desarrollo, mantenimiento, explotación, ofimática, calidad, redes, dirección, etc.
- Suministrar una visión global de la auditoría informática en diversos sectores: banca, sector aéreo, público, PYMES, etc.

- Proporcionar pautas y experiencias que ayuden al profesional informático en las tareas de auditoría.

En esta segunda edición del libro se han actualizado y corregido varios capítulos, incorporando otros nuevos, con el fin de ofrecer una panorámica actual y completa de este campo.

CONTENIDO

La obra está dividida en tres partes claramente diferenciadas:

Parte I: Introducción

En esta primera parte, que consta de siete capítulos, se exponen diversos conceptos fundamentales de la auditoría informática. En el primer capítulo se describe la utilización de la informática como herramienta del auditor financiero, mientras que en el segundo capítulo ya empieza la auditoría informática propiamente dicha, analizándose su relación con el control interno, dedicándose el capítulo siguiente a exponer las principales metodologías de control interno, seguridad y auditoría informática.

El capítulo 4 trata de uno de los aspectos fundamentales de la auditoría y de cuya calidad depende realmente el éxito de la misma: el informe de auditoría. Otro aspecto esencial es la organización del departamento de auditoría informática, que se analiza en el capítulo siguiente.

Esta parte finaliza con dos capítulos que se dedican a explorar sendos aspectos a los que no se les suele dedicar la extensión necesaria en los libros existentes: el marco jurídico y la deontología del auditor informático, pero que nosotros estimamos imprescindibles en la formación de cualquier profesional que trabaje en esta área.

Parte II: Principales áreas de la auditoría informática

Los capítulos que configuran esta parte central del libro se dedican a analizar las diversas áreas a las que se aplica la auditoría informática. Así, se empieza en el capítulo 8 con la auditoría física, mientras que el capítulo siguiente se dedica a la auditoría de la ofimática, que cada día tiene un mayor peso en las empresas e instituciones; y el capítulo 10 a la auditoría de la dirección.

Los capítulos 11 al 13 se dedican a exponer las consideraciones de auditoría informática sobre tres áreas bastante relacionadas: explotación, desarrollo y mantenimiento; que se complementan con el contenido de los dos capítulos siguientes que abordan las bases de datos y la técnica de sistemas respectivamente.

Dos aspectos que cada día cobran más importancia dentro de la aplicación de las Tecnologías de la Información a las empresas, la calidad y la seguridad, son objeto de los capítulos 16 y 17.

El capítulo 18 se dedica por completo a analizar la auditoría de redes, uno de los componentes más importantes en un sistema de información, que está experimentando un cambio espectacular en la última década.

El capítulo siguiente se dedica a exponer los principales elementos que deben examinarse a la hora de auditar las aplicaciones informáticas; mientras que el capítulo 20 profundiza en estos aspectos para las auditorías de los sistemas EIS/DSS y las aplicaciones de simulación.

Esta parte finaliza con un capítulo dedicado a la auditoría de los entornos informáticos desde el punto de vista jurídico, totalmente actualizado para esta segunda edición.

Parte III: Auditoría informática en diversos sectores

No queríamos dejar fuera de esta obra algunas consideraciones sobre la aplicación de la auditoría informática a diversos sectores económicos que sirviera para aglutinar de forma práctica los conceptos expuestos en la parte anterior.

Siguiendo esta filosofía, dedicamos el capítulo 22 a la auditoría informática en el sector bancario, mientras que el capítulo 23 analiza la auditoría informática en el sector transportes, específicamente el aéreo. Los capítulos 24 y 25 tratan sobre la auditoría informática en dos sectores muy importantes en nuestro país: la Administración Pública y las PYMES.

Parte IV: Otras cuestiones relacionadas con la auditoría informática

En esta segunda edición del libro se han incorporado dos nuevos capítulos que complementan a los anteriores tratando importantes cuestiones relacionadas con la auditoría informática. El capítulo 26 aborda la relación entre el peritaje y la auditoría informática, mientras que el capítulo 27 analiza el contrato de auditoría.

El libro finaliza con una amplia bibliografía que ha servido de referencia y que, en parte, también se ofrece como lecturas recomendadas en cada uno de los capítulos. También hemos incluido en cada capítulo unas preguntas de repaso que pueden indicar al lector el grado de asimilación que ha alcanzado sobre la materia.

Por último se incluyen los acrónimos utilizados en el texto.

ORIENTACIÓN A LOS LECTORES

Aunque un conocimiento en profundidad de las técnicas y herramientas de la auditoría informática puede estar reservado a los profesionales de la materia, nuestro propósito al editar esta obra ha sido dirigirnos a una audiencia mucho más amplia que comprende:

- Participantes en seminarios o cursos monográficos sobre auditoría informática, bien sean de introducción o más avanzados.
- Profesionales informáticos y economistas que estén trabajando en el área de auditoría, ya sea financiera o informática, y que deseen ampliar y perfeccionar sus conocimientos.
- Directivos que sean responsables de la gestión del departamento de sistemas de información, su desarrollo o explotación.
- Profesionales del Derecho que se encuentren trabajando en el campo informático.
- Estudiantes universitarios de la asignatura Auditoría Informática, que afortunadamente se va incorporando actualmente en los planes de estudio de un mayor número de universidades.
- Consultores informáticos y usuarios avanzados que tengan interés en adquirir algunos conocimientos sobre auditoría informática.

Debido a la diversidad de la audiencia, el estudio de esta obra puede realizarse de maneras muy distintas, dependiendo de la finalidad y conocimientos previos del lector, ya sea auditor o auditado.

Cada parte y cada capítulo pueden consultarse de manera autónoma sin tener que seguir el orden que se ha establecido.

AGRADECIMIENTOS

Querríamos expresar nuestro agradecimiento, en primer lugar, a los autores que colaboran en esta obra y que son sus verdaderos artífices. Sus conocimientos, experiencias y autoridad en el campo de la auditoría informática constituyen, sin lugar a dudas, una garantía de la calidad de su contenido.

Queremos agradecer a Rafael Rodríguez de Cora, antiguo presidente de la OAI (Organización de Auditoría Informática), el haber aceptado escribir el prólogo a la primera edición de esta obra, y a Marina Touriño presidenta actual de la OAI por el prólogo a esta segunda edición, pues al igual que el resto de los compañeros de la

OAI, ha sido durante varios años una fuente constante de aprendizaje y de intercambio de ideas, manteniendo encendida la llama de la auditoría informática en nuestro país.

Asimismo agradecemos a Miguel Recio Gayo su inestimable ayuda en la revisión de la obra.

Desde estas páginas queremos también agradecer a los lectores de la primera edición del libro por sus sugerencias y felicitaciones, ya que ellos han hecho posible la realización de esta segunda edición.

Mario Piattini quiere dejar testimonio de su reconocimiento a los distintos profesores que tuvo, ya hace varios años, en el Máster de Auditoría Informática dirigido por Carlos Manuel Fernández, organizado por la empresa CENEI. Ellos despertaron su interés por un área cada día más relevante dentro de la Informática.

Emilio del Peso quiere expresar particularmente su agradecimiento a todos aquellos que han confiado en él siendo el que menos sabe en esta materia; a su familia que siempre, de una forma u otra, colabora en todo aquello que hace, y especialmente a sus hijas Nuria y María del Mar, que han colaborado en la transcripción y corrección de esta obra.

Por último, nos resta dar las gracias a Ana M.ª Reyes por sus valiosas sugerencias que, como en otras muchas ocasiones, han contribuido a mejorar considerablemente este libro, así como a la empresa Albadalejo, S.L., que se encargó de la composición del mismo, y a la editorial Ra-Ma, especialmente a José Luis Ramírez, por su apoyo y confianza.

Mario Piattini
Emilio del Peso

Madrid, Octubre 2000

PRÓLOGO A LA PRIMERA EDICIÓN

Tengo el gran placer de presentar *Auditoría Informática: Un enfoque práctico*, de los Editores Emilio del Peso y Mario Piattini. Me parece un libro extraordinariamente oportuno para la situación en que vivimos, desde el punto de vista tecnológico, de los negocios, y de la auditoría y seguridad informática, ya que aporta un enfoque integrado y completo.

Estamos inmersos en un profundo cambio de todo tipo que nos llevará al próximo siglo XXI. Las empresas y organizaciones dependen de los órdenes económicos, industriales, y sociales en los que se encuentran inmersas por lo que, si las tendencias tecnológicas y los entornos económicos e industriales cambian, deben **adaptarse rápidamente** a las nuevas circunstancias para sobrevivir. Una de las tendencias actuales más significativas es la que se dirige desde una **Sociedad Industrial** hacia la llamada **Sociedad de Información**.

Este cambio es muy rápido, está afectando al mundo entero, y su comprensión es fundamental para las organizaciones de todo tipo, particularmente en el contexto de los Sistemas y Tecnologías de Información. Aunque los avances tecnológicos de los últimos veinte años han sido constantes y espectaculares, en los últimos cinco años se ha producido una verdadera **revolución tecnológica** de gran calado e impacto para la propia industria informática, así como de consecuencias importantes para el resto de los sectores.

Cada vez un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes. De igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad, controles, seguridad e información, son indispensables. La gerencia debe establecer un sistema de control interno adecuado. Tal sistema debe soportar debidamente los procesos del negocio.

Haciéndose eco de estas tendencias, la propia Organización ISACA (Information Systems Audit and Control Association), a través de su Fundación, publicó en diciembre de 1995 el CobiT (Control Objectives for Information and Related Technology), como consecuencia de cuatro años de intensa investigación y del trabajo de un gran equipo de expertos internacionales.

El marco del CobiT es la definición de estándares y conducta profesional para la gestión y el control de los Sistemas de Información, en todos sus aspectos, y unificando diferentes estándares, métodos de evaluación y controles anteriores. Adicionalmente, esta metodología aporta un factor diferencial enormemente importante: la orientación hacia el negocio. Está diseñado no sólo para ser utilizado por usuarios y auditores, sino también como una extensa guía para gestionar los procesos de negocios.

Sin embargo, en términos generales, podemos decir que a pesar de los grandes adelantos tecnológicos, la situación actual de los Sistemas de Información en las Empresas y Organizaciones españolas se caracteriza frecuentemente por una falta de asimilación de las nuevas tecnologías, por una infrautilización de los equipos informáticos, por un descontento generalizado de los usuarios, por una obsolescencia de las aplicaciones informáticas actuales, por una falta de planificación de los Sistemas de Información, y por soluciones planteadas parcialmente que, al no estar integradas, producen islotes de mecanización y de procesos manuales difíciles de controlar y caros de mantener. En definitiva, por una falta de estándares y metodologías, y por una falta de formación y cultura generalizada, sobre todo en los aspectos de control y de seguridad informática.

La Auditoría Informática ha aportado soluciones, en el pasado, para estos problemas; pero se ha realizado frecuentemente, hasta ahora, sólo en grandes empresas y, en la mayoría de los casos, como un complemento a la Auditoría Financiera.

Por diversas razones y por el mayor impacto que están adquiriendo las Tecnologías de Información en la empresa, esta disciplina está siendo cada vez más importante y su aplicación puede llevarse a cabo también en la PYME. La Auditoría Informática plantea unos métodos y procedimientos de control de los Sistemas de Información que son válidos para cualquier tamaño de empresa.

Aquí es donde creo que este libro de *Auditoría Informática: Un enfoque práctico* es de una gran utilidad al presentar un compendio exhaustivo de los temas de más actualidad por los autores más cualificados del sector.

Puede servir de base, por un lado, para llevar a cabo la cultura y formación sobre Auditoría Informática, a la que me refería anteriormente, desde un punto de vista técnico; por otro lado, toca otros temas de interés actual y práctico, desde el punto de vista del negocio y de la empresa, relativos a la organización, a la deontología, al marco jurídico, a la responsabilidad del empresario, y a la aplicación práctica de la Auditoría Informática en diversos sectores empresariales.

Es de destacar, y de agradecer, el subtítulo de *Un enfoque práctico*. La mayoría de las publicaciones de Auditoría Informática se han escrito en otros idiomas o han sido traducidas en Sudamérica, y eran manejadas y utilizadas por especialistas, pero no han calado suficientemente en "el público en general". Muchas de ellas se han orientado hacia especialistas de Auditoría Informática para realizar su trabajo, lo que está también ampliamente descrito en él, pero entiendo que este libro además, tal como está planteado, supone ese acercamiento de la Auditoría a los empresarios, a los usuarios y a ese público en general.

La competencia global ya está aquí. Las empresas y organizaciones se deben reestructurar hacia operaciones cada vez más competitivas y, como consecuencia, deben aprovechar los avances de las tecnologías de los Sistemas de Información para mejorar su situación competitiva.

Hoy día hablamos de reingeniería de negocios y de procesos, de calidad total, de procesos distribuidos, de organizaciones planas, de EIS/DSS, etc., como cambios que generan un impacto en la manera en que operan las organizaciones privadas y públicas. Estos cambios están teniendo y continuarán teniendo implicaciones profundas para la gestión y para las estructuras de control en las organizaciones del mundo entero.

Entre las implicaciones de las tecnologías de información sobre la gestión empresarial no quiero desaprovechar la oportunidad para comentar el gran impacto, en las empresas y organizaciones, que tendrá el efecto del cambio al *euro* y del problema del año 2000 en las aplicaciones actuales.

Esto será un ejemplo dramático de que la previsión, el control, la seguridad, y la reducción de costes, implicados en los Sistemas de Información mecanizados, pueden convertirse en una estrategia fundamental de las organizaciones. La automatización de las funciones y procesos de la organización, por su propia naturaleza, genera una mayor dependencia de mecanismos de control en los computadores y redes desde el punto de vista del hardware y del software.

En este marco, de cambio acelerado, si los responsables van a estar a la altura de las circunstancias, es necesario que se pongan al día en cuanto a tecnología y entorno de la Auditoría Informática. Este libro, compilado por Emilio del Peso y Mario Piattini, puede ser fundamental para ello.

Desde las Organizaciones como la OAI, que nos dedicamos a difundir y a promocionar esta actividad, deseamos fervientemente que el libro tenga la divulgación que se merece y que efectivamente llegue a crear una "escuela" española, que se echa de menos en nuestro entorno, para mentalizar a la Sociedad de la importancia de esta disciplina.

por *Rafael Rodríguez de Cora*

Presidente de la Organización de Auditoría Informática
Capítulo español de la ISACA

PRÓLOGO A LA SEGUNDA EDICIÓN

Lo importante es mirar nuevamente
teniendo en cuenta las obras ya existentes,
teniendo en cuenta sus leyes,
sus códigos semánticos
e interrelaciones.
Equipo Crónica

Al releer este libro, ***Auditoría Informática: un enfoque práctico,*** entendí que iba a resultar una labor muy ardua poder añadir algún concepto de interés a los incluidos ya en las páginas siguientes. Por esta razón, me he permitido un primer atrevimiento: esbozar algunas reflexiones propias sobre la Auditoría de Sistemas de Información, así como comentarios sobre el contenido de esta obra.

El segundo atrevimiento es, en esta presentación, hablar de "Auditoría de Sistemas de Información" en vez de "auditoría informática". La primera denominación está sustituyendo de alguna manera a la segunda. La expresión Auditoría de Sistemas de Información, que se está consolidando en todo el mundo, corresponde a la realidad y previsión actual del avance de las tecnologías. Actualmente el acento está en la información, siendo el elemento técnico un componente variado, diverso y cambiante, al servicio de la información. Este cambio también ha sido adoptado hace varios años por la Information Systems Audit and Control Association (ISACA), reflejándolo en el nombre para la asociación.

Volviendo la vista atrás, y tratando de explicarme, también a mí misma, qué aliciente tiene ser un profesional de la Auditoría de Sistemas de Información, descubro que la principal atracción está en su aspecto "creativo". De ahí la elección, como prólogo, de una frase de un equipo de creadores que resume para mí una concepción aplicable a la actividad de la que hablamos: aprender de las obras de otros, con una

mirada nueva y actualizada, tener en cuenta los fundamentos básicos para el desarrollo de la profesión, establecer un lenguaje común de comunicación e integrador de todas las disciplinas o actividades que están relacionadas, y al mismo tiempo, investigar en nuevas direcciones. Ésta, es tal vez la razón más importante que me ha hecho permanecer en esta profesión.

La opción para esta permanencia engloba otro factor: la creciente consciencia del cometido social que puede desempeñar esta profesión. La tecnología está cada día más presente en nuestras vidas, desde la doméstica y privada hasta la profesional, y frente a este imparable impulso tecnológico, la sociedad necesita tener una opinión objetiva e independiente sobre el margen de confianza que puede tener en los sistemas de información.

Por lo tanto, sigo convencida de lo acertado de la decisión cuando acepté en el año 1977 "convertirme" en un auditor informático. Para mí, en ese momento en España era una profesión incipiente, aunque, en otros países tuviese ya mayoría de edad. Desde aquel entonces la Auditoría de Sistemas de Información ha experimentado en España, una notable expansión, hasta el punto de convertirse en un elemento clave con relación a fiabilidad de los servicios, usos y prestaciones de los sistemas informáticos y nuevas tecnologías.

Publicaciones como la presente son de vital importancia para la difusión de la actividad y utilidad de la Auditoría de Sistemas de Información, y además permiten, especialmente para aquellos que se inician en esta actividad, apoyarse en el camino ya recorrido por otros profesionales como punto de referencia.

La actividad profesional se basa en unas "buenas prácticas" consensuadas por los profesionales a través de sus asociaciones profesionales. Los auditores de sistemas de información deben ser los verdaderos protagonistas de establecer los fundamentos del ejercicio de su profesión de una forma coherente, meditada y atendiendo a los avances de la tecnología, así como a las necesidades de la sociedad a la cual se deben. Éste es uno de los objetivos de la Organización de Auditoría Informática, capítulo de la ISACA, que en España, de forma pionera, fue fundada en el año 1987. Una asociación de este tipo, con la participación activa de sus integrantes, debería intentar mejorar, desarrollar, consolidar y armonizar la profesión, logrando el afianzamiento de las metodologías de Auditoría de Sistemas de Información.

Se trata de establecer unas bases sólidas que tienen que ver, principalmente, con el objetivo de la Auditoría de Sistemas de Información, el conocimiento de los elementos auditados y la capacidad para detectar riesgos. La Auditoría de Sistemas de Información, tal como se entiende en el ámbito internacional, en los colectivos de profesionales, no tiene como propósito esencial saber si un determinado control, tanto predeterminado como adecuado, se ha implantado simplemente, sino saber qué control o controles existen con la misma finalidad, qué objetivo y fin tienen, cómo se realizan

y la eficacia tienen en cuanto al cumplimiento, y qué riesgos existen aún para los sistemas de información, o bien qué perjuicios pueden causar indirectamente.

A partir de aquí, dada la diversidad de la tecnología y sus usos e implantación, se puede decir que no existe una verdad absoluta y taxativa sobre qué se considera buenos mecanismos de control, ya que éstos son siempre el producto de una situación determinada, así como de su especificidad. Por eso los auditores de Sistemas de Información, a través de sus experiencias, colaboran para mejorar, consolidar y armonizar las prácticas de esta profesión.

La mejora se obtendrá con una actitud innovadora y creativa de los profesionales que las comparten y contrastan para tratar de consolidar y armonizar un referente común tanto para los integrantes del colectivo como para los usuarios de sus servicios.

En los últimos tiempos, la legislación relacionada con las tecnologías de la información y con el tratamiento de datos personales, alude a las auditorías sin darles un apellido determinado, ni una definición concreta. Se entiende, dado el elemento auditado y los resultados que se le pide a esa auditoría, que debería tratarse de una Auditoría de Sistemas de Información. Tampoco esta actividad está definida en los diccionarios, incluyendo el de la Lengua Española. La más cercana es la auditoría contable, o la de auditor, que no cooperan al esclarecimiento de la profesión, sino que al contrario, es posible que confundan aún más. Sin embargo, se desprende de todas ellas, a mi entender, la idea de la independencia u objetividad del auditor, así como la necesidad de un trabajo profesional claramente definido.

A modo de ilustración sobre los principios de la actividad, se incluyen dos manifestaciones de la ISACA: "Los objetivos de la Auditoría de Sistemas de Información deben brindar a la Dirección de una seguridad razonable que los controles se cumplen, fundamentar los riesgos resultantes donde existan debilidades significativas de control y aconsejar a la Dirección sobre acciones correctivas"; así como "la realización de una Auditoría de Sistemas de Información implica la evaluación y emisión de una opinión objetiva e independiente, y de recomendaciones sobre la fiabilidad de un sistema de información".

La Auditoría de Sistemas de Información, dada su relación intrínseca con las tecnologías de la información, con las entidades y organizaciones que utilizan estas tecnologías, y con los usuarios en general, mantiene necesariamente interrelaciones con otras disciplinas o actividades profesionales, con las que comparten proyectos aunque, con distintas metas, áreas de actuación y responsabilidades.

De hecho, la profesión se ha nutrido y se nutre de expertos provenientes de distintas disciplinas afines. Los requisitos esenciales para realizar este tipo de actividad son: conocimientos sólidos de auditoría, así como conocimientos técnicos y entrenamiento permanente en las nuevas tecnologías. Esta situación, dados los avances

de la tecnología, está llevando a los auditores de sistemas de información a especializarse en determinadas áreas o entornos tecnológicos. La realidad señala que los equipos de Auditoría de Sistemas de Información de las entidades de dimensión importante están formados por profesionales multidisciplinares.

El presente libro ***Auditoría Informática: un enfoque práctico***, incluye acertadamente este aspecto de las interrelaciones, desde la utilización de la informática o herramientas tecnológicas, en concreto con respecto a los auditores financieros, al impacto de la creciente legislación con relación a la utilización de las tecnologías. Oportunamente, se analizan aquellos elementos comunes para distintos tipos de auditoría, como son los principios de un informe de auditoría, y los aspectos éticos que debe observar un auditor. Es de agradecer la clarificación sobre un sistema de control interno y la realización de una Auditoría de Sistemas de Información. El ejercicio de ambas actividades tiene puntos en común, incluso en situaciones determinadas se utilizan las mismas herramientas técnicas. Sin embargo, existen diferencias específicas que se indican en los capítulos correspondientes. El control interno de los sistemas de información es una responsabilidad primaria de sus responsables. Además aporta aspectos prácticos tanto de la organización de la función de Auditoría de Sistemas de Información, como de la realización de peritajes informáticos.

Coincidiendo con las definiciones de la ISACA referidas en esta presentación, la Auditoría de Sistemas de Información abarca la revisión y evaluación de todos los aspectos (o alguna sección/área) de los sistemas automatizados de procesamiento de información, incluyendo procedimientos relacionados no automáticos, y las interrelaciones entre ellos. De ahí que, eficazmente, se hayan previsto tratamientos separados de distintas áreas objeto de la Auditoría de Sistemas de Información, desde la seguridad física y ofimática, hasta los aspectos de tipo legal, la calidad, y la seguridad, considerando también los aspectos de gestión de los sistemas de información, la adecuación de la actividad a entornos medios, las áreas de desarrollo, sistemas concretos y tecnologías específicas.

Es importante destacar que este enfoque práctico abarca asimismo el ejercicio de esta actividad en determinados sectores de actividad, que pueden imprimir en la realización del trabajo del auditor una cierta particularización, ya que los riesgos de los sistemas de información, en muchos casos, varían y dependen de la actividad empresarial.

Los profesionales que han hecho posible este libro, están haciendo un aporte cualitativo a este "camino que se hace al andar", contribuyendo a que la Auditoría de Sistemas de Información se entienda en cuantos a sus objetivos, y que al mismo tiempo cumpla con su función social de dar confianza en los sistemas de información a sus responsables y a la sociedad en general que recibe sus servicios.

Quiero personalmente agradecer a Mario Piattini y Emilio del Peso, por haberme honrado con la petición de hacer esta presentación. Como parte del colectivo

profesional de auditores de sistemas de información, agradezco también el esfuerzo dedicado para llevar a buen término estas publicaciones, y su difusión y, asimismo hago extensivo mi reconocimiento a los distintos autores por su contribución.

Marina Touriño
Certified Information Systems Auditor
Presidenta de la Organización de Auditoría Informática

CONTENIDO

CAPÍTULO 14. AUDITORÍA DE BASES DE DATOS

CAPÍTULO 15. AUDITORÍA DE TÉCNICA DE SISTEMAS

CAPÍTULO 1

LA INFORMÁTICA COMO HERRAMIENTA DEL AUDITOR FINANCIERO

Alonso Hernández García

1.1. DEFINICIÓN DEL ENTORNO

Definid y no discutiréis. Y aun sin la pretensión de que lo que se exponga en este capítulo sea indiscutible, parece muy conveniente delimitar el campo en que nos desenvolvemos.

Dentro de una especialidad tan reciente y expansiva como la llamada auditoría informática, cabe perfectamente la confusión conceptual tanto entre los diferentes aspectos, áreas o enfoques en sí mismos como por la debida a la vertiginosa evolución que experimenta la especialidad.

Pero como ya pretende explicitar el título del capítulo, vamos a tratar de auditoría financiera. Parece indicarse que en cierta medida nos desgajamos del contenido general del libro y nos desviamos hacia las auditorías financieras.

No es exactamente así. Si desmenuzamos el contenido de la auditoría y su evolución podemos observar que el concepto permanece inamovible y son su objeto y finalidad lo que puede variar.

También parece procedente hacer una alusión específica a la consultoría como especialidad profesional, ya que se hace preciso delimitar sus respectivos campos que en ocasiones se confunden y superponen.

1.2. AUDITORÍA. CONCEPTO

Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

1) contenido:	una **opinión**
2) condición:	**profesional**
3) justificación:	sustentada en determinados **procedimientos**
4) objeto:	una determinada información obtenida en un cierto soporte
5) finalidad:	determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su **fiabilidad**.

En todo caso es una función que se acomete a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

1.3. CLASES DE AUDITORÍA

Los elementos 4 y 5 distinguen de qué clase o tipo de auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata. A título ilustrativo podríamos enumerar entre otras:

Clase	Contenido	Objeto	Finalidad
Financiera	Opinión	Cuentas anuales	Presentan realidad
Informática	Opinión	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas
Gestión	Opinión	Dirección	Eficacia, eficiencia, economicidad
Cumplimiento	Opinión	Normas establecidas	Las operaciones se adecuan a estas normas

1.4. PROCEDIMIENTOS

La opinión profesional, elemento esencial de la auditoría, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma.

Como es natural, cada una de las clases o tipos de auditoría posee sus propios procedimientos para alcanzar el fin previsto aun cuando puedan en muchos casos coincidir. El alcance de la auditoría, concepto de vital importancia, nos viene dado por los procedimientos. La amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance.

En las auditorías altamente reglamentadas como la financiera es preceptivo "aplicar las Normas Técnicas y decidir los procedimientos de auditoría". "Cualquier limitación... que impida la aplicación de lo dispuesto en las Normas Técnicas debe ser considerada en el Informe de auditoría como una reserva al alcance".

Se pretende garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias, etc. que sean significativas.

Para ello se establecen unas normas y procedimientos que en cuanto a la ejecución de la auditoría se resumen en que:

– El trabajo se planificará apropiadamente y se supervisará adecuadamente.

– Se estudiará y evaluará el sistema de control interno.

– Se obtendrá evidencia suficiente y adecuada.

Como corolario se establece que la evidencia obtenida deberá recogerse en los papeles de trabajo del auditor como justificación y soporte del trabajo efectuado y la opinion expresada.

Estas tres normas se deducen claramente de la situación real actual de los riesgos que ha de afrontar el auditor.

Inicialmente, cuando el objeto de la auditoría, los documentos financieros a auditar, eran relativamente cortos y contenían más bien escasas operaciones, los procedimientos llamados de arriba a abajo, que parten de los documentos financieros y auditan hacia abajo, hacia la evidencia de auditoría subyacente, que se verificaba en su integridad, tradicionalmente conocido por censura de cuentas o en base a las cuentas, era adecuado, suficiente y viable.

Sin embargo, cuando llegó la llamada revolución cuantitativa, que trajo consigo la creación de sociedades con importantes medios, que las operaciones se multiplicaran enormemente y que la gestión y propiedad se diferenciaran cada vez más claramente, el método tradicional resultó laborioso, tedioso, largo, ineficaz y económicamente inviable.

No era posible verificar la totalidad de las muy cuantiosas operaciones y, por tanto, había que reducir el campo de acción del auditor a **parte** de la numerosa información.

También, como nos manifiesta Dale S. Flesher, a partir de los primeros años del siglo XX, la banca se convirtió en el principal usuario de las auditorías de cara al seguimiento de sus créditos, y no estaba interesada en la exactitud administrativa de las cuentas sino "en la calidad y representatividad de los balances".

Este nuevo planteamiento, sin embargo, traía implícito un riesgo evidente, al no verificarse la totalidad de los movimientos.

Los controles establecidos por la entidad auditada pudieran permitir que se produjeran irregularidades, potencialmente significativas, casuales o voluntarias.

Al no someterse a revisión todas y cada una de las operaciones, cabe la posibilidad de que escape a la atención del auditor alguna de aquellas irregularidades.

El auditor tiene el cometido irrenunciable de mantener el riesgo de que esto ocurra dentro de límites tolerables.

Este aserto podría representarse de forma aritmética como:

$R(c) * R(d) = S(e)$.

R(c) = al riesgo en el proceso o riesgo de control.

R(d) = riesgo de detección.

S(e) = constante o parámetro admisible en que se desea mantener el riesgo de auditoría.

Es inmediato el hecho de que el riesgo de control y el riesgo de detección dentro de la ecuación planteada son inversamente proporcionales. Si añadimos que el riesgo de control es ajeno al auditor, pues depende de las normas establecidas por la entidad en su sistema, es evidente que para definir el riesgo de detección que está dispuesto a admitir, ha de evaluarse primero el riesgo de control existente.

De ahí se justifica la imposición de las Normas Técnicas que establecen que la revisión del sistema tiene por objeto el que sirva como base para las pruebas de cumplimiento y para la evaluación del sistema.

En esta línea las Normas de Auditoría en su apartado 2.4.34, explicitan que el riesgo final del auditor es una combinación de dos riesgos separados.

- El primero de éstos está constituido por aquellos errores de importancia que ocurran en el proceso contable, del cual se obtienen las cuentas anuales.

- El segundo riesgo es de que cualquier error de importancia que pueda existir sea o no detectado por el examen del auditor.

El auditor confía en:

- el control interno establecido por la entidad auditada para reducir el primer riesgo y

- en sus pruebas de detalle y en sus otros procedimientos para disminuir el segundo.

Basados en estos conceptos podemos esquematizar los procedimientos de auditoría financiera establecidos por las Normas en relación con la ejecución de la auditoría, de la siguiente forma:

Planificación y seguimiento	Análisis y evaluación del c.i.	Evidencias sustantivas
Plan Global	Revisión del sistema	Analíticas
Preparación del programa	Cumplimiento	De saldo De apuntes

1.5. VARIACIÓN DEL OBJETO

Por añadidura es innegable, (y aquí sí reclamaríamos la condición de indiscutible para el aserto), que con mayor o menor profundidad la gestión de las entidades ha experimentado un cambio sustancial y hoy, salvo casos dignos del Guinness, se utiliza la TI (Tecnología de la Información) en todo proceso contable.

Se ha introducido un nuevo elemento cualitativo en el objeto de la auditoría, el uso de la informática como factor consustancial a la gestión, con la introducción de la

Tecnología de la Información (TI) en los sistemas, muy probablemente basada en las ventajas que aporta la informatización con respecto al trabajo manual, entre las que, según C. Martin, se podrían distinguir:

	Humano	Computador
Costo de explotación	Alto	Bajo
Costo de operación	Alto	Bajo
Rendimiento continuado	Disminuye	Constante
Consistencia	Poca	Excelente
Capacidad de cálculo	Buena	Pobre
Reacción ante lo inesperado	Buena	Pobre
Sentido común	Excelente	Pobre
Lenguaje	Bueno	Pobre

Este nuevo elemento, la Tecnología de la Información, puede estar y de hecho tiende a estar en todos los niveles del sistema.

Este mero hecho impone un nuevo condicionante al auditor: ha de trabajar ante y con elementos de Tecnología de la Información. Dado que según las propias Normas Técnicas de auditoría que regulan su actuación el auditor ha de tener en cuenta todos los elementos de la entidad **incluso los informáticos**, el cumplir con esta función no es una decisión graciable del auditor sino una obligación definida por la Norma. Sería más que coherente que una firma de auditoría que por la razón que fuere no quiere o no puede cumplir con este requisito se viera obligada a introducir una limitación al alcance de su trabajo. Es evidente que no habría aplicado todos los procedimientos precisos.

En un excelente trabajo acometido por The Canadian Institute of Chartered Accountants, una institución de reconocido prestigio internacional, se plantea la cuestión de cuáles son actualmente los "libros" o soporte de los documentos financieros objeto de la labor del auditor en un entorno informatizado, y concluye que dichos libros están materializados en los archivos electrónicos, es decir los archivos creados y mantenidos en forma electrónica por las aplicaciones contables.

El objeto es distinto. Está en un soporte diferente. El auditor financiero ve alterado el objeto de su actividad en el sentido de que se ha introducido la TI, ahora está en soporte magnético y este cambio trae consecuencias de gran calado en cuanto a procedimientos de auditoría financiera.

Ha de cambiar sus procedimientos en función de las nuevas circunstancias y, por tanto, de la expansión de su alcance. La auditoría financiera sigue siendo auditoría y financiera con la diferencia de que en su objeto, el mismo de siempre, es decir en la información financiera, se ha introducido la TI.

Se presenta la alternativa al auditor de utilizar los listados procedentes de los referidos archivos magnéticos como fuente de información o acceder directamente a los archivos electrónicos y proceder a su análisis de forma también electrónica.

La situación se hace más dramática por el hecho cada vez más extendido de que el soporte documental de los apuntes electrónicos no exista en absoluto. El rastro de auditoría tradicional ha desaparecido como, por ejemplo, en el EDI o EFT.

Afortunadamente la propia TI que incide en los procedimientos que el auditor ha de aplicar proporciona paralelamente medios de ejecutarlos de forma eficiente y directa. Las CAATS (Técnicas de Auditoría asistidas por computador) ponen a disposición del auditor una amplia variedad de herramientas que no sólo viabilizan los nuevos procedimientos sino que mejoran sensiblemente su aplicación y amplían la gama disponible.

Por tanto, deducimos claramente que la introducción de la TI en los sistemas de información afecta a los auditores de una forma dual:

- cambia el soporte del **objeto** de su actividad
- posibilita la utilización de medios informatizados (CAATs) para la realización de sus **procedimientos**.

De todo ello se desprende la nueva situación del auditor financiero: ha de aplicar procedimientos que utilizan técnicas asistidas por computador a un objeto consistente en un sistema de información basado en la TI.

1.6. CONSULTORÍA. CONCEPTO

Y es en esta fase de la exposición cuando parece pertinente añadir una referencia a la consultoría. Conviene distinguir su concepto del de auditoría para precisar nuestro entorno con más exactitud.

La consultoría consiste en "dar asesoramiento o consejo sobre lo que se ha de hacer o cómo llevar adecuadamente una determinada actividad para obtener los fines deseados".

Las diferencias se hacen evidentes. Los elementos de la consultoría podrían resumirse en:

1) contenido:	Dar **asesoramiento o consejo**
2) condición:	de carácter **especializado**
3) justificación:	en base a un **examen o análisis**

4) objeto:	la **actividad o cuestión** sometida a consideración
5) finalidad:	establecer la **manera de llevarla a cabo** adecuadamente

Es una función a priori con el fin de determinar cómo llevar a cabo una función o actividad de forma que obtenga los resultados pretendidos. La auditoría verifica a posteriori si estas condiciones, una vez realizada esta función o actividad, se cumplen y los resultados pretendidos se obtienen realmente.

A título enunciativo podríamos relacionar los siguientes tipos o clases de consultoría:

Clase	Contenido	Objeto	Finalidad
Financiera	Asesoramiento	Planes de cuentas. Procedimientos administrativos	Diseño e implantación
Informática	Asesoramiento	Aplicaciones. Planes de Contingencia	Desarrollo. Diseño e implantación.

Especialmente el elemento ***I*** distingue claramente la auditoría de la consultoría. Dependiendo de que su contenido sea opinar sobre unos resultados vs. dar asesoramiento o consejo en relación con una actividad a desarrollar, se tratará de auditoría o consultoría. Esta distinción nos resultará importante cuando queramos delimitar las funciones.

Se observa, sin embargo, que las definiciones de la auditoría informática tienden a englobar el concepto de consultoría. La auditoría financiera, con siglos de experiencia, se encuentra perfectamente definida; pero las definiciones, reseñas o referencias a la auditoría informática son variadas, lo que es lógico en una especialidad tan reciente.

Dentro del abanico de definiciones, podemos citar:

A) Desde definiciones como la de A. J. Thomas en el sentido de que "la auditoría informática, que es una parte integrante de la auditoría, se estudia por separado para tratar problemas específicos y para aprovechar los recursos de personal. La auditoría informática debe realizarse dentro del marco de la auditoría general. El cometido de la auditoría informática se puede dividir en:

- Un estudio del sistema y un análisis de los controles organizativos y operativos del departamento de informática.

- Una investigación y análisis de los sistemas de aplicación que se estén desarrollando o que ya estén implantados.

- La realización de auditorías de datos reales y de resultados de los sistemas que se estén utilizando.

- La realización de auditorías de eficiencia y eficacia."

B) Incluyendo la de un destacado miembro de la OAI, Miguel Ángel Ramos, que define, según sus manifestaciones simplificadamente, en su tesis doctoral la auditoría informática como "la revisión de la propia informática y de su entorno" y desglosa sin carácter exhaustivo que las actividades a que da lugar esta definición pueden ser:

- Análisis de riesgos.

- Planes de contingencia.

- Desarrollo de aplicaciones.

- Asesoramiento en paquetes de seguridad.

- Revisión de controles y cumplimiento de los mismos, así como de las normas legales aplicables.

- Evaluación de la gestión de los recursos informáticos.

C) A la de J. J. Acha que por su parte la define como "Un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente".

De ellas se desprende que tienden a abarcar conceptos tanto de auditoría como de consultoría. En la línea de análisis que hemos trazado la primera distinción a realizar sería la diferenciación entre auditoría y consultoría. No son términos equivalentes y es preciso distinguirlos.

Nuestro enfoque pretende centrarse en la **auditoría** según el concepto que ya hemos dejado explicitado. Y dentro de ella la **financiera** de acuerdo con su objeto y finalidad que incluye el soporte informático.

1.7. VENTAJAS DE LA INFORMÁTICA COMO HERRAMIENTA DE LA AUDITORÍA FINANCIERA

1.7.1. Grado de informatización

En la doble vertiente relativa a la introducción e influencia de la TI en el objeto por una parte y en los procedimientos por otra de la auditoría financiera hemos de referirnos en primer lugar al grado o intensidad de su utilización.

En cuanto al objeto puede considerarse desde el uso de un simple PC con un par de aplicaciones básicas como pueden ser la contabilidad y un procesador de textos, a un sistema complejo, distribuido, utilizando base de datos en cliente servidor, integrado y comunicado con otros sistemas con los que interactúa directamente como en el EDI. Parece evidente que las tres Normas para la ejecución de la auditoría adquieren una complejidad y amplitud diferentes. Mientras más desarrollado es el sistema, más problemático resulta su enfoque por parte del auditor. Si bien los riesgos de un pequeño PC pueden ser sustantivos, la complejidad de los mismos en un gran sistema es decisiva.

Entre los procedimientos (técnicas) que las tres Normas de ejecución de la auditoría establecen como medios de los que debe valerse el auditor en la ejecución de su trabajo destacan la inspección, observación, averiguación, confirmación, cálculo y análisis. De estas seis al menos cuatro se ejecutan de forma más eficiente con medios informáticos:

- Inspección: como la comparación de datos en dos archivos o cuentas distintas, conciliaciones.
- Cálculo: de amortizaciones, provisiones, ratios, etc.
- Análisis: regresiones o datos que cumplan determinadas condiciones.
- Confirmación: cálculo estadístico, selección y emisión de muestras, cumplimiento, etc.

1.7.2. Mejora de las técnicas habituales

No resulta difícil justificar que las posibilidades del auditor utilizando medios electrónicos se amplía enormemente con respecto a trabajos manuales sobre listados en papel. El incremento en velocidad, eficiencia y seguridad es evidente.

Para todo ello el auditor puede valerse sustancialmente de las diversas herramientas informáticas que tiene a su disposición y que podríamos catalogar de la siguiente forma:

Tipo	Planificación de la Auditoría	Ejecución de la Auditoría
General	Tratamiento de textos *Flowcharting* Utilidades	Tratamiento de textos Hojas de cálculo
Acceso directo		ACL
Específico	Generadores de papeles de trabajo Administración	Simulación paralela Revisión analítica
Especializados	Integradores	Sistemas expertos *Test check*

De forma somera podríamos reseñar los objetivos que se cubren con la utilización de las diversas herramientas enumeradas:

- *Tratamiento de textos*, utilizado generalmente en la práctica como una máquina de escribir superautomatizada para circulares, memorandos, memoria, etc.

  Con una mayor especialización permite automatizar operaciones, generar documentos, relacionar diversos documentos, etc.

- *Hoja de cálculo*, utilizada para efectuar cálculos, automatizar resultados de diferentes documentos numéricos y en algunos casos obtención de ratios, etc., así como generar actualizaciones automáticas, importar archivos de otras aplicaciones, y producir gráficos disponiendo de una amplia gama de fórmulas financieras, económicas, etc.

- *Generador de papeles de trabajo*, fundados esencialmente en el tratamiento de textos de donde se obtienen plantillas, formatos, etc.; permite edición y actualización. Clasifica los documentos por áreas, sectores, personal involucrado, etc.

- *Flowcharting*: produce diagramas representativos de funciones realizadas o a realizar, flujo de documentos, etc.

- *Utilidades*: existe una amplia gama que cubre desde comunicaciones, visualizadores de archivos, búsquedas o incluso rectificadores de archivos.

  El OCR es una asignatura pendiente.

- *Administradores*: efectúan el seguimiento administrativo de las auditorías. Horas empleadas, áreas, control presupuestario, etc.

- *Acceso directo*: todas las aplicaciones a que nos hemos referido hasta el momento y las posteriores se refieren a datos o "archivos" específicos de las mismas que el auditor ha tecleado en las aplicaciones o ha copiado de otras ya existentes. La gran ventaja del acceso directo es que adopta como archivo a leer o analizar "los de la firma auditada", generalmente los que contienen la contabilidad de la misma. Sea cual sea la aplicación de contabilidad que haya utilizado la firma auditada, las aplicaciones de acceso directo, como su nombre indica, adoptan como archivos propios los realizados por esas aplicaciones. De esta forma se materializa directamente la aseveración de que los libros del auditor son los archivos informáticos del auditado.

Tomando como hilo conductor la estructura de ACL (véase figura 1.1), una de las aplicaciones más destacadas de este estilo y posiblemente la más extendida mundialmente, tomaremos como esquema básico, que vemos en la página siguiente.

Los archivos de datos son exactamente los existentes en el auditado, es decir los archivos físicos de la firma auditada, de la forma y con la codificación con que hayan sido grabados. Estos datos no cambian. ACL crea para su tratamiento el "documento" que contiene la información necesaria en cuanto a definiciones del formato del archivo de datos, batches, índices, vistas y espacio de trabajo.

La definición del formato contiene la estructura y contenido del archivo de datos. Incluye información como nombre de los campos, codificación de los datos, márgenes donde comienzan y donde terminan. Con esta información ACL es capaz de leer e interpretar el archivo de datos original a auditar.

Figura 1.1. Estructura de ACL

Partiendo de esta situación ACL puede manipular los datos del archivo prácticamente de cualquier forma o manera:

- Ordenar
- Cronologizar
- Extraer según condiciones
- Estadísticas
- Muestras
- Clasificar
- Contar
- Agregar
- Totalizar
- Estratificar
- Comparar

Sólo existen dos limitaciones a los análisis, cálculos, verificaciones, etc. que puede hacer ACL:

- Que el dato deseado esté en el archivo. (Por ejemplo, no se podría cronologizar si en el archivo no figuraran las fechas.)

- La imaginación del auditor, que combina los diferentes mandatos para obtener la información final que desea. Creando incluso nuevos campos computados, producto del tratamiento de uno o varios de los ya existentes.

Es de destacar la posibilidad de seleccionar la información que cumpla una o varias condiciones. Estos filtros resultan de incalculable valor cuardo se audita.

Si añadimos que la respuesta a cualquier solicitud, sea cual sea el tamaño del archivo de datos, se realiza en segundos y en cualquier caso en pocos minutos, la importancia de esta aplicación queda perfectamente clara.

A título meramente enunciativo y como punto de partida para el auditor interesado, de los 101 cálculos y análisis que se practican en las áreas más habituales, seleccionamos dos a título de ejemplo:

Ejemplo 1: COMPROBACIÓN DE BALANCE

Se indica la relación de mandatos que permite realizar esta operación.

OPEN Contabilidad	Abre el archivo "Contabilidad".
STRATIFY ON Cuenta ACCUMULATE Debe Haber Saldo	Genera, para cada cuenta del plan, su total al debe, al haber, y el saldo.

Ejemplo 2: CONCILIACIÓN ENTRE COMPRAS Y PROVEEDORES

Se indica la relación de mandatos que permite realizar esta operación.

OPEN Contabilidad	Abre el archivo "Contabilidad".
SORT ON Importe TO Compras IF Cuenta="604" AND DH="D"	Produce el archivo "Compras" con aquellos asientos de la contabilidad cuya cuenta sea la 604 y al debe, ordenado por el importe.
SORT ON Importe TO Proveedores	Produce el archivo "Proveedores" con IF Cuenta="400" AND DH="H" aquellos asientos de la contabilidad cuya cuenta sea la 400 y al haber, ordenado por el importe.
OPEN Compras	Abre el recién creado archivo "Compras".
OPEN Proveedores SECONDARY	Abre el recién creado archivo "Proveedores" como archivo secundario.
JOIN Fecha Asiento Importe WITH Importe Asiento Fecha TO "Conciliación Compras-Proveedores" PKEY Importe SKEY Importe PRIMARY SECONDARY	Produce el archivo "Conciliación Compras-Proveedores" con el resultado de conciliar "Compras" con "Proveedores", utilizando el importe como campo que los relaciona.

Revisión analítica

Normalmente se utiliza la hoja de cálculo para obtener, de los datos que habitualmente se le introducen (Balance, Cuentas de Pérdidas y Ganancias, etc.), los ratios, proporciones o funciones que proporcionan una nueva visión comparativa de su contenido.

Sistemas expertos

Las aplicaciones más avanzadas en cualquier campo son las conocidas como sistemas expertos relativos a la también llamada inteligencia artificial. Se trata de usar el computador para que proporcione resultados o conclusiones producto del procesamiento de unos datos específicos en base a unos conocimientos preexistentes en el mismo.

Este sistema ya se ha utilizado en diversos campos, por ejemplo la medicina, para dar diagnósticos o tratamientos en base a los datos del paciente que se introducen en la aplicación.

En el campo de la auditoría su utilización más evidente es en el análisis y evaluación del control interno. No ha sido hasta el momento una aplicación que se haya prodigado, posiblemente por la dificultad de completar una base de conocimientos adecuada que sólo los expertos pueden proporcionar. Se dice, como es costumbre, que las grandes empresas ya han desarrollado sistemas expertos que aplican en mayor o menor medida. Sin embargo, que se sepa, no se ha dado mucha publicidad al respecto.

Los fundamentos de un sistema experto, aplicando la misma filosofía establecida por las Normas Técnicas, consiste en crear unos cuestionarios cuya respuesta sea "sí" o "no" para evitar matices opinables, divididos por áreas de actividad y que se parta de la base de que una totalidad de respuestas positivas implica un sistema excelente. Menos de un determinado nivel implicaría un control débil o muy débil.

Ha de incorporar las pruebas de cumplimiento correspondientes cuya cuantía se designe por medios estadísticos y que sirvan sus respuestas como retroalimentación para una clasificación definitiva del sistema.

Esta clasificación a su vez proporciona un tamaño de muestra para las pruebas sustantivas a realizar así como una definición de las mismas.

Destacan entre sus ventajas, siempre bajo la supervisión del auditor: la objetividad del sistema, la utilización de fórmulas estadísticas, la cuantificación y especificación de pruebas de cumplimiento y sustantivas adecuadas, la actualización

de la base de conocimiento con los nuevos sistemas analizados y el soporte legal que implica en caso de litigio.

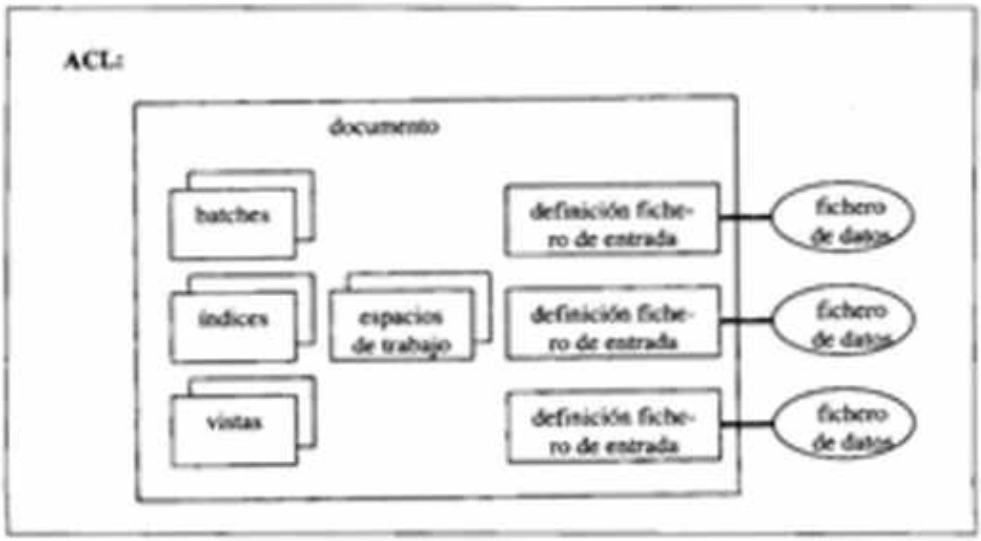


Figura 1.2. Ejemplo de aplicación de sistema experto a la auditoría

Test Check

Esta práctica, cada vez en menor uso, consiste en introducir en la aplicación que el auditado utilice un conjunto de valores cuyo resultado se conoce. Estos valores se comparan con los que eventualmente proporcione la aplicación.

Integradores

Es decir, aquellas aplicaciones que interrelacionan todas las demás para crear un entorno único que utiliza la totalidad de la información obtenida a través de las diferentes herramientas creando un "sistema de auditoría".

Varias de las aplicaciones mencionadas proporcionan medios de programación o, sin ser tan ambiciosos, la posibilidad de crear "batches" de funcionamiento automático. Estos batches o conjuntos de instrucciones pueden operar conjuntamente brindando la posibilidad de realizar operaciones complejas de forma directa y cómoda.

Si tomamos en consideración el proceso completo de auditoría financiera –desde las normas y procedimientos establecidos para antes del propio inicio de la auditoría como la propuesta, contrato, cálculo de costes hasta el informe y recomendaciones finales pasando naturalmente por los procedimientos de ejecución de la auditoría, incluyendo el sistema experto, el acceso directo a archivos informáticos, las pruebas analíticas y adicionales o puntuales que el auditor debe llevar a cabo, y las integramos

en un sistema que automatice tanto las actualizaciones pertinentes en base a los cambios introducidos como la emisión y ordenación de papeles de trabajo justificativos de los procedimientos aplicados–, tendremos un sistema o metodología de integración que sitúa en un solo entorno las diversas fases, documentos, resultados, actualizaciones, etc. de una auditoría. A todo este proceso es a lo que denominaríamos un integrador que aun cuando no abunda, se viene percibiendo su necesidad.

Figura 1.3. Proceso completo de la auditoría financiera

1.7.3. Evolución

El propio Canadian Institute of Chartered Accountants, que se ha preocupado muy especialmente por esta problemática, define un camino hacia la plena institución de un sistema de auditoría informatizado. En un planteamiento al que llama la Hipótesis de Evolución ha distinguido diferentes etapas o niveles que a continuación transcribimos literalmente por su representatividad e importancia:

Las firmas de auditoría más avanzadas han cubierto las dos primeras etapas y actualmente algunas intentan adentrarse en la tercera. Las otras sólo consisten en "buenos deseos" para el futuro, pero que si las seguimos sucintamente vemos que nos conducen a que "la auditoría se convierte en una herramienta para la construcción de realidades políticas y económicas" donde la auditoría y consultoría se entrelazan.

Hipótesis de evolución

	Alcance A Aumento de la competitividad	**Alcance B** Creación de riqueza	**Alcance C** Mejora de la calidad de vida
Nivel 5 Nuevos conceptos y paradigmas basados en la TI	**A5** El valor añadido se convierte en el objetivo de toda auditoría	**B5** La auditoría adopta "el carácter de un servicio de consultoría y análisis continuado"	**C5** La auditoría se convierte en una herramienta para la [illegible] políticas económicas
Nivel 4 Gestión estratégica basada en la TI	**A4** Los auditores adoptan un nuevo concepto de su propia actividad	**B4** La integración de las herramientas de auditoría potencia la eficiencia de la auditoría	**C4** Mejor comprensión de todas las partes implicadas de los beneficios de una auditoría
Nivel 3 Nuevos productos dependientes de la TI	**A3** Las herramientas del auditor se equiparan en sofisticación al sistema de los clientes como EDI o EFT	**B3** Desarrollo de una amplia gama de software-herramienta de auditoría	**C3** Se acaba el expectation gap
Nivel 2 Aumento de la calidad	**A2** Ampliación de la cobertura de auditoría	**B2** Aumento cuantitativo y cualitativo de los descubrimientos	**C2** Menos argumentos en cuanto al papel del auditor
Nivel 1 Reducción de costos	**A1** Reducción de horas de auditoría	**B1** Incremento en la recuperación de costos	**C1** Reducción de trabajo administrativo

Figura 1.4. Intensidad del efecto de la evolución

1.7.4. Grado de utilización

Asalta de inmediato la idea de por qué, visto lo expuesto, el grado de utilización de estas posibilidades por los auditores es bajo y en muchos casos incipiente.

Se han efectuado diversos estudios y parece desprenderse que algunas de las razones pueden ser:

Costo económico

Falta de convencimiento en cuanto a la disminución de costos. No se ve con claridad que la inversión necesaria se vea compensada por la eficiencia que se alcanza.

Parece innegable que los costos tanto del hardware como del software han disminuido extraordinariamente en los últimos años y que la eventual inversión en un sistema para informatización de la auditoría no es en absoluto significativo. Cualquier somero estudio demuestra que su rentabilidad porcentual es siempre sumamente elevada.

Complejidad técnica

Cierto temor reverencial a una nueva técnica que mirada desde el exterior parece sumamente compleja y algo mágico que de por sí ahuyenta. Esta idea puede traer como corolarios otras consideraciones negativas como que se cree que:

* Se depende de los técnicos.
* No se puede revisar el trabajo de los técnicos.
* Problemas de comunicación entre el técnico y el auditor.
* Costo de los técnicos.

La introducción y ampliación de las posibilidades del PC que con sistemas operativos sumamente fáciles de usar pueden realizar trabajos hasta hace pocos años reservados a las grandes instalaciones, simplifica enormemente y pone al alcance de cualquier auditor medianamente familiarizado con la informática una importantísima gama de labores. Todas las que hemos venido exponiendo.

Falta de entrenamiento y experiencia

Es innegable que la utilización de las técnicas de auditoría asistidas por computador requieren un mínimo de entrenamiento y conocimiento. La gran diferencia es que estos mínimos son perfectamente asequibles como ya hemos descrito y consiguen que el auditor retenga el control del proceso de auditoría.

Según Klen, el auditor ha de estar en posesión como mínimo de las siguientes cualidades:

- Ser experto auditor (financiero).
- Entender el diseño y modo de operar del S.I.
- Tener conocimientos básicos de técnicas y lenguajes de programación.
- Estar familiarizado con los sistemas operativos.
- Serle factible poder identificar problemas con los formatos y estructuras de base de datos.
- Ser capaz de tender un puente con el profesional de la TI.
- Saber cuándo pedir apoyo de un especialista.

No cabe duda de que en el entramado multidisciplinar que constituye el acervo de conocimientos de un auditor, este aspecto viene a ampliar su "programa". Es una nueva faceta que viene a enriquecer su perfil. Si nos atenemos a las estadísticas disponibles en EE.UU., el auditor viene adquiriendo estos nuevos conocimientos en un 70% de los casos por medio de entrenamiento en la propia empresa, en un 22% en seminarios y conferencias al efecto y en el 8% en el entorno académico. Mientras la Academia no desarrolle más sus servicios no cabe duda de que la pequeña y mediana empresa de auditoría se enfrenta al nuevo reto de resolver su reciclaje.

Otras incluyendo la preocupación del cliente en cuanto a la seguridad de datos.

1.8. CONCLUSIONES

El objeto de la auditoría financiera ha cambiado. Incorpora la TI. Esto trae consigo el cambio de los "libros" a analizar e igualmente la necesidad de aplicar nuevos procedimientos que utilizan herramientas informáticas.

En la práctica, al auditor se le presenta una disyuntiva: o se adapta a la nueva situación abordando el carro de la evolución hacia metas sumamente halagueñas, para lo que ha de adoptar una actitud receptiva hacia las nuevas tecnologías, o indefectiblemente será una víctima de la evolución que no quiso o no supo afrontar.

1.9. CUESTIONES DE REPASO

1. ¿Cuáles son los elementos fundamentales del concepto de auditoría?

2. ¿Cuántas clases diferentes de auditoría existen?

3. ¿Qué sector es uno de los principales usuarios de las auditorías?

4. ¿Qué ventajas aporta el computador respecto al trabajo manual?

5. ¿Qué significan las siglas CAAT?

6. ¿En qué afecta a los auditores la introducción de las TI en los sistemas de información?

7. ¿Qué diferencias hay entre auditoría y consultoría?

8. ¿Cuáles son las ventajas de la informática como herramienta de la auditoría financiera?

9. ¿Qué pueden aportar los sistemas expertos a la auditoría informática?

10. ¿Cuáles son las razones de la baja utilización de las TI como herramienta de la auditoría financiera?

CAPÍTULO 2

CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

Gloria Sánchez Valriberas

2.1. INTRODUCCIÓN

Tradicionalmente en materia de control interno se adoptaba un enfoque bastante restringido limitado a los controles contables internos. En tanto se relacionaba con la información financiera, el control interno era un tema que interesaba principalmente al personal financiero de la organización y, por supuesto, al auditor externo. El concepto de control interno de mucha gente no incluía muchas de las actividades operativas claves destinadas a prevenir los riesgos efectivos y potenciales a los que se enfrentan las organizaciones. Al producirse la quiebra de numerosas cajas de ahorro y otras organizaciones resultó evidente que no había suficiente conciencia de la necesidad de los controles para evitar que los problemas surgieran y crecieran.

Durante el ultimo decenio la prensa ha informado sobre muchos escándalos relativos a errores en el otorgamiento de créditos con la garantía de inmuebles inexistentes o extremadamente sobrevalorados, la manipulación de información financiera, operaciones bursátiles realizadas con información privilegiada, y muchos otros conocidos fallos de los controles que han afectado a empresas de diferentes sectores. En España se han dado pasos importantes como consecuencia de nuestra incorporación y adaptación a Europa.

Además de la mayor atención que prestan las autoridades al problema, se observan importantes cambios en las empresas. Dichos cambios someten a una gran

tensión a los controles internos existentes. La mayoría de las organizaciones han acometido varias iniciativas en tal sentido, tales como:

- La reestructuración de los procesos empresariales (BPR -*Bussiness Process Re-engineering*).
- La gestión de la calidad total (TQM -*Total Quality Management*).
- El redimensionamiento por reducción y/o por aumento del tamaño hasta el nivel correcto.
- La contratación externa *(outsourcing)*.
- La descentralización.

El mundo en general está cambiando cada vez más rápidamente, sometiendo a las empresas a la acción de muchas fuerzas externas tales como la creciente necesidad de acceder a los mercados mundiales, la consolidación industrial, la intensificación de la competencia, y las nuevas tecnologías.

Las tendencias externas que influyen sobre las empresas son, entre otras, las siguientes:

- La globalización.
- La diversificación de actividades.
- La eliminación de ramas de negocio no rentables o antiguas.
- La introducción de nuevos productos como respuesta a la competencia.
- Las fusiones y la formación de alianzas estratégicas.

Ante la rapidez de los cambios, los directivos toman conciencia de que para evitar fallos de control significativos deben reevaluar y reestructuar sus sistemas de controles internos. Deben actuar de manera proactiva antes de que surjan los problemas, tomando medidas audaces para su propia tranquilidad, así como para garantizar a los consejos de administración, accionistas, comités y público que los controles internos de la empresa están adecuadamente diseñados para hacer frente a los retos del futuro y asegurar la integridad en el momento actual.

Un centro de informática de una empresa del sector terciario suele tener una importancia crucial por soportar los sistemas de información del negocio, por el volumen de recursos y presupuestos que maneja, etc. Por lo tanto, aumenta la complejidad de las necesidades de control y auditoría, surgiendo en las organizaciones, como medidas organizativas, las figuras de control interno y auditoría informáticos.

La auditoría ha cambiado notablemente en los últimos años con el enorme impacto que han venido obrando las técnicas informáticas en la forma de procesar la información para la gerencia. La necesidad de adquirir y mantener conocimientos actualizados de los sistemas informáticos se vuelve cada vez más acuciante, si bien los

aspectos básicos de la profesión no han variado. Los auditores informáticos aportan conocimientos especializados, así como su familiaridad con la tecnología informática. Se siguen tratando las mismas cuestiones de control en la auditoría, pero los especialistas en auditoría informática de sistemas basados en computadores prestan una ayuda valiosa a la Organización y a los otros auditores en todo lo relativo a los controles sobre dichos sistemas.

En muchas organizaciones, el auditor ha dejado de centrarse en la evaluación y la comprobación de los resultados de procesos, desplazando su atención a la evaluación de riesgos y la comprobación de controles. Muchos de los controles se incorporan en programas informáticos o se realizan por parte de la función informática de la organización, representado por el Control Interno Informático. El enfoque centrado en controles normalmente exige conocimientos informáticos a nivel de la tecnología utilizada en el área o la organización que se examina.

2.2. LAS FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICOS

2.2.1. Control Interno Informático

El Control Interno Informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y no normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales.

La misión del Control Interno Informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

Control Interno Informático suele ser un órgano *staff* de la Dirección del Departamento de Informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.

- Asesorar sobre el conocimiento de las normas.

- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al Grupo.

- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informática, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

Realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC's, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes actividades operativas sobre:

- El cumplimiento de procedimiento, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambios y versiones del *software*.
- Controles sobre la producción diaria.
- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del *software* y del servicio informática.
- Controles en las redes de comunicaciones.
- Controles sobre el *software* de base.
- Controles en los sistemas microinformáticos.
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):

  – Usuarios, responsables y perfiles de uso de archivos y bases de datos.
  – Normas de seguridad.
  – Control de información clasificada.
  – Control dual de la seguridad informática.

- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

2.2.2. Auditoría Informática

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza

eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informativos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computador.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

2.2.3. Control interno y auditoría informáticos: campos análogos

La evolución de ambas funciones ha sido espectacular durante la ultima década. Muchos controles internos fueron una vez auditores. De hecho, muchos de los actuales responsables de Control Interno Informático recibieron formación en seguridad informática tras su paso por la formación en auditoría. Numerosos auditores se pasan al campo de Control Interno Informático debido a la similitud de los objetivos profesionales de control y auditoría, campos análogos que propician una transición natural.

Aunque ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar:

	CONTROL INTERNO INFORMÁTICO	AUDITOR INFORMÁTICO
SIMILITUDES	Personal interno Conocimientos especializados en Tecnología de la Información Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información	
DIFERENCIAS	Análisis de los controles en el día a día Informa a la Dirección del Departamento de informática Sólo personal interno El alcance de sus funciones es únicamente sobre el Departamento de Informática	Análisis de un momento informático determinado Informa a la Dirección General de la Organización Personal interno y/o externo Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización

2.3. SISTEMA DE CONTROL INTERNO INFORMÁTICO

2.3.1. Definición y tipos de controles internos

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos".

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto último habrá que analizar el coste-riesgo de su implantación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software) han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta interesante observar, sin embargo, que hasta en los sistemas servidor/cliente avanzados, aunque algunos controles son completamente automáticos, otros son

completamente manuales, y muchos dependen de una combinación de elementos de software y de procedimientos.

Históricamente, los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- *Controles preventivos*: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- *Controles detectivos*: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- *Controles correctivos*: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un archivo dañado a partir de las copias de seguridad.

Como el concepto de controles se originó en la profesión de auditoría, resulta importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría. Se trata de un tema difícil por el hecho de que, históricamente, cada método de control ha estado asociado unívocamente con un objetivo de control (por ejemplo, la seguridad de archivos de datos se conseguía sencillamente manteniendo la sala de computadores cerrada con llave).

Sin embargo, a medida que los sistemas informáticos se han vuelto más complejos, los controles informáticos han evolucionado hasta convertirse en procesos integrados en los que se atenúan las diferencias entre las categorías tradicionales de controles informáticos.

Por ejemplo, en los actuales sistemas informáticos puede resultar difícil ver la diferencia entre seguridad de los programas, de los datos y objetivos de control del software del sistema, porque el mismo grupo de métodos de control satisface casi totalmente los tres objetivos de control.

La relación que existe entre los métodos de control y los objetivos de control puede demostrarse mediante el siguiente ejemplo, en el que un mismo conjunto de métodos de control se utiliza para satisfacer objetivos de control tanto de mantenimiento como de seguridad de los programas:

- *Objetivo de Control de mantenimiento*: asegurar que las modificaciones de los procedimientos programados están adecuadamente diseñadas, probadas, aprobadas e implantadas.

- *Objetivo de Control de seguridad de programas*: garantizar que no se pueden efectuar cambios no autorizados en los procedimientos programados.

2.3.2. Implantación de un sistema de controles internos informáticos

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- *Entorno de red*: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los computadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.

- *Configuración del computador base*: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.

- *Entorno de aplicaciones*: procesos de transacciones, sistemas de gestión de bases de datos y entornos de procesos distribuidos.

- *Productos y herramientas*: software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

- *Seguridad del computador base*: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para la implantación de un sistema de controles internos informáticos habrá que definir:

Gestión de sistemas de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

- Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

- Gestión del cambio: separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

La implantación de una política y cultura sobre la seguridad requiere que sea realizada por fases y esté respaldada por la Dirección. Cada función juega un papel importante en las distintas etapas:

Dirección de Negocio o Dirección de Sistemas de Información (S.I.): Han de definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.

Dirección de Informático: Ha de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de Informática mediante la creación y publicación de procedimientos, estándares, metodología y normas, aplicables a todas las áreas de Informática así como a los usuarios, que establezcan el marco de funcionamiento.

Control Interno Informático: Ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y ser diseñados conforme a los objetivos de negocio y dentro del marco legal aplicable. Éstos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles establecidos de Control Interno Informático informando de las

desviaciones a la Dirección de Informática y sugiriendo cuantos cambios crea convenientes en los controles, así como transmitirá constantemente a toda la organización de Informática la cultura y políticas del riesgo informático.

Auditor interno/externo informático: Ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

A continuación se indican algunos controles internos (no todos los que deberían definirse) para sistemas de información, agrupados por secciones funcionales, y que serían los que Control Interno Informático y Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

1. Controles generales organizativos

- Políticas: deberán servir de base para la planificación, control y evaluación por la Dirección de las actividades del Departamento de Informática.

- Planificación:
  - *Plan Estratégico de Información,* realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas tecnologías de información así como las amenazas y oportunidades de su uso o de su ausencia.
  - *Plan Informático,* realizado por el Departamento de Informática, determina los caminos precisos para cubrir las necesidades de la Empresa plasmándolas en proyectos informáticos.
  - *Plan General de Seguridad (física y lógica),* que garantice la confidencialidad, integridad y disponibilidad de la información.
  - *Plan de emergencia ante desastres,* que garantice la disponibilidad de los sistemas ante eventos.
- Estándares: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.
- Procedimientos: que describan la forma y las responsabilidades de ejecutoria para regular las relaciones entre el Departamento de Informática y los departamentos usuarios.
- Organizar el Departamento de Informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
- Descripción de las funciones y responsabilidades dentro del Departamento con una clara separación de las mismas.
- Políticas de personal: selección, plan de formación, plan de vacaciones y evaluación y promoción.
- Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.
- Asegurar que existe una política de clasificación de la información para saber dentro de la Organización qué personas están autorizadas y a qué información.
- Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática (estas dos figuras se nombrarán internamente en base al tamaño del Departamento de Informática).

2. Controles de desarrollo, adquisición y mantenimiento de sistemas de información

Para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones.

- Metodología del ciclo de vida del desarrollo de sistemas: su empleo podrá garantizar a la alta Dirección que se alcanzarán los objetivos definidos para el sistema. Éstos son algunos controles que deben existir en la metodología:

  - La alta Dirección debe publicar una normativa sobre el uso de metodología de ciclo de vida del desarrollo de sistemas y revisar ésta periódicamente.
  - La metodología debe establecer los papeles y responsabilidades de las distintas áreas del Departamento de Informática y de los usuarios, así como la composición y responsabilidades del equipo del proyecto.
  - Las especificaciones del nuevo sistema deben ser definidas por los usuarios y quedar escritas y aprobadas antes de que comience el proceso de desarrollo.
  - Debe establecerse un estudio tecnológico de viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis coste-beneficio –de cada alternativa–.
  - Cuando se seleccione una alternativa debe realizarse el plan director del proyecto. En dicho plan deberá existir una metodología de control de costes.
  - Procedimientos para la definición y documentación de especificaciones de: diseño, de entrada, de salida, de archivos, de procesos, de programas, de controles de seguridad, de pistas de auditoría, etc.
  - Plan de validación, verificación y pruebas.
  - Estándares de prueba de programas, de prueba de sistemas.
  - Plan de conversión: prueba de aceptación final.
  - Los procedimientos de adquisición de software deberán seguir las políticas de adquisición de la Organización y dichos productos debieran ser probados y revisados antes de pagar por ellos y ponerlos en uso.
  - La contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto.
  - Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.

- Explotación y mantenimiento: el establecimiento de controles asegurará que los datos se tratan de forma congruente y exacta y que el contenido de

sistemas sólo será modificado mediante autorización adecuada. Éstos son algunos de los controles que se deben implantar:

- Procedimientos de control de explotación.
- Sistema de contabilidad para asignar a usuarios los costes asociados con la explotación de un sistema de información.
- Procedimientos para realizar un seguimiento y control de los cambios de un sistema de información.

3. Controles de explotación de sistemas de información

- Planificación y Gestión de recursos: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de los equipos.

- Controles para usar, de manera efectiva los recursos en computadores:

  - Calendario de carga de trabajo.
  - Programación de personal.
  - Mantenimiento preventivo del material.
  - Gestión de problemas y cambios.
  - Procedimientos de facturación a usuarios.
  - Sistema de gestión de la biblioteca de soportes.

- Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y control de cambios.

- Seguridad física y lógica:

- Definir un grupo de seguridad de la información, siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes.
- Controles físicos para asegurar que el acceso a las instalaciones del Departamento de Informática queda restringido a las personas autorizadas.
- Las personas externas a la Organización deberán ser acompañadas por un miembro de la plantilla cuando tengan que entrar en las instalaciones.
- Instalación de medidas de protección contra el fuego.
- Formación y concienciación en procedimientos de seguridad y evacuación del edificio.
- Control de acceso restringido a los computadores mediante la asignación de un identificados de usuario con palabra clave personal e intransferible.

- Normas que regulen el acceso a los recursos informáticos.
- Existencia de un plan de contingencias para el respaldo de recursos de computador críticos y para la recuperación de los servicios del Departamento Informático después de una interrupción imprevista de los mismos.

4. Controles en aplicaciones

Cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, validez y mantenimiento completos y exactos de los datos. Las cuestiones más importantes en el control de los datos son:

- Control de entrada de datos: procedimientos de conversión y de entrada, validación y corrección de datos.

- Controles de tratamientos de datos para asegurar qae no se dan de alta, modifican o borran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.

- Controles de salidas de datos: sobre el cuadre y reconciliación de salidas, procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

5. Controles específicos de ciertas tecnologías

- Controles en Sistemas de Gestión de Bases de Datos:

- El software de gestión de bases de datos para prever el acceso a, la estructuración de, y el control sobre los datos compartidos, deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.
- Que están definidas las responsabilidades sobre la planificación, organización, dotación y control de los activos de datos, es decir, un administrador de datos.
- Que existen procedimientos para la descripción y los cambios de datos así como para el mantenimiento del diccionario de datos.
- Controles sobre el acceso a datos y de concurrencia.
- Controles para minimizar fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación.
- Controles para asegurar la integridad de los datos: programas de utilidad para comprobar los enlaces físicos –punteros– asociados a los datos, registros de

control para mantener los balances transitorios de transacciones para su posterior cuadre con totales generados por el usuario o por otros sistemas.

- Controles en informática distribuida y redes:

- Planes adecuados de implantación, conversión y pruebas de aceptación para la red.
- Existencia de un grupo de control de red.
- Controles para asegurar la compatibilidad de conjunto de datos entre aplicaciones cuando la red es distribuida.
- Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión con la distribución del contenido de bases de datos entre los departamentos que usan la red.
- Que se identifican todos los conjuntos de datos sensibles de la red y que se han determinado las especificaciones para su seguridad.
- Existencia de inventario de todos los activos de la red.
- Procedimientos de respaldo del hardware y del software de la red.
- Existencia de mantenimiento preventivo de todos los activos.
- Que existen controles que verifican que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.
- Controles de seguridad lógica: control de acceso a la red, establecimiento de perfiles de usuario.
- Procedimientos de cifrado de información sensible que se transmite a través de la red.
- Procedimientos automáticos para resolver cierres del sistema.
- Monitorización para medir la eficiencia de la red.
- Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local dentro de la organización.
- Detectar la correcta o mala recepción de mensajes.
- Identificar los mensajes por una clave individual de usuario, por terminal, y por el número de secuencia del mensaje.
- Revisar los contratos de mantenimiento y el tiempo medio de servicio acordados con el proveedor con objeto de obtener una cifra de control constante.
- Determinar si el equipo multiplexor/concentrador/procesador frontal remoto tiene lógica redundante y poder de respaldo con realimentación automática para el caso de que falle.
- Asegurarse de que haya procedimientos de recuperación y reinicio.
- Asegurarse de que existan pistas de auditoría que puedan usarse en la reconstrucción de los archivos de datos y de las transacciones de los diversos

terminales. Debe existir la capacidad de rastrear los datos entre la terminal y el usuario.
- Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.

- Controles sobre computadores personales y redes de área local:

- Políticas de adquisición y utilización.
- Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones.
- Procedimientos de control del software contratado bajo licencia.
- Controles de acceso a redes, mediante palabra clave, a través de computadores personales.
- Revisiones periódicas del uso de los computadores personales.
- Políticas que contemplen la selección, adquisición e instalación de redes de área local.
- Procedimientos de seguridad física y lógica.
- Departamento que realice la gestión y soporte técnico de la red. Controles para evitar modificar la configuración de una red. Recoger información detallada sobre los Minis existentes: Arquitectura (CPU's, Discos, Memoria, Streamers, Terminales, etc.), Conectividad (LAN, *mini to host*, etc.), software (sistema operativo, utilidades, lenguajes, aplicaciones, etc.), Servicios soportados.
- Inventario actualizado de todas las aplicaciones de la Entidad.
- Política referente a la organización y utilización de los discos duros de los equipos, así como para la nomenclatura de los archivos que contienen, y verificar que contiene al menos: obligatoriedad de etiquetar el disco duro con el número de serie del equipo, creación de un subdirectorio por usuario en el que se almacenarán todos sus archivos privados, así como creación de un subdirectorio público que contendrá todas las aplicaciones de uso común para los distintos usuarios.
- Implantar herramientas de gestión de la red con el fin de valorar su rendimiento, planificación y control.
- Procedimientos de control de los *file-transfer* que se realizan y de controles de acceso para los equipos con posibilidades de comunicación. Políticas que obliguen a la desconexión de los equipos de las líneas de comunicación cuando no se está haciendo uso de ellas.
- Adoptar los procedimientos de control y gestión adecuados para la integridad, privacidad, confidencialidad y seguridad de la información contenida en redes de área local.

- Cuando exista conexión PC-Host, comprobar que opera bajo los controles necesarios para evitar la carga/extracción de datos de forma no autorizada.
- Contratos de mantenimiento (tanto preventivo como correctivo o detectivo).
- Cuando en las acciones de mantenimiento se requiera la acción de terceros o la salida de los equipos de los límites de la oficina, se deberán establecer procedimientos para evitar la divulgación de información confidencial o sensible.
- Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo.
- Los computadores deberán estar conectados a equipos de continuidad (UPS's, grupo, etc.).
- Protección contra incendios, inundaciones o electricidad estática.
- Control de acceso físico a los recursos microinformáticos: Llaves de PC's. Áreas restringidas. Ubicación de impresoras (propias y de red). Prevención de robos de dispositivos. Autorización para desplazamientos de equipos. Acceso físico fuera de horario normal.
- Control de acceso físico a los datos y aplicaciones: almacenamiento de disquetes con copias de backup u otra información o aplicación, procedimientos de destrucción de datos e informes confidenciales, identificación de disquetes/cintas, inventario completo de disquetes almacenados, almacenamiento de documentación.
- En los computadores en que se procesen aplicaciones o datos sensibles instalar protectores de oscilación de línea eléctrica y sistemas de alimentación ininterrumpida.
- Implantar en la red local productos de seguridad así como herramientas y utilidades de seguridad.
- Adecuada identificación de usuarios en cuanto a las siguientes operaciones: altas, bajas y modificaciones, cambios de password, explotación del log del sistema.
- Controlar las conexiones remotas in/out (CAL): Modems, Gateways, Mapper.
- Procedimientos para la instalación o modificación de software y establecer que la dirección es consciente del riesgo de virus informáticos y otros software maliciosos, así como de fraude por modificaciones no autorizadas de software y daños.
- Controles para evitar la introducción de un sistema operativo a través de disquete que pudiera vulnerar el sistema de seguridad establecido.

2.4. CONCLUSIONES

La importancia alcanzada por el uso de la informática durante los últimos años ha sido espectacular. Tras este fenómeno se encuentra el deseo de beneficiarse de los cuatro grandes logros que esta tecnología ha aportado:

- Racionalización de costos.
- Mejora de la capacidad de toma de decisiones, haciendo éstas más rápidas y de menor riesgo, al contar, de manera casi inmediata, con la información precisa. Mejora de la calidad de los servicios debido al incremento de la capacidad para adaptarse dinámicamente al mercado.
- Nacimiento de servicios a clientes basados en la nueva tecnología sin cuyo uso serían imposibles de ofrecer.

La informática no es algo neutro en la empresa, sino que tiene un efecto estructurante que, añadido a su carácter cada vez más intensivo, a la variedad creciente de las aplicaciones y a la de los medios distribuidos, la hacen estratégica. Todo ello ha permitido mejorar, de manera sustancial, los resultados económicos al tiempo que se han disparado los costes de las inversiones informáticas.

La informática no sólo ha dejado de ser una simple herramienta para transformarse en un modo de estructuración de la empresa, sino que la información es uno de los activos más importantes. Las aplicaciones de un funcionamiento anormal, aunque sea temporal, de la informática tendrán repercusiones cada vez más graves para la empresa, pudiendo incluso poner en peligro su supervivencia ante la enorme dependencia de los sistemas informáticos. La integración, en particular gracias a las redes, hace el problema todavía más grave: las consecuencias de una anomalía pueden propasarse al exterior de la empresa e incluso alcanzar al usuario final. No hay que ocultar los problemas con el pretexto de tranquilizarse, sino que conviene prepararse para aportar soluciones aun cuando éstas sean parciales al principio.

Es responsabilidad de la Dirección plantear una estrategia de inversiones en recursos informáticos así como implantar sistemas de controles internos de manera que se garanticen unos grados de eficiencia y seguridad suficientes de los activos informáticos. Como consecuencia, aumenta la complejidad de las necesidades de control y auditoría surgiendo en las organizaciones como medidas preventivas, detectivas y correctivas las figuras de Control Interno y Auditoría Informáticos.

Es preciso supervisar continuamente los controles internos informáticos para asegurarse de que el proceso funciona según lo previsto. Esto es muy importante, porque a medida que cambian los factores internos y externos, controles que una vez resultaron idóneos y efectivos pueden dejar de ser adecuados y de dar a la Dirección la razonable seguridad que ofrecían antes.

Las funciones de Control Interno y Auditoría Informáticos prestan un servicio de valor añadido al ayudar a las organizaciones y a sus directivos a cumplir sus obligaciones relativas al control interno mediante el proceso de recoger, agrupar y evaluar evidencias para determinar así un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la Organización y utiliza eficientemente los recursos.

2.5. LECTURAS RECOMENDADAS

EDP Auditing. Auerbach Publications.

Fitzgerald, Jerry. *Controles internos para sistemas de computación*. Ed. Limusa Wiley.

Martin, James. *Security, Accuracy and Privacy in Computer System*. Ed. Prentice Hall.

Seguridad integral en las organizaciones. Ed. Trillas.

Instituto Auditores Internos de España. *Control interno, auditoría y seguridad informática.*

2.6. CUESTIONES DE REPASO

1. ¿Qué cambios en las empresas provocan tensión en el control interno existente?
2. ¿Cuáles son las funciones del control interno informático?
3. ¿Cuáles son los objetivos de la Auditoría Informática?
4. ¿Cuáles son las semejanzas y diferencias entre Control Interno y Auditoría Informática?
5. Ponga ejemplos de controles correctivos en diversas áreas informáticas.
6. ¿Cuáles son los principales controles en el área de desarrollo?
7. ¿Qué procesos definiría para controlar la informática distribuida y las redes?
8. ¿Qué controles se deberían establecer en las aplicaciones?

9. ¿Cómo justificaría ante un directivo de empresa la inversión necesaria en control y auditoría informática?

10. Describa la informática como modo de estructuración de las empresas.

CAPÍTULO 3

METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORÍA INFORMÁTICA

José María González Zubieta

3.1. INTRODUCCIÓN A LAS METODOLOGÍAS

Según el *Diccionario de la Lengua de la Real Academia Española,* MÉTODO es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra METODOLOGÍA como "conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal". Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad que llamaremos METODOLOGÍA.

La Informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, y cómo no, la auditoría de los sistemas de información.

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de "acierto /error".

Asimismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

La proliferación de metodologías en el mundo de la auditoría y el control informáticos se pueden observar en los primeros años de la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos). Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de metodologías constituye una practica habitual. Una de ellas es la seguridad de los sistemas de información.

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada está más lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

Éste y no otro, debe ser el campo de actuación de un auditor informática de finales del siglo XX, en uno de los grandes símbolos del desarrollo tecnológico de la época de la humanidad que nos ha tocado vivir.

Si definimos la "SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN" como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

Por tanto, el nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

Resumiendo, la informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de contramedidas, y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos. Ésta es una de las funciones de los auditores informáticos. Por tanto, debemos profundizar más en ese entramado de contramedidas para ver qué papel tienen las metodologías y los auditores en el mismo. Para explicar este aspecto diremos que cualquier contramedida nace de la composición de varios factores expresados en el "gráfico valor" de la figura 3.1.

Todos los factores de la pirámide intervienen en la composición de una contramedida.

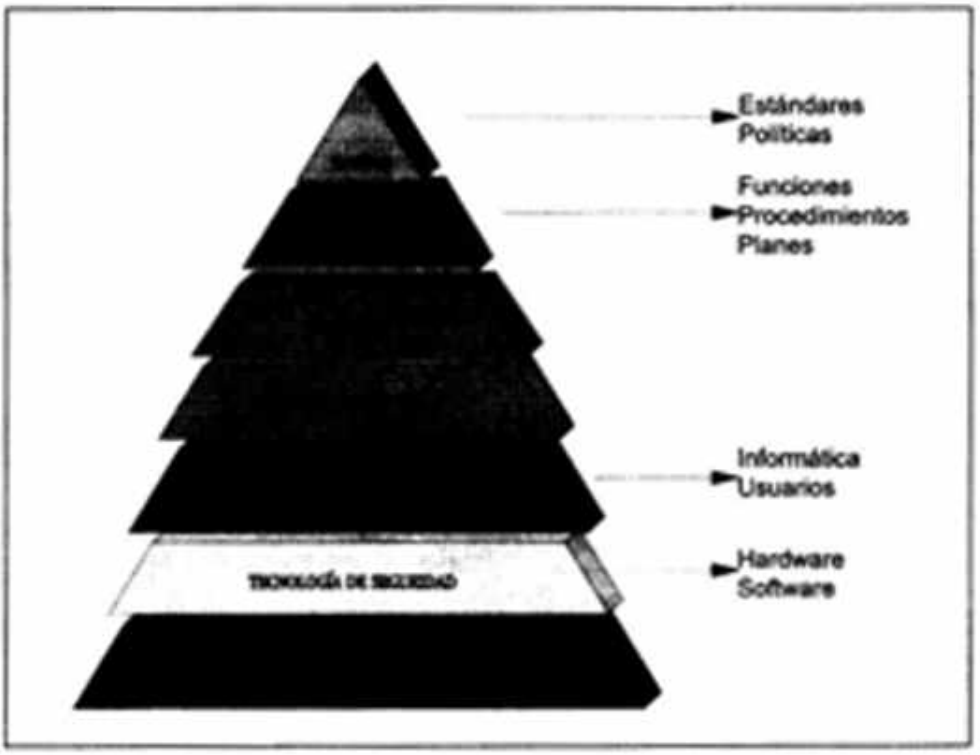


Figura 3.1. Factores que componen una contramedida

- **LA NORMATIVA** debe definir de forma clara y precisa todo lo que debe existir y ser cumplido, tanto desde el punto de vista conceptual, como práctico, desde lo general a lo particular. Debe inspirarse en estándares, políticas, marco jurídico, políticas y normas de empresa, experiencia y práctica profesional. Desarrollando la normativa, debe alcanzarse el resto del **"gráfico valor".** Se puede dar el caso en que una normativa y su carácter disciplinario sea el único control de un riesgo, pero no es frecuente.

- **LA ORGANIZACIÓN** la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Éste es el aspecto más importante, dado que sin él, nada es posible. Se pueden establecer controles sin alguno de los demás aspectos, pero nunca sin personas, ya que son estas las que realizan los procedimientos y desarrollan los Planes (Plan de Seguridad, Plan de contingencias, auditorías, etc.).

- **LAS METODOLOGÍAS** son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

- **LOS OBJETIVOS DE CONTROL** son los objetivos a cumplir en el control de procesos. Este concepto es el más importante después de "LA ORGANIZACIÓN", y solamente de un planteamiento correcto de los mismos saldrán unos procedimientos eficaces y realistas.

- **LOS PROCEDIMIENTOS DE CONTROL** son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por tanto, deben de estar documentados y aprobados por la Dirección. La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al "control o contramedida", pero no debemos olvidar que "UNA HERRAMIENTA NUNCA ES UNA SOLUCIÓN SINO UNA AYUDA PARA CONSEGUIR UN CONTROL MEJOR". Sin la existencia de estos procedimientos, las herramientas de control son solamente una anécdota.

- Dentro de la **TECNOLOGÍA DE SEGURIDAD** están todos los elementos, ya sean **hardware** o **software,** que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifradores, autentificadores, equipos "tolerantes al fallo", las herramientas de control, etc.

- **LAS HERRAMIENTAS DE CONTROL** son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, así como la calidad de cada uno con la de los demás. Cuando se evalúa el nivel de **Seguridad de Sistemas** en una institución, se están evaluando todos estos factores **(pirámide)** y se plantea un **Plan de Seguridad** nuevo que mejore todos los factores, aunque conforme vayamos realizando los distintos proyectos del plan, no irán mejorando todos por igual. Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

Llamaremos PLAN DE SEGURIDAD a una estrategia planificada de acciones y productos que lleven a un sistema de información y sus centros de proceso de una situación inicial determinada (y a mejorar) a una situación mejorada.

En la figura 3.2 se expone la tendencia actual en la organización de la seguridad de sistemas en la empresa. Por una parte un comité que estaría formado por el director de la estrategia y de las políticas. Y por otra parte control interno y auditoría informáticos. La función de control interno se ve involucrada en la realización de los procedimientos de control y es una labor de día a día. La función de auditoría informática está centrada en la evaluación de los distintos aspectos que designe su PLAN AUDITOR, con unas características de trabajo que son las visitas concretas al centro, con objetivos concretos y, tras terminar su trabajo, la presentación del informe de resultados. Por tanto, las características de su función son totalmente distintas. Lógicamente también sus métodos de trabajo.

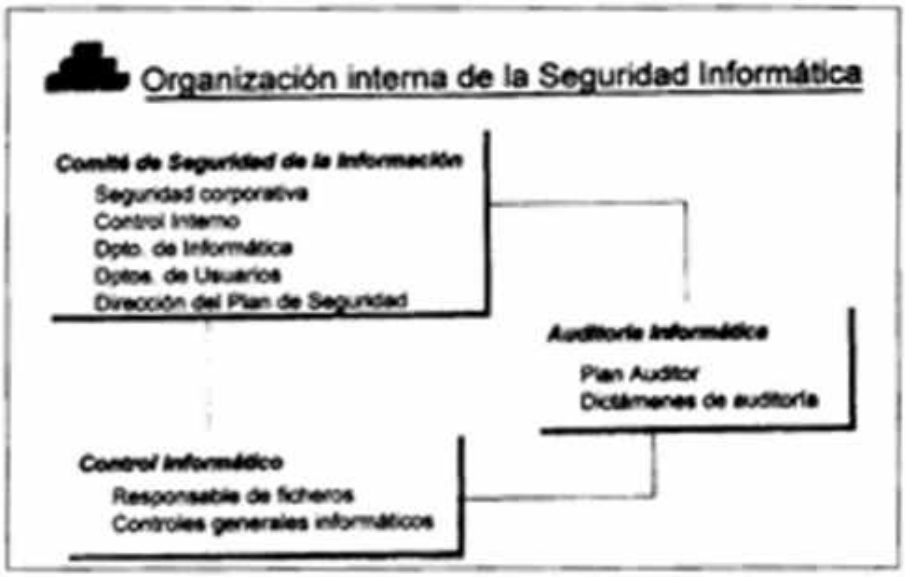


Figura 3.2. Organización interna de la seguridad informática

Queda, pues, por decir que ambas funciones deben ser independientes de la informática, dado que por la disciplina laboral la labor de las dos funciones quedaría mediatizada y comprometida. Esto es lo que se llama "segregación de funciones" entre éstas y la informática.

3.2. METODOLOGÍAS DE EVALUACIÓN DE SISTEMAS

3.2.1. Conceptos fundamentales

En el mundo de la seguridad de sistemas se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática.

Las dos metodologías de evaluación de sistemas por antonomasia son las de ANÁLISIS DE RIESGOS y las de AUDITORÍA INFORMÁTICA, con dos enfoques distintos. La auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras el análisis de riesgos facilita la "evaluación" de los riesgos y recomienda acciones en base al costo-beneficio de las mismas.

Introduzcamos una serie de definiciones para profundizar en estas metodologías.

- AMENAZA: una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplos: inundación, incendio, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de

datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

- VULNERABILIDAD: La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático. Ejemplos: falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de soportes magnéticos, falta de separación de entornos en el sistema, falta de cifrado en las telecomunicaciones, etc.

- RIESGO: La probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.

- EXPOSICIÓN O IMPACTO: La evaluación del efecto del riesgo. Ejemplo: es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.

Las amenazas reales se presentan de forma compleja y son difíciles de predecir. Ejemplo: por varias causas se rompen las dos entradas de agua, inundan las líneas telefónicas (pues existe un poro en el cable), hay un cortocircuito y se quema el transformador de la central local. En estos casos la probabilidad resultante es muy difícil de calcular.

Las metodologías de análisis de riesgos se utilizan desde los años setenta, en la industria del seguro basándose en grandes volúmenes de datos estadísticos agrupados en tablas actuarias. Se emplearon en la informática en los ochenta, y adolecen del problema de que los registros estadísticos de incidentes son escasos y, por tanto, el rigor científico de los cálculos probabilísticos es pobre. Aunque existen bases de incidentes en varios países, estos datos no son muy fiables por varios motivos: la tendencia a la ocultación de los afectados, la localización geográfica, las distintas mentalidades, la informática cambiante, el hecho de que los riesgos se presentan en un período de tiempo solamente (ventana de criticidad), etc.

Todos los riesgos que se presentan podemos:

- EVITARLOS (por ejemplo: no construir un centro donde hay peligro constante de inundaciones).
- TRANSFERIRLOS (por ejemplo: uso de un centro de cálculo contratado).
- REDUCIRLOS (por ejemplo: sistema de detección y extinción de incendios).
- ASUMIRLOS. Que es lo que se hace si no se controla el riesgo en absoluto.

Para los tres primeros, se actúa si se establecen controles o contramedidas. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo más baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

3.2.2. Tipos de metodologías

Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informáticos, se pueden agrupar en dos grandes familias. Éstas son:

- Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo.
- Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

3.2.2.1. Metodologías cuantitativas

Diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencias son datos de probabilidad de ocurrencia (riesgo) de un evento que se debe extraer de un registro de incidencias donde el número de incidencias tienda al infinito o sea suficientemente grande. Esto no pasa en la práctica, y se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podríamos aceptarlo.

Hay varios coeficientes que conviene definir:

- A.L.E. *(Annualized Loss Expentacy):* multiplicar la pérdida máxima posible de cada bien/recurso por la amenaza con probabilidad más alta.
- Reducción del A.L.E. *(Annualized Loss Expectancy):* Es el cociente entre el *coste anualizado* de la instalación y el mantenimiento de la medida contra el valor total del bien/recurso que se está protegiendo, en tanto por ciento.
- Retorno de la inversión (R.O.I.): A.L.E. original menos A.L.E. reducido (como resultado de la medida), dividido por el coste anualizado de la medida.

Todos estos coeficientes y otros diseñados por los autores de las metodologías son usados para el juego de simulación que permite elegir entre varias contramedidas en el análisis de riesgos.

Por tanto, vemos con claridad dos grandes inconvenientes que presentan estas metodologías: por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otra la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden acaecer frente a la ventaja de poder usar un modelo matemático para el análisis.

3.2.2.2. Metodologías cualitativas/subjetivas

Basadas en métodos estadísticos y lógica borrosa (humara, no matemática, *fuzzy logic*). Precisan de la *involucración* de un profesional experimentado. Pero requieren menos recursos humanos/tiempo que las metodologías cuantitativas.

La tendencia de uso en la realidad es la mezcla de ambas. En la figura 3.3 se observa un cuadro comparativo.

	Cuantitativa	Cualitativa / Subjetiva
PROS	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra "justificante" para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Incluye factores intangibles.
CONTRAS	Estimación de probabilidad depende de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodologías estándares. Difíciles de mantener o modificar. Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. Dependencia de un profesional.

Figura 3.3. Comparación entre metodologías cuantitativas y cualitativas

3.2.3. Metodologías más comunes

Las metodologías más comunes de evaluación de sistemas que podemos encontrar son de análisis de riesgos o de diagnósticos de seguridad, las de plan de contingencias, y las de auditoría de controles generales.

3.2.3.1. Metodologías de análisis de riesgos

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. Existen dos tipos: LAS CUANTITATIVAS y LAS CUALITATIVAS, de las que existen gran cantidad de ambas clases y sólo citaremos algunas de ellas.

El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado en la figura 3.4.

Figura 3.4. Esquema básico de una metodología de análisis de riesgos

En base a unos cuestionarios se identifican vulnerabilidades y riesgos y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que llamaremos "¿QUÉ PASA SI...?") analizamos el efecto de las distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación.

De forma genérica las metodologías existentes se diferencian en:

- Si son cuantitativas o cualitativas, o sea si para el "¿Qué pasa si...?" utilizan un modelo matemático o algún sistema cercano a la elección subjetiva. Aunque, bien pensado, al aproximar las probabilidades por esperanzas matemáticas subjetivamente, las metodologías cuantitativas, aunque utilicen aparatos matemáticos en sus simulaciones, tienen un gran componente subjetivo.
- Y además se diferencian en el propio sistema de simulación.

En el INFOSEC'92 proyecto S2014 se identificaron 66 metodologías de las cuales, por limitaciones de tiempo, se analizaron sólo 12 con sus respectivos paquetes,

y así el informe de este trabajo acabó siendo un contraste de las prestaciones de dichos paquetes según los fabricantes y la opinión de los consultores del equipo. Estos métodos analizados eran: ANALIZY, BDSS, BIS RISK ASSESOR, BUDDY SYSTEM, COBRA, CRAMM, DDIS MARION AP+, MELISA, RISAN, RISKPAC, RISKWATCH.

Después de estas metodologías han nacido muchas otras como, por ejemplo, la MAGERIT, desarrollada por la administración española. Citaremos algunas a modo de ejemplo:

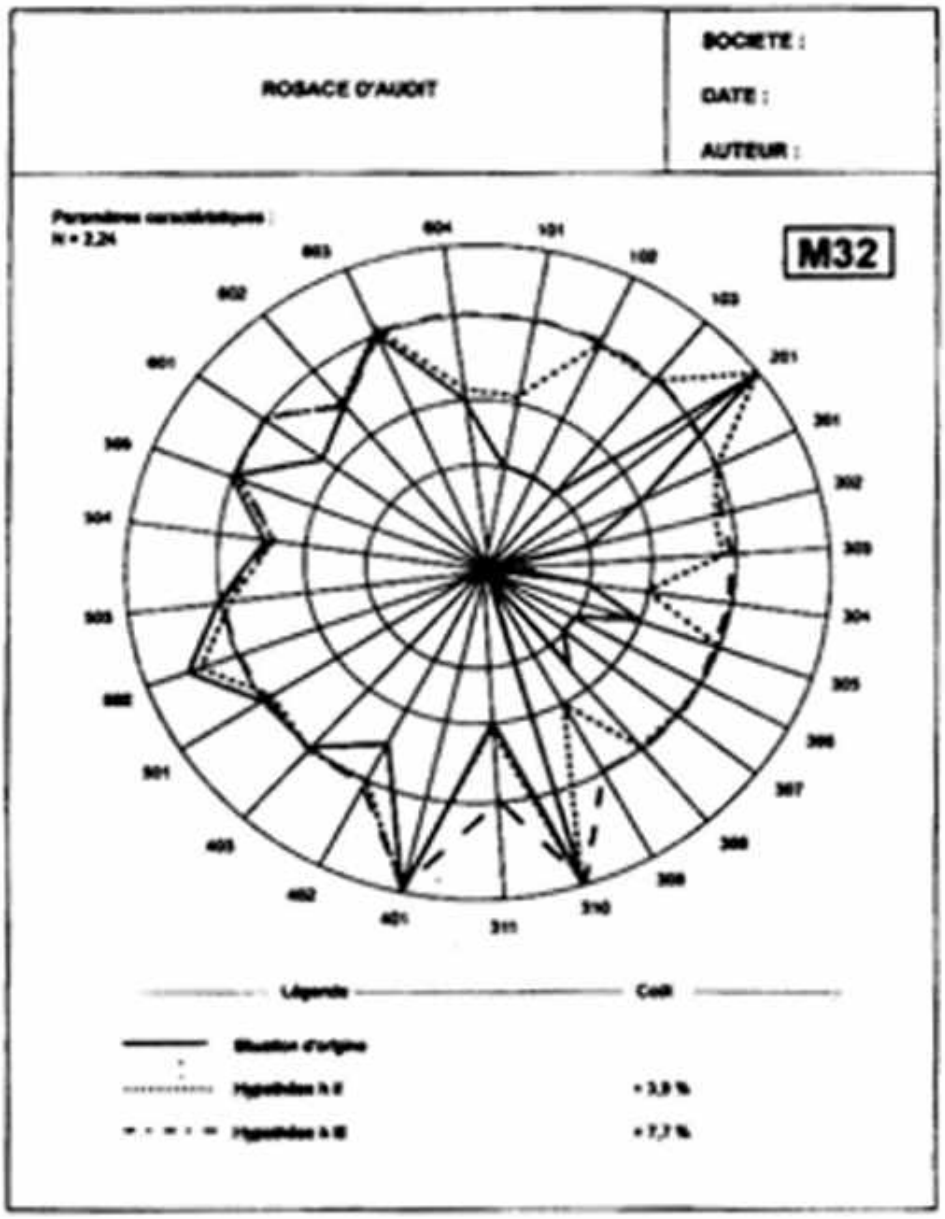


Figura 3.5. Diagrama de vulnerabilidad

CHAPITRE: Appréciation générale de la securité		Nº 1	Ponderation: 95		Page:
FACTEUR DE SECURITE: Organisation générale		Nº 01	Ponderation: 95		Page:
QUESTION	LIBELLE		NOTE	PONDÉRATION	RESPONSE PONDEREE
01	Existe-t-il un organigramme hiérachique de l'intreprise remis à jour périodiquement (au moins une fois par an)?			0,5	
02	Existe-t-il un organigramme fonctionnel de l'entreprise remis à jour périodiquement (au moins une fois par an)?			0,5	
03	Y a-t-il une réunion de Direction Générale de présentation de l'organigramme à laquelle participent tous les responsables de fonction?			0,5	
04	Existe-t-il une définition de fonction et partage des responsabilités pour chaque poste furant sur l'organigramme?			1	
05	La Direction Générale manifeste-t-elle son interêt par des réunions specifiques de sécurité (hors CHSCT) au moins une fois par an?			1,5	
06	Existe-t-il un comité permanent chargé d'étudier tous les problèmes liés à la sécurité, composé de représentants de la D.G., direction informatique et organisation, fonctions utilisateurs, audit interne, getion de risques juridique et assurances, se réunissant au moins quatre fois par an?			3	
07	Le compte rendu de ces réunions est-il consigné dans un rapport précédemment cité?			1	
08	Y a-t-il un suivi et un contrôle des recommandations prescrites par le rapport précédemment cité?			1	
09	Y a-t-il eu une étude sur la vulnerabilité de l'entreprise face à différéents types de risques physiques ou non physiques (pas nécessairement informatiques) dans les trois dernières annés (rapport écrit)?			3	
10	Cette étude a-t-elle entraine la mise en place d'un plan de sauvegarde de l'entreprise?			3	
11	Existe-t-il un responsable de la sécurité générale (bâtiments, environnement, accès)?			2	
12	La sécurité informatique dispose-t-elle d'un poste spécifique sur l'organigramme avec un rattachement hiérchique élevé assorti d'une définition de fonction précisant clairment les responsabilités et d'un bugget spécifique?			3,5	
13	Y a-t-il ou responsable "Assurances" dans l'entreprise?			0,5	
14	Le choix des garanties en mebère informatique est-il le résultat d'une étude spécifique?			0,5	

Figura 3.6. Cuestionario para valorar la seguridad

MARION

Método documentado en dos libros de los cuales el más actual es *La Securité des reseaux-Methodes et Techniques* de J.M. Lamere y Leroux, J. Tourly. Tiene dos productos: MARION AP+, para sistemas individuales, y MARION RSX para sistemas distribuidos y conectividad.

Es un método cuantitativo y se basa en la encuesta anual de miembros del C.L.U.S.1.F. (base de incidentes francesa). No contempla probabilidades, sino esperanzas matemáticas que son aproximaciones numéricas (valores subjetivos).

La MARION AP+ utiliza cuestionarios y parámetros correlacionados enfocados a la representación gráfica de las distintas soluciones de contramedidas (figura 3.5), en cada uno de los factores (27 factores en seis categorías). Las categorías son: seguridad informática general, factores socioeconómicos, concienciación sobre la seguridad de software y materiales, seguridad en explotación y seguridad de desarrollo.

Secteur	Catégorie	
I	– Etablissements financiers.	2,20
	– Banques.	2,61
	– Assurances.	2,04
II	– Agriculture.	1,24
	– Energie, extraction.	2,53
	– Métalurgie, sidérurgie.	2,00
	– Construction aéronautique, automobile, mécanique, électrique.	2,00
	– Electronique, optique, informatique.	2,35
	– Verre, céramique.	1,82
	– Chimie, pharmacie.	2,28
	– Pétrole et dérivés.	2,61
	– Agro-alimentaire.	1,95
	– Textile, habillement.	2,08
	– Industries diverses.	2,28
	– Bâtiment, TP.	1,82
III	– Transport.	1,78
	– Transmissions, télécommunications.	2,21
	– Distribution, commerce.	2,10
	– Hôtellerie.	2,41
	– Sociétés de services.	2,28
	– Administration.	2,14
	– Santé.	2,29
	– Enseignement.	1,35
	– Publicité, presse, éditions.	2,06
	– Divers.	1,63

DEFINICIÓN SECTORIAL I, II, III USADO.

Figura 3.7. Valores de ponderación para diferentes sectores

En la figura 3.6 se puede ver un cuestionario al que hay que responder sí con un 4, no con un cero, y 3 *no aplicable*, para luego aplicarles unos valores de ponderación según los sectores de la figura 3.7 de negocio de la empresa donde se esté pasando la metodología. El cuestionario de la figura 3.6 correspondería al factor 101.

El análisis de riesgos lo hace sobre diez áreas problemáticas con otros cuestionarios. Estas áreas son riesgos materiales, sabotajes físicos, averías, comunicaciones, errores de desarrollo, errores de explotación, fraude, robo de información, robo de software, problemas de personal. Sirve para evaluar el impacto (figura 3.8).

Groupe d'interview:	Fonction:	Auteur:
Participants:	Sous-Fontions:	Date:
Binôme d'interview:	Application:	

M11-U2

Type de Pertes / Type de Risques	Dommages matériels	Frais Suppl.	Pertes d'expl.	Pertes de biens	Pertes de fonds	Autres Pertes
1. Risques matériels						
2. Sabotage physique						
3. Pannes						
4. Erreurs (saisie, transmission)						
5. Erreurs (conception, realisation)						
6. Erreurs (exploitation)						
7. Fraude, détournement, sabotage immatériel						
8. Détournement d'information						
9. Détournement de logiciel						
10. Problèmes humains						

DEFINICIÓN CUALITATIVA DE PÉRDIDAS (MARION AP+)

Figura 3.8. Definición cualitativa de pérdidas

Las pérdidas posibles no deben sobrepasar nunca el valor del "RIESGO MÁXIMO ADMISIBLE", valor extraído de los valores dados por un estudio del Banco de Francia donde figuran 50 ratios para distintas áreas sectoriales ya mencionadas en la figura 3.7. El diagrama de la figura 3.5 se llama de radar, y la metodología MELISA usa uno similar. Esta metodología es de las más antiguas y difíciles de entender y manejar.

RISCKPAC

Todas las metodologías que se desarrollan en la actualidad están pensadas para su aplicación en herramientas. La primera de esta familia la desarrolló PROFILE ANALYSIS CORPORATION, y la primera instalación en cliente data de 1984. Según DATAPRO es el software más vendido.

Su enfoque es metodología cualitativa/subjetiva. Sus resultados son exportables a procesadores de texto, bases de datos, hoja electrónica o sistemas gráficos. Está estructurada en los tres niveles Entorno/Procesador/Aplicaciones con 26 categorías de riesgo en cada nivel. Tiene un "¿qué pasa si...?" con un nivel de riesgo de evaluación subjetiva del 1 al 5 y ofrece una lista de contramedidas o recomendaciones básicas para ayuda al informe final o plan de acciones.

CRAMM

Se desarrolló entre 1985 y 1987 por BIS y CCTA (CENTRAL COMPUTER & TELECOMUNICATION AGENCY RISK ANALISIS & MANAGEMENT METHOD, Inglaterra). Implantado en más de 750 organizaciones en Europa, sobre todo de la administración pública. Es una metodología cualitativa y pennite hacer análisis "¿Qué pasa si...?".

PRIMA (PREVENCIÓN DE RIESGOS INFORMÁTICOS CON METODOLOGÍA ABIERTA)

Es un compendio de metodologías españolas desarrolladas entre los años 1990 y la actualidad con un enfoque subjetivo. Sus características esenciales son:

- Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad.
- Fácilmente adaptable a cualquier tipo de herramienta.
- Posee cuestionarios de preguntas para la identificación de debilidades o faltas de controles.

- Posee listas de ayuda para los usuarios menos experimentados de debilidades, riesgos y contramedidas (sistema de ayuda).
- Permite fácilmente la generación de informes finales.
- Las "Listas de ayuda" (figura 3.10) y los cuestionarios son abiertos, y por tanto es posible introducir información nueva o cambiar la existente. De ahí la expresión Abierta de su nombre.
- Tiene un "¿qué pasa si...?" cualitativo, y capacidad de aprendizaje al poseer una base de conocimiento o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo.

En las figuras 3.9 y 3.10 se expone la metodología de análisis de riesgos PRIMA.

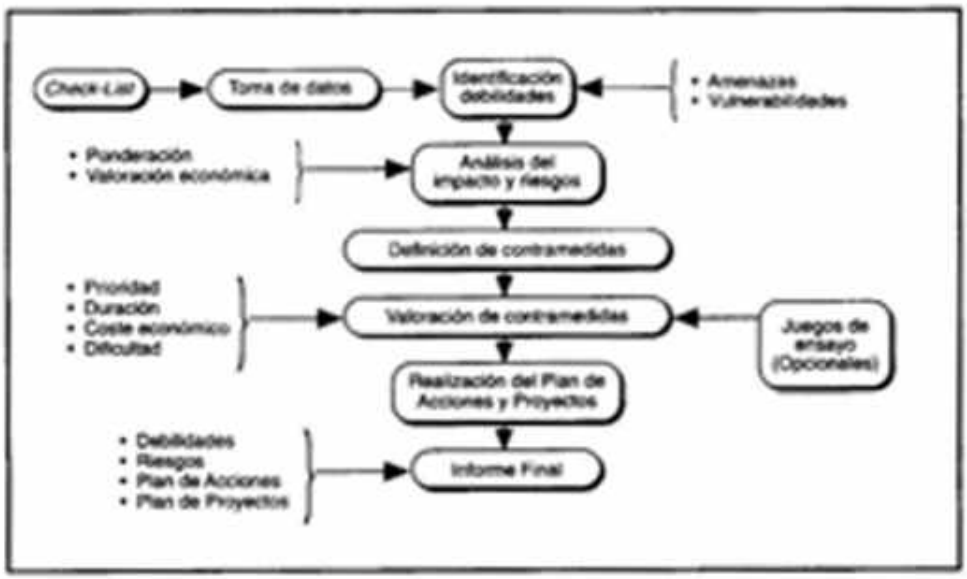


Figura 3.9. Fases de la metodología PRIMA

Con la misma filosofía abierta existen del mismo autor, en la actualidad, las siguientes metodologías:

- Análisis de riesgos.
- Plan de contingencias informática y de recuperación del negocio.
- Plan de restauración interno informático.
- Clasificación de la información.
- Definición y desarrollo de procedimientos de control informáticos.
- Plan de cifrado.
- Auditoría informática.
- Definición y desarrollo de control de acceso lógico. Entornos distribuidos y single *sig-on*.

Figura 3.10. Lista de ayuda de la metodología PRIMA

3.2.3.2. Plan de contingencias

El auditor debe conocer perfectamente los conceptos de un plan de contingencias para poder auditarlo. Hay varias formas de llamarlo, pero conviene no confundir los conceptos que se manejan alrededor de los nombres. El plan de contingencias y de recuperación del negocio es lo mismo, pero no así el plan de restauración interno. Éste va enfocado hacia la restauración del C.P.D., pero sobre eventos que suceden dentro del entorno (caídas del sistema, roturas leves, etc.), y cuya duración no afecta gravemente a la continuidad del negocio.

También se manejan a veces los conceptos de plan de contingencias informática y plan, de contingencias corporativo, cuyos conceptos son sólo de alcance. El corporativo cubre no sólo la informática, sino todos los departamentos de una entidad, y puede incluir también el informativo como un departamento más. Frecuentemente se realiza el informático.

DEFINICIÓN. El Plan de Contingencias es una estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Esa estrategia, materializada en un manual, es el resultado de todo un proceso de análisis y definiciones que es lo que da lugar a las metodologías. Esto es, las metodologías que existen versan sobre el proceso necesario para obtener dicho plan.

Es muy importante tener en cuenta que el concepto a considerar es "la continuidad, el negocio"; estudiar todo lo que puede paralizar la actividad y producir pérdidas. Todo lo que no considere este criterio no será nunca un plan de contingencias.

FASES DE UN PLAN. Las fases de un plan son las siguientes:

FASE I. ANÁLISIS Y DISEÑO. Se estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el coste/beneficio de las mismas. Ésta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión de que no es viable o es muy costoso su seguimiento. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas. Éstas son las de "RISK ANALISIS" y las de "BUSINESS IMPACT".

Las de Risk Analisis se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Aunque los registros de incidentes, al igual que ocurría en las metodologías de análisis de riesgos, son escasos y poco fiables, aun así es más fácil encontrar este tipo de metodologías que las segundas.

Las de Bussines Impact, se basan en el estudio del impacto (pérdida económica o de imagen) que ocasiona la falta de algún recurso de los que soporta la actividad del negocio. Estas metodologías son más escasas, pero tienen grandes ventajas como es el mejor entendimiento del proceso o el menor empleo de tiempo de trabajo por ir más directas al problema.

Las tareas de esta fase en las metodologías de Risk Analisis son las siguientes:

1. Identificación de amenazas.
2. Análisis de la probabilidad de materialización de la amenaza.
3. Selección de amenazas.
4. Identificación de entornos amenazados.
5. Identificación de servicios afectados.
6. Estimación del impacto económico por paralización de cada servicio.
7. Selección de los servicios a cubrir.
8. Selección final del ámbito del Plan.
9. Identificación de alternativas para los entornos.
10. Selección de alternativas.
11. Diseño de estrategias de respaldo.
12. Selección de las estrategias de respaldo.

Las tareas para las de Business Impact son las siguientes:

1. Identificación de servicios finales.
2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos no económicos, lo que les da una ventaja en los casos en los que intervienen otros valores que no sean los económicos.
3. Selección de servicios críticos.
4. Determinación de recursos de soporte.
5. Identificación de alternativas para entornos.
6. Selección de alternativas.
7. Diseño de estrategias globales de respaldo.
8. Selección de la estrategia global de respaldo.

Como puede verse, el enfoque de esta segunda es más práctico y se va más directo a las necesidades reales de la entidad sin tener que justificar con datos de probabilidades que aportan poco por la pobreza de los datos. Éstas se basan en hechos ciertos, que se analizan y se justifican económicamente. Permiten, por tanto, hacer estudios coste/beneficio que justifican las inversiones con más rigor que los estudios de probabilidad que se obtienen con los análisis de riesgos.

Hay un factor importante a determinar en esta fase que es el *Time Frame* o tiempo que la empresa puede asumir con paralización de la actividad operativo antes de incurrir en pérdidas significativas. Este factor marcará las estrategias de recuperación y se extraerá del análisis del impacto.

FASE II: DESARROLLO DEL PLAN. Esta fase y la tercera son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.

Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la *alternativa* debe concluirse con la reconstrucción de la situación inicial antes de la contingencia, y esto es lo que no todas las metodologías incluyen.

FASE III: PRUEBAS Y MANTENIMIENTO. En esta fase se definen las pruebas, sus características y sus ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como mentalizar al personal implicado.

Asimismo se define la estrategia de mantenimiento, la organización destinada a ello y la normativa y procedimientos necesarios para llevarlo a cabo.

HERRAMIENTAS. En este caso, como en todas las metodologías la herramienta es una anécdota, y lo importante es tener y usar la metodología apropiada para

desarrollar más tarde la herramienta que se necesite. El esquema de una herramienta debe tener al menos los siguientes puntos:

- base de datos relacionar
- módulo de entrada de datos
- módulo de consultas
- proceso de textos
- generador de informes
- ayudas *on-line*
- hoja de cálculo
- gestor de proyectos
- generador de gráficos

Existen en el mercado productos que cubren estas metodologías, en menor cantidad que los de análisis de riesgos y enfocados sobre todo a análisis de riesgos con datos de poca significación científica. Hoy en día la mayoría de los equipos profesionales desarrollan su software al comienzo de los trabajos tras definir la metodología.

Es importante para terminar este punto decir que una práctica habitual es realizar la fase I y contratar un servicio de *back-up* sin desarrollar las fases II y III. Esto no sólo constituye un error conceptual, sino que en realidad sólo se tiene un estudio y un contrato de servicios pero no un PLAN DE CONTINGENCIAS.

3.3. LAS METODOLOGÍAS DE AUDITORÍA INFORMÁTICA

Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorías de CONTROLES GENERALES como producto estándar de la auditores profesionales, que son una homologación de las mismas a nivel internacional, y las METODOLOGÍAS de los auditores internos.

El objetivo de las auditorías de controles generales es "dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera". El resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generalistas.

Tienen apartados para definir "pruebas" y anotar sus resultados. Ésta es una característica clara de la diferencia con las metodologías de evaluación de la consultaría como las de análisis de riesgos *que no tienen estos apartados*, aunque también tratan de identificar vulnerabilidades o falta de controles. Esto es, la realización de pruebas es consustancial a la auditoría, dado que tanto el trabajo de consultaría como el análisis de riesgos espera siempre la colaboración del analizado, y

por el contrario la auditoría debe demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener el apartado de las pruebas. Llegando al extremo de que hay auditorías que se basan sólo en pruebas como la "auditoría de integridad".

Estas metodologías están muy desprestigiadas, pero no porque sean malas en sí mismas, sino porque dependen mucho de la experiencia de los profesionales que las usan y existe una práctica de utilizarlas profesionales sin ninguna experiencia.

Ninguna de estas metodologías usa ayudas de contramedidas, llegándose a la aberración de que se utilizan metodologías de análisis de riesgos para hacer auditorías.

Todas estas anomalías nacen de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente. Esto es una utopía. El auditor informático necesita una larga experiencia tutelada y una gran formación tanto auditora como informática. Y esta formación debe ser adquirida mediante el estudio y la práctica tutelada.

Llegamos al punto en el que es necesario decir que la metodología de auditor interno debe ser diseñada y desarrollada por el propio auditor, y ésta será la significación de su grado de experiencia y habilidad.

Por tanto, entre las dos metodologías de evaluación de sistemas (análisis de riesgos y auditoría) existen similitudes y grandes diferencias. Ambas tienen papeles de trabajo obtenidos del trabajo de campo tras el plan de entrevistas, pero los cuestionarios son totalmente distintos. Los de la figura 3.6 son de análisis de riesgos y se trata de preguntas dirigidas a la identificación de la falta de controles. Se ven dirigidas a consultores por la planificación de los tiempos y por ser preguntas más concretas.

En el punto 3.7 se expone un ejemplo real de una metodología de auditor interno necesaria para revisar cualquier aplicación. Como se ve en el ejemplo está formada por recomendaciones de plan de trabajo y de todo el proceso que debe seguir. También define el objetivo de la misma, que habrá que describirlo en el memorándum de apertura al auditado. Asimismo lo describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar.

En este caso del auditor interno informático le servirá de guía para confeccionar el programa real de trabajo de la auditoría. El auditor deberá hacer los cuestionarios más detallados si así lo estima oportuno y definir cuantas pruebas estime oportunas. Asimismo, si cuando empieza una auditoría el auditor detecta vías alternativas a revisar, su deber es seguirlas cambiando el plan de trabajo. Por tanto, el concepto de las metodologías de análisis de riesgos de "tiempos medidos" es más bien para consultores profesionales que para auditores internos. Éstos, aunque deben planificar

sus tiempos, en principio no deben constituir nunca su factor principal, dado que su función es la de vigilancia, y ésta se cumple si el auditado se siente vigilado.

El auditor interno debe crear sus metodologías necesarias para auditar los distintos aspectos o áreas que defina en el plan auditor que veremos en el siguiente punto.

También es interesante aclarar que hay herramientas software de ayuda a la auditoría de cuentas que aunque se les llame herramientas de auditoría, sólo lo son para los auditores de cuentas, y esto no es auditoría informática sino ayuda a la auditoría de cuentas.

Es decir, que no es lo mismo ser una informática de los auditores que ser auditor informático. La auditoría financiera es *un dictamen sobre los estados de cuentas.* Y la auditoría informática es una auditoría en sí misma, y si el auditor informático no certifica la integridad de los datos informáticos que usan los auditores financieros, éstos no deben usar los sistemas de información para sus dictámenes. Tal es la importancia de la existencia de los auditores informáticos, que son los garantes de la veracidad de los informes de los auditores financieros que trabajan con los datos de los sistemas de información.

El esquema metodológico del auditor está definido por el plan auditor que vemos a continuación.

3.4. EL PLAN AUDITOR INFORMÁTICO

Es el esquema metodológico más importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que realiza en la entidad. Debe estar en sintonía con el plan auditor del resto de los auditores de la entidad.

Las partes de un plan auditor informático deben ser al menos las siguientes:

- **Funciones.** Ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la Informática y de control interno informático, y éste debe ser auditado también. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

- **Procedimientos** para las distintas tareas de las auditorías. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

- **Tipos de auditorías** que realiza. Metodologías y cuestionarios de las mismas. Ejemplo: revisión de la aplicación de facturación, revisión de la LOPD, revisión de seguridad física, revisión de control interno, etc. Existen tres tipos de auditorías según su alcance: la Full o completa de una área (por ejemplo: control interno, informática, limitada a un aspecto; por ejemplo: una aplicación, la seguridad lógica, el software de base, etc.), la Corrective Action Review (CAR) que es la comprobación de acciones correctivas de auditorías anteriores.

- **Sistema de evaluación** y los distintos aspectos que evalúa. Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc., así como realizar una evaluación global de resumen para toda la auditoría. En nuestro país esta evaluación suele hacerse en tres niveles que son "Bien", "Regular", o "Mal", significando la visión de grado, de gravedad. Esta evaluación final nos servirá para definir la fecha de repetición de la misma auditoría en el futuro según el nivel de exposición que se le haya dado a este tipo de auditoría en cuestión.

CICLO DE AUDITORÍAS

Nivel Exposición	Evaluación	Frecuencia Visitas
10 - 9	"B"	18 meses
	"R"	9 meses
	"M"	6 meses
8 - 7	"B"	18 meses
	"R"	12 meses
	"M"	9 meses
6 - 5	"B"	24 meses
	"R"	18 meses
	"M"	12 meses
4 - 1	"B"	36 meses
	"R"	24 meses
	"M"	18 meses

Figura 3.11. Nivel de exposición para definir la frecuencia de la auditoría

- **Nivel de exposición.** Como ejemplo podemos ver la figura 3.11. El nivel de exposición es en este caso un número del uno al diez definido subjetivamente y que me permite en base a la evaluación final de la última auditoría realizada sobre ese tema definir la fecha de la repetición de la misma auditoría. Este número no conviene confundirlo con ninguno de los parámetros utilizados en el análisis de riesgos que está enfocado a probabilidad de ocurrencia. En este caso el valor del nivel de exposición significa la suma de factores como impacto, peso del área, situación de control en el área. O sea se puede incluso

rebajar el nivel de un área auditada porque está muy bien y no merece la pena revisarla tan a menudo.

- **Lista de distribución de informes.**
- **Seguimiento de las acciones correctoras.**
- **Plan quinquenal.** Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartiese en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas, deberá componer anualmente el plan de trabajo anual.
- **Plan de trabajo anual.** Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado nos dé un resultado de horas de trabajo previstas y, por tanto, de los recursos que se necesitarán.

Debemos hacer notar que es interesante tener una herramienta programada con metodología abierta que permita confeccionar los cuestionarios de las distintas auditorías y cubrir fácilmente los hitos y fases de los programas de trabajo una vez definida la metodología completa. Esto se puede hacer sin dificultad con cualquier herramienta potente de las que existen en la actualidad.

Las metodologías de auditoría informática son del tipo cualitativo/subjetivo. Podemos decir que son las subjetivas por excelencia. Por tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continuada. Sólo así esta función se consolidará en las entidades, esto es, por el "respeto profesional" a los que ejercen la función.

3.5. CONTROL INTERNO INFORMÁTICO. SUS MÉTODOS Y PROCEDIMIENTOS. LAS HERRAMIENTAS DE CONTROL

3.5.1 La función de control

Hoy en día la tendencia generalizada es contemplar, al lado de la figura del auditor informático, la de control interno informático. Tal es el caso de la organización internacional I.S.A.C.A. (Information Systems Audit and Control Association) que con anterioridad se llamó The EDP Auditors Association Inc.

Aunque hay una cierta polémica profesional con esta función y no existe una aceptación tan clara como la función de auditoría informática, parece razonable y sin intención de crear doctrina definirla como existe en general en muchas multinacionales.

La función de Control Informático Independiente debería ser en primer lugar independiente del departamento controlado. Ya que "por segregación de funciones la informática no debería controlarse a sí misma". Partiendo de la base de un concepto en el que la seguridad de sistemas abarca un campo mucho mayor de lo que es la seguridad lógica, podríamos decir que:

- El área informática monta los procesos informáticos seguros.
- El Control interno monta los controles.
- La Auditoría Informática evalúa el grado de control.

Por tanto, podríamos decir que existen claras diferencias entre las funciones de control informático y las de auditoría informática.

La Auditoría Informática

- Tiene la función de vigilancia y evaluación mediante dictámenes, y todas sus metodologías van encaminadas a esta función.
- Tiene sus propios objetivos distintos a los auditores de cuentas, aunque necesarios para que éstos puedan utilizar la información de sus sistemas para sus evaluaciones financieras y operativas. Evalúan eficiencia, costo y seguridad en su más amplia visión, esto es todos los riesgos informativos, ya sean los clásicos (confidencialidad, integridad y disponibilidad), o los costos y los jurídicos, dado que ya no hay una clara separación en la mayoría de los casos.
- Operan según el plan auditor.
- Utilizan metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
- Establecen planes quinquenales como ciclos completos.
- Sistemas de evaluación de repetición de la auditoría por nivel de exposición del área auditada y el resultado de la última auditoría de esta área.
- La función de soporte informático de todos los auditores (opcionalmente), aunque dejando claro que no se debe pensar con esto que la auditoría informática consiste en esto solamente.

Control Interno Informático

- Tiene funciones propias (administración de la seguridad lógica, etc.).
- Funciones de control dual con otros departamentos.
- Función normativa y del cumplimiento del marco jurídico.

- Operan según procedimientos de control en los que se ven involucrados y que luego se desarrollarán.
- Al igual que en la auditoría y de forma opcional pueden ser el soporte informático de control interno no informático.

Podemos pasar ya a proponer las funciones de control interno más comunes:

- Definición de propietarios y perfiles según "Clasificación de la Información" (utilizando metodología).
- Administración delegada en Control Dual (dos personas intervienen en una acción como medida de control) de la seguridad lógica.
- Responsable del desarrollo y actualización del Plan de Contingencias, Manuales de procedimientos y Plan de Seguridad.
- Promover el Plan de Seguridad Informática al Comité de Seguridad.
- Dictar Normas de Seguridad Informática.
- Definir los Procedimientos de Control.
- Control del Entorno de Desarrollo.
- Control de Soportes Magnéticos según la Clasificación de la Información. Control de Soportes Físicos (listados, etc.).
- Control de Información Comprometida o Sensible.
- Control de Microinformática y Usuarios.
- Control de Calidad de Software.
- Control de Calidad del Servicio Informático.
- Control de Costes.
- Responsable del Departamento (gestión de recursos humanos y técnicos). Control de Licencias y Relaciones Contractuales con terceros.
- Control y Manejo de Claves de cifrado.
- Relaciones externas con entidades relacionadas con la Seguridad de la Información.
- Definición de Requerimientos de Seguridad en Proyectos Nuevos.
- Vigilancia del Cumplimiento de las Normas y Controles.
- Control de Cambios y Versiones.
- Control de Paso de Aplicaciones a Explotación.
- Control de Medidas de Seguridad Física o corporativa en la Informática.
- Responsable de Datos Personales (LOPD y Código Penal).
- Otros controles que se le designen.
- Otras funciones que se le designen.

Todas estas funciones son un poco ambiciosas para desarrollarlas desde el instante inicial de la implantación de esta figura, pero no debemos perder el objetivo de que el control informático es el componente de la "actuación segura" entre los usuarios, la informática y control interno, todos ellos auditados por auditoría informática.

Para obtener el entramado de contramedidas o controles compuesto por los factores que veíamos en la figura 3.1, deberemos ir abordando proyectos usando distintas metodologías, tal como se observa en la figura 3.12, que irán conformando y mejorando el número de controles.

Figura 3.12. Obtención de los controles

Este plan de proyectos lo llamaremos "Plan de Seguridad Informática". Dos de estos proyectos de vital importancia son la "Clasificación de la Información" y los "Procedimientos de Control". El punto B) de la figura corresponde al primero y el C) al segundo, y sus metodologías se ven a continuación.

3.5.2. Metodologías de clasificación de la información y de obtención de los procedimientos de control

Clasificación de la información

No es frecuente encontrar metodologías de este tipo, pero la metodología PRIMA tiene dos módulos que desarrollan estos dos aspectos y que vemos a continuación.

Contemplando la figura 3.12 podríamos preguntarnos si es suficiente con un análisis de riesgos para obtener un plan de contramedidas que nos llevará a una situación de control como se desea. La respuesta es no, dado que todas las entidades de información a proteger no tienen el mismo grado de importancia, y el análisis de riesgos metodológicamente no permite aplicar una diferenciación de contramedidas según el activo o recurso que protege, sino por la probabilidad del riesgo analizado.

Tiene que ser otro concepto, como el que se baraja en la clasificación de la información. Esto es "SI IDENTIFICAMOS DISTINTOS NIVELES DE CONTRAMEDIDAS PARA DISTINTAS ENTIDADES DE INFORMACIÓN CON DISTINTO NIVEL DE CRITICIDAD, ESTAREMOS OPTIMIZANDO LA EFICIENCIA DE LAS CONTRAMEDIDAS Y REDUCIENDO LOS COSTOS DE LAS MISMAS".

Por ejemplo, si en vez de cifrar la red de comunicaciones por igual somos capaces de diferenciar por qué líneas va la información que clasificamos como Restringida a los propietarios de la misma, podremos cifrar solamente estas líneas para protegerla sin necesidad de hacerlo para todas, y de esa manera disminuiremos el costo de la contramedida "cifrado".

Tradicionalmente el concepto de información clasificada se aplicó a los documentos de papel, aunque los criterios y jerarquías nunca han sido más de dos (secreto y no). Con la tecnología de la información, el concepto ha cambiado, e incluso se ha perdido el control en entornos sensibles. Nace pues el concepto de ENTIDAD DE INFORMACIÓN como el objetivo a proteger en el entorno informático, y que la clasificación de la información nos ayudará a proteger especializando las contramedidas según el nivel de confidencialidad o importancia que tengan.

Esta metodología es del tipo cualitativo/subjetivo, y como el resto de la metodología PRIMA tiene listas de ayuda con el concepto abierto, esto es, que el profesional puede añadir en la herramienta niveles o jerarquías, estándares y objetivos a cumplir por nivel, y ayudas de contramedidas.

Ejemplos de Entidades de Información son: una pantalla, un listado, un archivo de datos, un archivo en un "streamer", una microficha de saldos, los sueldos de los directivos, los datos de tipo "salud" en un archivo de personal, una transación, un JCL, un editor, etc.

O sea los factores a considerar son los requerimientos legislativos, la sensibilidad a la divulgación (confidencialidad), a la modificación (integridad), y a la destrucción.

Las jerarquías suelen ser cuatro, y según se trate de óptica de preservación o de protección, los cuatro grupos serían: Vital-Crítica-Valuada-No sensible o bien Altamente confidencial-Confidencial-Restringida-No sensible.

PRIMA, aunque permite definirla a voluntad, básicamente define:

- Estratégica (información muy restringida, muy confidencial, vital para la subsistencia de la empresa).
- Restringida (a los propietarios de la información).

- De uso interno (a todos los empleados).
- De uso general (sin restricción).

Los pasos de la metodología son los siguientes:

1. IDENTIFICACIÓN DE LA INFORMACIÓN.

2. INVENTARIO DE ENTIDADES DE INFORMACIÓN RESIDENTES Y OPERATIVAS. Inventario de programas, archivos de datos, estructuras de datos, soportes de información, etc.

3. IDENTIFICACIÓN DE PROPIETARIOS. Son los que necesitan para su trabajo, usan o custodian la información.

4. DEFINICIÓN DE JERARQUÍAS DE INFORMACIÓN. Suelen ser cuatro, porque es difícil distinguir entre más niveles.

5. DEFINICIÓN DE LA MATRIZ DE CLASIFICACIÓN. Esto consiste en definir las políticas, estándares objetivos de control y contramedidas por tipos y jerarquías de información.

6. CONFECCIÓN DE LA MATRIZ DE CLASIFICACIÓN. En la figura 3.13 se observa un ejemplo de matriz de clasificación en la que se relaciona cada entidad de información con los elementos que se correlacionan, como son transacción, archivos, soportes, propietarios, y jerarquía. En esta fase se cumplimenta toda la matriz, asignándole a cada entidad un nivel de jerarquía, lo que la asocia a una serie de hitos a cumplir según el punto anterior, para cuyo cumplimiento deberemos desarrollar acciones concretas en el punto siguiente.

7. REALIZACIÓN DEL PLAN DE ACCIONES. Se confecciona el plan detallado de acciones. Por ejemplo, se reforma una aplicación de nóminas para que un empleado utilice el programa de subidas de salario y su supervisor lo apruebe.

8. IMPLANTACIÓN Y MANTENIMIENTO. Se implanta el plan de acciones y se mantiene actualizado.

Y así se completa esta metodología.

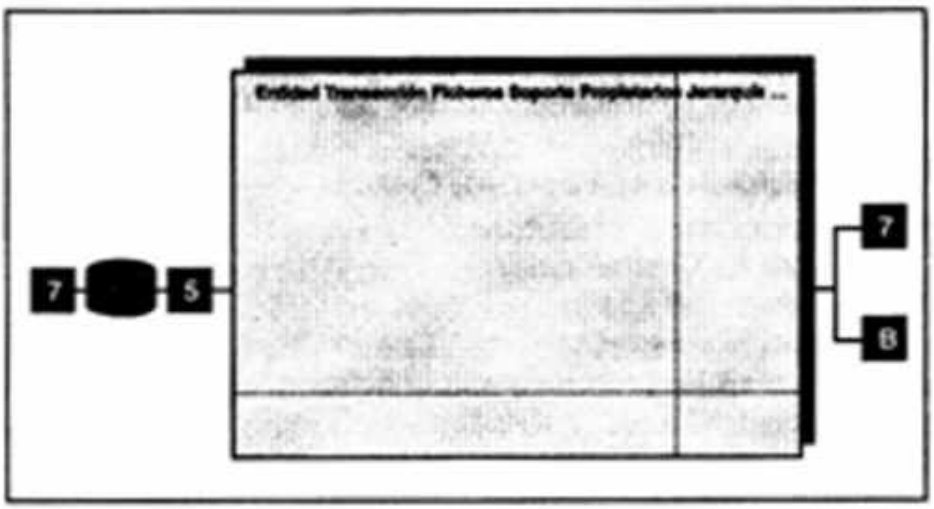


Figura 3.13. Ejemplo de matriz de clasificación

Obtención de los procedimientos de control

Otra metodología necesaria para la obtención de los controles expresados en la figura 3.1, es "la Obtención de los Procedimientos de Control". Es frecuente encontrar manuales de procedimientos en todas las áreas de la empresa que explican las funciones y cómo se realizan las distintas tareas diariamente, siendo éstos necesarios para que los auditores realicen sus revisiones operativas, evaluando si los procedimientos son correctos y están aprobados y sobre todo si se cumplen.

Pero podríamos preguntarnos si desde el punto de vista de control informático es suficiente y cómo se podrían mejorar.

La respuesta nos la da la metodología que se expone a continuación, que nos dará otro plan de acciones que tal como trata de expresar la figura 3.12, contribuirá sumándose a los distintos proyectos de un plan de seguridad para mejorar el entramado de contramedidas.

Metodología

Fase I. Definición de Objetivos de Control.

Se compone de tres tareas.

Tarea 1. Análisis de la empresa. Se estudian los procesos, organigramas y funciones.

Tarea 2. Recopilación de estándares. Se estudian todas las fuentes de información necesarias para conseguir definir en la siguiente fase los objetivos de control a cumplir (por ejemplo, ISO, ITSEC, CISA, etc.).

Tarea.3. Definición de los Objetivos de Control.

Fase II. Definición de los Controles.

Tarea 1. Definición de los Controles. Con los objetivos de control definidos, analizamos los procesos y vamos definiendo los distintos controles que se necesiten.

Tarea 2. Definición de Necesidades Tecnológicas (hardware y herramientas de control).

Tarea 3. Definición de los Procedimientos de Control. Se desarrollan los distintos procedimientos que se generan en las áreas usuarias, informática, control informático y control no informático.

Tarea 4. Definición de las necesidades de recursos humanos.

Fase III. Implantación de los controles.

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, no resta más que implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los afectados de cambio. Los procedimientos resultantes serán:

- Procedimientos propios de control de la actividad informática (control interno informático).
- Procedimientos de distintas áreas usuarias de la informática, mejorados.
- Procedimientos de áreas informáticas, mejorados.
- Procedimientos de control dual entre control interno informática y el área informática, los usuarios informáticos, y el área de control no informático.

3.5.3. Las herramientas de control

Ya hemos hablado de todas las capas de la figura 3.1, excepto del último substrato de la pirámide, esto es, las herramientas de control. En la tecnología de la seguridad informática que se ve envuelta en los controles, existe tecnología hardware (como los cifradores) y software. Las herramientas de control son elementos software que por sus características funcionales permiten vertebrar un control de una manera más actual y más automatizada. Pero no olvidemos que la herramienta en sí misma no es nada. Ya hemos visto en el punto anterior que el control se define en todo un proceso metodológico, y en un punto del mismo se analiza si existe una herramienta que automatice o mejore el control para más tarde definir todo el control con la herramienta incluida, y al final documentar los procedimientos de las distintas áreas involucradas para que éstas; los cumplan y sean auditados. O sea, comprar una herramienta sin más y ver qué podemos hacer con ella es, un error profesional grave, que no conduce a nada, comparable a trabajar sin método e improvisando en cualquier disciplina informática.

Las herramientas de control (software) más comunes son:

- Seguridad lógica del sistema.
- Seguridad lógica complementaria al sistema (desarrollado a medida).
- Seguridad lógica para entornos distribuidos.
- Control de acceso físico. Control de presencia.
- Control de copias.
- Gestión de soportes magnéticos.
- Gestión y control de impresión y envío de listados por red.
- Control de proyectos.
- Control de versiones.
- Control y gestión de incidencias.
- Control de cambios.
- Etc.

Todas estas herramientas están inmersas en controles nacidos de unos objetivos de control y que regularán la actuación de las distintas áreas involucradas. Por ejemplo, si el objetivo de control es "separación de entornos entre desarrollo y producción", habrá un procedimiento en desarrollo de "paso de aplicaciones a explotación" y otro en explotación de "paso a explotación de aplicaciones de desarrollo". Soportado todo por una herramienta de control de acceso lógico que en un proceso de clasificación ha definido distintos perfiles en desarrollo y explotación, y tras implantarlo en la herramienta, impide acceder a uno y a otros al entorno que no es el suyo. Por tanto, para pasar una aplicación de uno a otro cuando está terminada, se necesita un procedimiento en el que intervengan las dos áreas y un control informático que actúa de llave. Esto que parece dificultoso, no lo es en la práctica.

Sólo a modo de ejemplo pongamos los objetivos de control en el acceso lógico al igual que deberíamos ir haciendo en cada una de las herramientas de control antes enumeradas.

Objetivos de control de acceso lógico

- Segregación de funciones entre los usuarios del sistema: productores de software, jefes de proyecto (si existe un proceso metodológico así), técnicos de sistemas, operadores de explotación, operadores de telecomunicaciones, grupos de usuarios de aplicaciones (con perfiles definidos por la Clasificación de la información), administrador de la seguridad lógica (en control dual al ser de alto riesgo), auditoría, y tantos como se designen.

- Integridad de los "log" e imposibilidad de desactivarlos por ningún perfil para poder revisarlos. Fácilmente legibles e interpretables por control informático.

- Gestión centralizada de la seguridad o al menos única (por control informático).

- Contraseña única (a ser posible) para los distintos Sistemas de la red. Y la autentificación de entrada una sola vez. Y una vez dentro, controlar los derechos de uso.

- La contraseña y archivos con perfiles y derechos inaccesibles a todos, incluso a los administradores de seguridad.

- El sistema debe rechazar a los usuarios que no usan la clave o los derechos de uso correctamente, inhabilitando y avisando a control, que tomara las medidas oportunas.

- Separación de entornos. Significa que los distintos usuarios pueden hacer solamente lo qué y cómo se ha autorizado que hagan para su función. Habrá tantos entornos como se precisen y el control tendrá que estar en situación normal como en emergencia y no entorpecer la operatoria.

- El log, o los log's, de actividad no podrán desactivarse a voluntad, y si se duda de su integridad o carencia, resolver con un terminal externo controlado.

- El sistema debe obligar al usuario a cambiar la contraseña, de forma que sólo la conozca él, que es la única garantía de autenticidad de sus actos.

- Es frecuente encontrar mecanismos de *auto-logout*, que expulsan del sistema a la terminal que permanece inactiva más de un tiempo determinado, que son ayudas adicionales a la seguridad.

Muchos de estos objetivos se pueden sacar de los propios estándares (ISO, Libro Naranja, ITSEC, etc.).

Este ejemplo nos puede servir para introducir otra metodología del compendio PRIMA, utilizada para la implantación del control sobre los "Entornos distribuidos", verdadero reto de nuestros días.

Todo estaba controlado en los grandes sistemas en su nivel C2/E2 (no es mucho, pero suficiente para el nivel comercial, según los fabricantes). Y llega la proliferación de los entornos distribuidos... "el caos". ¿Está controlada la seguridad lógica en la actualidad? ¡Cada responsable de seguridad debe planteárselo! ¿Se cumple el marco jurídico sin seguridad lógica?

Se podría implantar el control de acceso lógico, sistema a sistema con los propios software de seguridad de cada uno de ellos, con un enorme esfuerzo de recursos humanos y complicada operativo. Podemos resolver mejor el problema adquiriendo e instalando un software de control de entornos distribuidos. ¿Pero qué hacer... cómo abordar el problema? ¿Ver muchos productos y escoger uno? ¿Será lo mejor para el futuro? ¿Cómo lo están haciendo los demás?

La forma más apropiada de resolver este problema, hasta donde se pueda, es utilizar un método práctico que paso a desarrollar.

ANÁLISIS DE PLATAFORMAS. Se trata de inventariar las múltiples plataformas actuales y futuras (MVS, UNIX, AIX3.2.5., TANDEN GUARDIAN D30, etc. que más tarde nos servirán para saber qué productos del mercado nos pueden ser válidos, tanto los productos actuales como los futuros planes que tengan los fabricantes.

CATÁLOGO DE REQUERIMIENTOS PREVIOS DE IMPLANTACIÓN. Desde el primer momento nace esta herramienta (control del proyecto), que inventaría lo que no se va a conseguir (limitaciones), así como lo necesario para la implantación, inventariado como acciones y proyectos, calendarizados, y su duración para su seguimiento y desarrollo.

ANÁLISIS DE APLICACIONES. Se trata de inventariar las necesidades de desarrollar INTERFACES con los distintos software de seguridad de las aplicaciones y bases de datos. Estos desarrollos deberían entrar en el catálogo de R.P.I. como proyectos a desarrollar. Por ejemplo: DB2, Oracle 7.1.6. SAP R/3.2.2, Checkpoint

Firewall-1, OFFICE 2.6, o la propia de Recursos Humanos, etc. Es importante la conexión a *Recursos Humanos* para que se detecten automáticamente las alteraciones en los empleados (altas, bajas, cambios). También en este punto conviene ver si el producto/interfaces soporta el tiempo real, o el proceso batch, o sus posibilidades de registros de actividad.

INVENTARIO DE FUNCIONALIDADES Y PROPIETARIOS. En este punto trataremos todo el esquema de funcionalidades de la seguridad lógica actual. Es el momento de crear unas jerarquías de estándares a cumplir (clasificación de la información) y tratar de definir en ese momento los controles que se deberían tener, ya sea de usuarios de las aplicaciones como de los usuarios de los sistemas y el uso de las herramientas.

Este punto es importante para ver si con el nuevo esquema de control al que vamos perdemos objetivos de control o nos salen acciones nuevas para el catálogo de R.P.I.'S.

Es importante inventariar también en este punto la situación de la administración de la seguridad lógica en los distintos entornos y las características de las contraseñas, así como la operativa tanto de los usuarios de los distintos sistemas como de las distintas administraciones de seguridad y el control de *log o reporting*.

Todo este inventario nos servirá para hacer un análisis de mejoras y pérdidas o limitaciones en los nuevos escenarios con los software de control de los entornos distribuidos, según convenga para elegir el mejor en costo/beneficio.

ADMINISTRACIÓN DE LA SEGURIDAD. Se analizarán, de las distintas opciones del mercado, las características de cada producto.

Figura 3.14. Herramientas de control de los entornos distribuidos

No olvidemos que se trata de conseguir que el escenario de los entornos distribuidos se pueda controlar como si de un computador con un solo control de acceso (véase la figura 3.14) se tratara. E incluso mejorando el nivel de control si se puede. Esto hará necesario un conjunto de software a instalar en cada plataforma, sumado a una serie de interfaces en las plataformas que lo necesiten y que a los efectos nos hará observar la seguridad lógica total como un todo.

En este punto nos interesa ver las siguientes funcionalidades u objetivos de control requeridos al nuevo sistema de control de acceso:

- ¿Permite el producto establecer un conjunto de reglas de control aplicables a todos los recursos del sistema?
- ¿Permite el producto al administrador de seguridad establecer un perfil de privilegios de acceso para un usuario o un grupo de usuarios?
- ¿Permite el producto al administrador de seguridad asignar diferentes administradores?
- ¿Permite el producto al administrador de seguridad asignar a estos administradores la posibilidad de gestionar privilegios de acceso para grupos y recursos definidos (por ejemplo, sistemas y aplicaciones)?
- ¿Permite a un administrador pedir acceso para el mismo, tanto como para cualquier usuario de su área de responsabilidad?
- ¿Impide el producto que un administrador se provea él mismo de sus propias peticiones?

Hay que recapitular todos los objetivos de control que se están demandando al conjunto de entornos, en lo referente a la administración de la seguridad, y saber con precisión cuál de las soluciones a analizar cumple mejor los requerimientos.

Es importante pensar en la conexión automática con la información del estado de los recursos humanos que componen el conjunto de usuarios para formatear incompatibilidades por segregación de funciones marcadas por la clasificación de la información y por tener actualizadas las bajas/altas y períodos de ausencia del parque de usuarios.

Son muchos otros los aspectos que deben exigirse, como son que se pueda soportar más de un perfil en un usuario, o que se puedan definir perfiles de todo un departamento o puesto de trabajo, asignaciones temporales de los *backup* de cada empleado para períodos de ausencia del titular, que el perfil de un ingeniero no pueda acceder a una aplicación crítica, que se sincronicen *password* en todos los entornos, etc. En resumen, tantos cuantos objetivos de control se le exijan.

SINGLE SIGN ON. Este concepto podemos definirlo como: "Que es necesario solamente un *password* y un *User ID*, para un usuario, para acceder y usar su

información y sus recursos, de todos los sistemas como si de un solo entorno se tratara". Evidentemente a este concepto habría que añadir todos los conceptos ya vistos en un control de acceso lógico *(time-out,* salvapantallas, log, etc.).

Además podríamos enumerar algunos de los requerimientos que se le piden a la plataforma dentro de este apartado:

- Sobre qué soporta el producto el single sig-on, ¿Windows 3.1, Windows NT, Windows 2000, Unix workstation, terminal 3270, un usuario remoto entrando a través de un servidor de acceso remoto?
- ¿El producto faculta al usuario de un recurso a acceder vía *single sig-on* mientras otros usuarios acceden al mismo recurso directamente?
- ¿El producto encripta las transacciones del *single sig-on* entre la *workstation* y el servidor de seguridad?

FACILIDAD DE USO Y REPORTING. En este punto se valora la "interfaz de usuario" y la calidad de la misma (si tiene interfaz gráfica, si tiene help menús, tanto para el usuario como para el administrador, si tiene mensajes de error, si enseña el perfil de un determinado usuario al administrador, mensajes en las modificaciones como *"are you sure?"*, mensajes a través de las aplicaciones, etc.).

Asimismo se evalúa el nivel de *reporting* para los administradores y auditores. Así como:

- ¿El producto ofrece un report de todas las plataformas y aplicaciones a las que los usuarios tienen acceso, así como un report de todos los usuarios que tienen acceso a una plataforma o aplicación?
- ¿Un report de todas las demandas que un administrador ha hecho, o en una fecha dada, o durante un período de tiempo, o a un centro de costo, o de todas las inactividades, o de todos los usuarios activos y privilegios de acceso de un centro de costo, o de demandas pendientes en orden de antigüedad de la demanda, o un report de actividad, de las aplicaciones y sistemas (por ejemplo, el número de demandas aceptadas, pendientes y rechazadas por cada sistema)?
- ¿Un log de violaciones?

En cualquier caso todo registro debe tener garantizada su integridad incluso para los administradores, no pudiendo desactivarse a voluntad, dado que quien quiera hacer algo "no permitido", lo primero que hará es asegurarse de que no quede constancia del hecho.

SEGURIDADES. En este punto se trata de ver aspectos de seguridad clásicos del propio producto, como que el administrador no vea las *password* de los usuarios, una longitud de *password* mínima, que el producto requiera un ID y *password* de

longitud mínima para el acceso al propio producto, el administrador pueda paralizar a un usuario determinado, dual control en las funciones de riesgo (esto es, con un user ID es necesario una *first password* y una *second password* como acceso dual de dos administradores físicos), cifrado de *password*, privacidad en la propagación de *password* en todo momento, acceso a los auditores para poder ver la ID database, un registro de rechazos e intentos infructuosos, la posibilidad de *recovery y backup* (incremental) de todo el sistema de seguridad, la posibilidad del *mirroring* de la database de seguridad para los planes de contingencias de conmutación en tiempo cero al centro alternativo, etc.

También facilidades especiales tales como que se pueda restringir el acceso a un recurso local a un usuario.

Hemos de hacer notar que las limitaciones que vayamos encontrando para todos los productos, tendremos que resolverlas con exclusiones o procedimientos que constarán en el catálogo de R.P.I.'s, verdadero artífice de la metodología que nos obligará a resolver las acciones antes de implantar el producto, y que será un control del proyecto durante su desarrollo.

ADQUISICIÓN, INSTALACIÓN E IMPLANTACIÓN. FORMACIÓN. MANUALES DE PROCEDIMIENTOS DE CONTROL. Tras los pasos anteriores, no queda más que comprar el producto e instalarlo, así como implantar el nuevo esquema de seguridad lógica. Y tras esto, dar la formación apropiada a los implicados y desarrollar los procedimientos de control, que generarán procedimientos operativos para los usuarios de aplicaciones, los usuarios informativos, y los administradores de seguridad lógica.

Todo este complejo proceso es vital hacerlo de modo ordenado y usando un método que permita en todo momento saber qué se "quiere" y qué se "puede" conseguir con los productos existentes de control de entornos, tratando de suplir con procedimientos de control los huecos que no podamos cubrir con tecnología. Aun así, el reto que tenemos por delante es importante, porque las soluciones que ofrecen los fabricantes van muy detrás frente a la proliferación de entornos y aplicaciones nuevos, y sólo una actitud responsable de estandarización en sus soluciones propietarias de seguridad, hará que los fabricantes de soluciones para entornos distribuidos tengan productos de seguridad cada vez mejores, y que en vez de "adaptar el nivel de seguridad lógica a los productos, sean los productos los que resuelvan las situaciones nuevas de seguridad lógica".

3.6. CONCLUSIONES

Son muchas pues las metodologías que se pueden encontrar en el mundo de la auditoría informática y control interno. Muchas hemos visto en este capítulo. Pero como resumen se podría decir que la metodología es el fruto del nivel profesional de cada uno y de su visión de cómo conseguir un mejor resultado en el nivel de control de cada entidad, aunque el nivel de control resultante debe ser similar.

Pero en realidad todas ellas son herramientas de trabajo mejores o peores que ayudan a conseguir mejores resultados. Sólo resta animar a los profesionales que lean este libro a trabajar con las únicas herramientas verdaderas de la auditoría y el control "LA ACTITUD y LA APTITUD", con una actitud vigilante y una formación continuada.

3.7. EJEMPLO DE METODOLOGÍA DE AUDITORÍA DE UNA APLICACIÓN

Metodología de trabajo

Revisión de controles sobre aplicaciones

Objetivo

Determinar que los sistemas producen informaciones exactas y completas en el momento oportuno. Esta área es tal vez la más importante en el trabajo de auditorías informativas.

Programa de la revisión

1. Identificar el área a revisar (por ejemplo, a partir del calendario de revisiones), notificar al responsable del área y prepararse utilizando papeles de trabajo de auditorías anteriores.

2. Identificar las informaciones necesarias para la auditoría y para las pruebas.

3. Obtener informaciones generales sobre el sistema. En esta etapa, se definen los objetivos y el alcance de la auditoría, y se identifican los usuarios específicos que estarían afectados por la auditoría (plan de entrevistas).

4. Obtener un conocimiento detallado de la aplicación/sistema. Se pasan las entrevistas con los usuarios y el personal implicado en el sistema a revisar; se examina la documentación de usuarios, de desarrollo y de operación, y se identifican los aspectos más importantes del sistema (entrada, tratamiento, salida de datos, etc.), la periodicidad de procesos, los programas fuentes, características y estructuras de archivos de datos, así como pistas de auditoría.

5. Identificar los puntos de control críticos en el sistema. Utilizando organigramas de flujos de informaciones, identificar los puntos de control críticos en entrevistas con los usuarios con el apoyo de la documentación sobre el sistema. El auditor tiene que identificar los peligros y los riesgos que podrían surgir en cada punto. Los puntos de control críticos son aquellos donde el riesgo es más grave, es decir, donde la necesidad de un control es más importante. A menudo, son necesarios controles en los puntos de interfaz entre procedimientos manuales y automáticos.

6. Diseño y elaboración de los procedimientos de la auditoría.

7. Ejecución de pruebas en los puntos críticos de control. Se podría incluir la determinación de las necesidades de herramientas informativas de ayuda a la auditoría no informática. Se revisa el cumplimiento de los procedimientos para verificar el cumplimiento de los estándares y los procedimientos formales, así como los procesos descritos por los organigramas de flujos. Así se verifican los controles internos del cumplimiento de a) planes, políticas, procedimientos, estándares, b) del trabajo de la organización, c) requerimientos legales, d) principios generales de contabilidad y e) prácticas generales de informática.

   Se hacen revisiones substantivas y pruebas, como resultado de la revisión del cumplimiento de procedimientos. Si las conclusiones de la revisión de cumplimentación fuesen generalmente positivas, se podrían limitar las revisiones substantivas. Dentro de este punto del programa de la revisión podríamos analizar si existen los siguientes controles:

Controles de preparación de datos

Revisar procedimientos escritos para iniciar, autorizar, recoger, preparar y aprobar los datos de entrada en la forma de un manual de usuario. Verificar que los usuarios entienden y siguen estos procedimientos.

Revisar que se dé la formación del "uso del terminal" necesaria a los usuarios.

Revisar los documentos fuente u otros documentos para determinar si son numerados. También revisar códigos de identificación de transacciones y otros

campos de uso frecuentes para determinar si son codificados previamente para minimizar errores en los procesos de preparación, entrada y conversión de datos.

Cuando sea necesario, verificar que todos los datos de entrada en un sistema pasan por validación y registro antes de su tratamiento.

Determinar si los usuarios preparan totales de control de los datos de entrada por terminales. Comprobar la existencia de una reconciliación de los totales de entrada con totales de salida.

Comprobar la existencia y seguimiento de calendarios de entrada de datos y de distribución de informes (listados).

Determinar si el archivo y retención de documentos fuente y otros formularios de entrada es lógica y accesible, y cumple las normas y requerimientos legales.

Revisar los procedimientos de corrección de errores.

Comprobar la existencia de períodos de retención para documentos fuente y soportes magnéticos.

Controles de entrada de datos

Establecer los procedimientos de entrada y control de datos que explican las revisiones necesarias de entradas y salidas, con fecha límite, criterios de validación de datos de entrada; códigos, mensajes y detección de errores; la corrección de errores y la reentrada de datos.

Para sistemas interactivos, verificar el uso de métodos preventivos para evitar la entrada incorrecta de datos funciones de ayuda a la pantalla, formatos fijos, el uso de menús y mensajes para el operador.

Para sistemas interactivos, determinar la grabación de datos de entrada con fecha y hora actual, así como con una identificación del usuario/terminal y ubicación.

Revisar log's de acceso por líneas de telecomunicaciones para determinar posibles accesos y entradas no autorizados.

Revisar los programas para determinar si contienen procesos internos de validación de datos (por ejemplo, chequeos de dígitos, test razonables, totales de batch, número de cuentas, etc.). Evaluar su exactitud.

Comparar, validar, apuntar y recalcular campos o elementos de datos críticos por métodos manuales o automáticos.

Para sistemas interactivos determinar que los datos se verifican en el momento de su entrada en el sistema.

Comprobar que los usuarios revisan regularmente las tablas internas del sistema para validar sus contenidos.

Revisar funciones matemáticas que redondean cálculos para ver si tienen implicaciones negativas.

Determinar que existen pistas de auditoría adecuadas en el diccionario de datos. Identificar la interrelación entre los programas y los datos para dejar la posibilidad de seguir la pista de datos dentro de programas y sistemas en los errores.

Revisar los procedimientos de corrección de errores.

Identificar con los usuarios cualquier código de errores críticos que deberían aparecer en momentos específicos pero que nunca surgen. ¿Se han desactivado los códigos o mensajes de error?

Controles de tratamiento y actualización de datos

Ver si hay establecidos controles internos automatizados de proceso, tales como rutinas de validación, en el momento de la actualización de los archivos de transacción, referencia y maestros.

Identificación de transacciones por el uso de números de batch, códigos de transacción y otros indicadores.

Revisión del log de transacciones para identificar problemas encontrados por el operador y las medidas seguidas.

Restricción de la posibilidad de pasar por encima de procesos de validación.

Aceptación por los usuarios finales de todas las transacciones y cálculos de la aplicación.

Revisar los totales de control de entrada de datos.

Verificar que existen totales de control para confirmar la buena interfaz entre jobs o programas.

Comprobar que existen validaciones entre totales de control, manuales y automáticos, en puntos de la interfaz entre procesos manuales y automatizados.

Verificar que los log's de actividad de sistemas son revisados por los responsables, para investigar accesos y manipulaciones no autorizados.

Ver los controles sobre la entrada de datos.

Controles de salida de datos

Determinar si los usuarios comparan totales de control de los datos de entrada con totales de control de datos de salida.

Determinar si el control de datos revisa los informes de salida (listados) para detectar errores evidentes tales como campos de datos que faltan, valores no razonables o formatos incorrectos.

Verificar que se hace una identificación adecuada sobre los informes, por ejemplo, nombre y número de informe, fecha de salida, nombre de área/departamento, etc.

Comparar la lista de distribución de informes con los usuarios que los reciben en realidad. ¿Hay personas que reciben el informe y que no deberían recibirlo?

Verificar que los informes que pasan de aplicabilidad se destruyen, y que no pasan simplemente a la basura, sin seguridad de destrucción.

Revisar la justificación de informes, que existe una petición escrita para cada uno y que se utilizan realmente, así como que está autorizada la petición.

Verificar la existencia de períodos de retención de informes y su suficiencia.

Revisar los procedimientos de corrección de los datos de salida.

Controles de documentación

Verificar que dentro de las actividades de desarrollo y mantenimiento de aplicaciones se produce la documentación de sistemas, programas, operaciones y funciones, y procedimientos de usuario.

Existencia de una persona específica encargada de la documentación y que mantiene un archivo de documentos ya distribuidos y a quiénes.

Comprobar que los jefes de área se informen de faltas de documentación adecuada para sus empleados.

Destrucción de toda la documentación de antiguos sistemas.

Que no se acepten nuevas aplicaciones por los usuarios sin una documentación completa.

Actualización de la documentación al mismo tiempo que los cambios y modificaciones en los sistemas.

La existencia de documentación de sistemas, de programas, de operación y de usuario para cada aplicación ya implantada.

Controles de backup y rearranque

Existencia de procedimientos de *backup* y rearranque documentados y comprobados para cada aplicación en uso actualmente. (No confundir con el plan de contingencias.)

Procedimientos escritos para la transferencia de materiales y documentos de *backup* entre el C.P.D. principal y el sitio de *backup* (centro alternativo). Mantenimiento de un inventario de estos materiales.

Existencia de un plan de contingencia.

Identificación de aplicaciones y archivos de datos críticos para el plan de contingencia.

Revisar los contratos del plan de contingencia y *backup* para determinar su adecuación y actualización.

Pruebas de aplicaciones críticas en el entorno de *backup*, con los materiales del plan de contingencia (soportes magnéticos, documentación, personal, etc.).

Determinación de qué se revisa, si cada aplicación de un sistema es crítica y si debería incluirse en el plan de contingencia.

Grabación de todas las transacciones ejecutadas por teleproceso, cada día; para facilitar la reconstrucción de archivos actualizados durante el día en caso del fallo del sistema.

Existencia de procesos manuales para sistemas críticos en el caso del fallo de contingencia.

Actualización del plan de contingencia cuando es necesario; pruebas anuales.

Controles sobre programas de auditoría

Distribución de políticas y procedimientos escritos a auditores y responsables de áreas sobre la adquisición, desarrollo y uso de software de auditoría.

Uso de software de auditoría únicamente por personas autorizadas.

Participación del auditor en la adquisición, modificación/adaptación, instalación de paquetes de software de auditoría.

Participación del auditor en la planificación, diseño, desarrollo e implantación de software de auditoría desarrollado internamente.

Formación apropiada para los auditores que manejan software de auditoría.

Participación del auditor en todas las modificaciones y adaptaciones del software de auditoría, ya sea externo o de desarrollo propio. Actualización de la documentación de software.

Verificación de que los programas de utilidad se utilizan correctamente (cuando no se puede utilizar el software de auditoría).

Revisión de tablas de contraseñas para asegurar que no se guardan identificaciones y contraseñas de personas que han causado baja.

Controles de la satisfacción de los usuarios

Disponibilidad de políticas y procedimientos sobre el acceso y uso de la información.

Resultados fiables, completos, puntuales y exactos de las aplicaciones (integridad de datos).

Utilidad de la información de salida de la aplicación en la toma de decisión por los usuarios.

Comprensión por los usuarios de los informes e informaciones de salida de las aplicaciones.

Satisfacción de los usuarios con la información que produce la aplicación.

Revisión de los controles de recepción, archivo, protección y acceso de datos guardados sobre todo tipo de soporte.

Participación activa de los usuarios en la elaboración de requerimientos de usuarios, especificaciones de diseño de programas y revisión de resultados de pruebas.

Controles por el usuario en la transferencia de informaciones por intercambio de documentos.

Resolución fácil de problemas, errores, irregularidades y omisiones por buenos contactos entre usuarios y el personal del C.P.D.

Revisiones regulares de procesos que podrían mejorarse por automatización de aspectos particulares o reforzamientos de procesos manuales

Evaluación de la revisión y/o resultados de pruebas. En esta etapa se identifican y se evalúan los puntos fuertes y débiles de los procedimientos y prácticas de control interno en relación con su adecuación, eficiencia y efectividad. Cuando se identifique una debilidad, se determinará su causa.

Se elaboran las conclusiones basadas sobre la evidencia; lo que deberá ser suficiente, relevante, fiable, disponible, comprobable y útil.

Preparación del informe. Recomendaciones.

Informe previo

Para mantener una relación buena con el área revisada, se emite un informe previo de los puntos principales de la revisión. Esto da a los responsables del área revisada la posibilidad de contribuir a la elaboración del informe final y permitirá una mejor aceptación por parte de ellos.

Informe final de la revisión

Se emite el informe final después de una reunión con los responsables del área implicados en la revisión. El contenido del informe debería describir los puntos de control interno de la manera siguiente:

- Opinión global (conclusión).
- Problema(s) específico(s).
- Explicación de la violación de los controles internos, planes organizacionales, estándares y normas.
- Descripción de los riesgos, exposición o pérdidas que resultarían de las violaciones.

Cuando sea posible, se identificará el impacto de cada problema en términos económicos. Se da una solución específica y práctica para cada debilidad. Se identificarán las personas que se responsabilizarán de cada aspecto de las soluciones. Las recomendaciones son razonables, verificables, interesantes económicamente y tienen en cuenta el tamaño de la organización.

El informe debe tener un tono constructivo. Si es apropiado se anotan los puntos fuertes.

Para su distribución, se preparará un resumen del informe.

Después de la revisión del informe final con los responsables del área revisada se distribuirá a las otras personas autorizadas.

El área auditada tiene la posibilidad de aceptar o rechazar cada punto de control. Todos los puntos rechazados se explicarán por escrito. El área acepta los riesgos implícitos de la debilidad encontrada por el auditor.

Se hace un seguimiento de la implantación de las recomendaciones para asegurarse de que el trabajo de revisión produce resultados concretos.

3.8. LECTURAS RECOMENDADAS

James A. Schweitzer. *Managing Infortnation Security* (Administrative, Electronic, and Legal Measures to Project Business Information). Buttervorths. ISBN 0-409-90195-4.

J. M. Lamete. *La Seguridad Informática* (Metodología). Ediciones Arcadia. ISBN 84-86299-13-6.

J. M. Lamere. *La securité des petits et moyens systèmes informatiques. Dunod* informatique. ISBN 2-04-018721-9.

J. M. Lamere, Y. Leroux, J. Orly. *La securité des reseaux* (Methodes et techniques). Dunod informatique. ISBN 2-04-018886-X.

3.9. CUESTIONES DE REPASO

1. ¿Qué diferencias y similitudes existen entre las metodologías cualitativas y las cuantitativas? ¿Qué ventajas y qué inconvenientes tienen?

2. ¿Cuáles son los componentes de una contramedida o control (pirámide de la seguridad)? ¿Qué papel desempeñan las herramientas de control? ¿Cuáles son las herramientas de control más frecuentes?

3. ¿Qué tipos de metodologías de Plan de Contingencias existen? ¿En qué se diferencian? ¿Qué es un Plan de Contingencias?

4. ¿Qué metodologías de auditoría informática existen? ¿Para qué se usa cada una?

5. ¿Qué es el nivel de exposición y para qué sirve?

6. ¿Qué diferencias existen entre las figuras de auditoría informática y control interno informático? ¿Cuáles son las funciones más importantes de éste?

7. ¿Cuáles son las dos metodologías más importantes para control interno informático? ¿Para qué sirve cada una?

8. ¿Qué papel tienen las herramientas de control en los controles?

9. ¿Cuáles son los objetivos de control en el acceso lógico?

10. ¿Qué es el *Single Sign On?* ¿Por qué es necesario un softwae especial para el control de acceso en los entornos distribuidos?

CAPÍTULO 4

EL INFORME DE AUDITORÍA

José de la Peña Sánchez

4.1. INTRODUCCIÓN

El tema de este capítulo es el **Informe de Auditoría Informática,** que a su vez es el objetivo de la Auditoría Informática.

Para comprender ésta, en función del Informe que realiza un, digamos, experto o perito –al que llamaremos Auditor Informático–, conviene explicar someramente el contexto en el que se desenvuelve hoy su práctica.

La sociedad actual, está en fase tecnológica; apenas guarda recuerdo práctico de anteriores etapas evolutivas (la artesanal, por ejemplo); más aún, las va olvidando a creciente velocidad, generación tras generación.

El dominio de la tecnología como motor de cambio social acelerado y como catalizador de cambios tecnológicos que se superponen, se hace rabiosamente evidente en las llamadas Tecnologías de Información y Comunicaciones de uso en las organizaciones. (Tras el mainframe y los terminales tontos, surgieron los PC's y las redes, el EDI, los entornos distribuidos, las arquitecturas cliente/servidor, las redes TCP/IP –intranets, extranets, redes privadas virtuales...–, los accesos remotos y móviles mediante portátiles y teléfonos móviles, y, finalmente –por ahora–, se nos proponen terminales domésticos vinculados con el equipo de televisión y terminales cuasitontos de trabajo conectados a servidores dominantes descentralizados... Y todo en un período no superior a ¡treinta y cinco años!)

Está claro: las tecnologías de la información, al tiempo que dominan de modo imparable las relaciones humanas (personales, familiares, mercantiles, internacionales...), tienen un ciclo de vida cada vez más corto.

Sea como fuere, una de las consecuencias de lo dicho consiste en la dificultad de asimilación rápida y equilibrada en la empresa de los entornos tecnológico y de organización (referido el primero a las Tecnologías de Información y Comunicaciones, y el segundo a lo mercantil).

En este sentido, el Auditor Informático, en tanto que experto, lo tiene crudo (menos, sin embargo, que el Auditor de Cuentas), al tener que encarar profesionalmente y en el paisaje que estoy presentando, plagado de necesidades de reciclaje y formación, el llamado **"desfase entre las expectativas de los usuarios y los informes de auditoría".** Las cosas ya no son como eran, y algo habrá que hacer para encontrar un punto de equilibrio razonable entre el desfase mencionado y la contabilidad de los usuarios en el Informe (y en el Auditor Informático).

La complejidad de los sistemas de información crece con sus prestaciones y características (conectividad, portabilidad...); la necesidad de utilizarlos que tienen las organizaciones –públicas y privadas– en todos sus ámbitos, alcanza hoy un valor estratégico de competitividad y supervivencia... Podemos afirmar que nunca antes hemos sido tan dependientes de los sistemas de información. Y nunca antes hemos necesitado tanto a expertos eficientes (no infalibles) en Auditoría Informática.

Conviene mencionar, al respecto de la práctica de la Auditoría (Informática), y siempre en función del Informe de Auditoría, la existencia del fraude y del error, sobre todo si son significativos, así como la valoración de las garantías que aportan los informes de los auditores informáticos a los usuarios, incluyendo gobiernos y organizaciones nacionales e internacionales.

La Informática es muy joven; por tanto, la Auditoría Informática lo es más (en España, por cierto, de modo superlativo). No está todo sin hacer; pero sí quedan muchos cabos por atar, y en esto el tiempo no es neutral.

En este capítulo (y en este contexto) vamos a tratar de fijar la práctica de la Auditoría Informática en función, como queda dicho, del Informe. Para ello, repasaremos someramente aspectos previos fundamentales, como son las **normas,** el concepto de **evidencia** en auditoría, las **irregularidades,** los **papeles de trabajo** o documentación para, finalmente, encarar el **Informe,** sus componentes, características y tendencias detectadas. Intentaremos, también, ofrecer algunas conclusiones de interés, sin perder de vista en todo caso que en el mundo auditor de hoy todo ejercicio de predicción es, en principio, una temeridad.

4.2. LAS NORMAS

En 1996 la Unión Europea publicó el **Libro Verde de la Auditoría,** dedicado al papel, la posición y la responsabilidad del auditor legal. Su contenido afecta a la Auditoría Informática.

En principio, el Libro acepta las Normas Internacionales IFAC para su adaptación *adecuada* a la Unión Europea; por tanto, se transmitirán a través de las Directivas correspondientes a España para que se transformen en legislación positiva.

En lo referente al Tratamiento Automatizado de Datos de Carácter Personal -incluso disponiendo de una Ley orgánica-, el asunto se resolverá por los mismos cauces, con la trasposición de la actual Directiva de protección de datos personales y, quizá, de otra, en forma de propuesta todavía, relacionada con los servicios de telecomunicaciones apoyados en tecnología digital y especialmente Red Digital de Servicios Integrados.

Otra fuente de Normas Internacionales es ISACF, ya más específica de Auditoría Informática. Nuestro país está representado en ISACA por la Organización de Auditoría Informática, en lento *take off*.

Hoy por hoy, la normativa española oficial que afecta, en mayor o menor medida, a la Auditoría Informática, es la siguiente:

- ICAC: Normas Técnicas de Auditoría: punto 2.4.10, Estudio y Evaluación del Sistema de Control Interno.

- AGENCIA DE PROTECCIÓN DE DATOS: Instrucción relativa a la prestación de servicios sobre solvencia patrimonial y créditos. Norma cuarta: Forma de Comprobación.

Del artículo 9 de la LORTAD se desprende el desarrollo reglamentario de medidas técnicas y organizativas alusivas a la seguridad en lo que concierne a integridad y confidencialidad de los datos personales automatizados. Todavía no ha sido publicado tal reglamento, pero sería de esperar que se incluyera en su texto algana referencia específica sobre Auditoría Informática.

También conviene reseñar que dentro de la Unión Europea, la FEE tiene en marcha el Proyecto EDIFICAS.EUROPE, dentro del UN/EDIFACT, en el que España está representada por el IACJCE, que se estructura en cuatro grupos de trabajo: Mensajes, **Auditoría** (Guías de Auditoría de entornos de EDI), Promoción y Asuntos Especiales.

La Auditoría Informática no está muy desarrollada y, por añadidura, se encuentra en un punto crucial para la definición del modelo en que deberá implantarse y practicarse en la Unión Europea y, por tanto, España, vía directivas UE/legislación positiva y normas profesionales.

Maticemos este aspecto: hay dos tendencias legislativas y de práctica de disciplinas: la anglosajona, basada en la *Common Law*, con pocas leyes y jurisprudencia relevante; y la latina, basada en el Derecho Romano, de legislación muy detallada.

La tensión entre estos dos modelos, esto es, entre el intervencionismo máximo latino y el mínimo intervencionismo anglosajón, es ya insostenible. Uno de los dos deberá prevalecer, si es que realmente nos encaminamos a la sociedad global.

Justo es reconocer que los parámetros del cambio tecnológico parecen hacer más práctico el modelo anglosajón: no en vano, en Estados Unidos, tanto la Auditoría como la Informática (y las Comunicaciones), tienen un desarrollo muy experimentado y, sobre todo, **adaptativo.** Los parámetros de velocidad y tiempo hacen aconsejable un esfuerzo por conseguir la disponibilidad armonizada de normas legales y normas de origen profesional.

Si la globalización antes mencionada es un hecho incuestionable, el sabio uso de los llamados *principios generalmente aceptados* hará posible la adaptación suficiente a la realidad de cada época.

En este sentido, no podemos olvidar que los organismos de armonización, normalización, homologación, acreditación y certificación tendrán que funcionar a un ritmo más acorde con las necesidades cambiantes. El conjunto ISO-CEN-AENOR y los vinculados con seguridad, ITSEC/ITSEM Europa, TCSEC USA y *Common Criteria* UE/Norteamérica, necesitan ir más rápido, ya que su lentitud está provocando, en un mundo tan acelerado, la aparición de multitud de organizaciones privadas, consorcios y asociaciones que con muy buena voluntad y óptimo sentido de la conveniencia mercantil, pretenden unificar normas y promocionar estándares.

Por último, conviene que se clarifique el panorama normativo, de prácticas y responsabilidades en lo que concierne a los problemas planteados por los **servicios profesionales multidisciplinares,** ya que el Informe de Auditoría Informática se compone de tres términos: **Informática, Auditoría e Informe.**

4.3. LA EVIDENCIA

En este epígrafe parece saludable reseñar algunos asuntos previos, referidos a la redacción del Informe, tratados en otros capítulos de esta obra, puesto que el referido Informe es su consecuencia.

Por tanto, tratemos de recordar en qué consiste la **evidencia** en Auditoría Informática, así como las pruebas que la avalan, sin olvidar la importarcia relativa y el riesgo probable, inherente y de control.

La certeza absoluta no siempre existe, según el punto de vista de los auditores; los usuarios piensan lo contrario. No obstante lo dicho, el desarrollo del control interno, incluso del específicamente informático, está en efervescencia, gracias al empuje de los Informes USA/Treadway (1987), UK/Cadbury (1992) y Francia/Vienot (1995), y en lugar destacado el USA/COSO (1992), traducido al español por Coopers & Lybrand y el Instituto de Auditores Internos de España.

Pero volvamos a la evidencia, porque ella es la base razonable de la opinión del Auditor Informático, esto es, el Informe de Auditoría Informática.

La evidencia tiene una serie de calificativos; a saber:

- La **evidencia relevante,** que tiene una relación lógica con los objetivos de la auditoría.
- La **evidencia fiable,** que es válida y objetiva, aunque con nivel de confianza.
- La **evidencia suficiente,** que es de tipo cuantitativo para soportar la opinión profesional del auditor.
- La **evidencia adecuada,** que es de tipo cualitativo para afectar a las conclusiones del auditor.

En principio, las **pruebas** son de **cumplimiento** o **sustantivas.**

Aunque ya tratado en otro capítulo, conviene recordar el escollo práctico de la **importancia relativa** o materialidad, así como el riesgo probable.

La opinión deberá estar basada en evidencias justificativas, es decir, desprovistas de prejuicios, si es preciso con evidencia adicional.

4.4. LAS IRREGULARIDADES

Las irregularidades, o sea, los fraudes y los errores, especialmente la existencia de los primeros, preocupa tanto que aparece con énfasis en el ya citado Libro Verde de la UE. La Dirección General XV (Comercio Interior) y el MARC (Maastricht) están claramente sensibilizados al respecto.

Recordemos antes de proseguir, que en los organismos y las empresas, la Dirección tiene la responsabilidad principal y primaria de la detección de irregularidades, fraudes y errores; la responsabilidad del auditor se centra en planificar, llevar a cabo y evaluar su trabajo para obtener una expectativa razonable de su detección.

Es, pues, indudablemente necesario diseñar pruebas antifraude, que lógicamente incrementarán el coste de la auditoría, previo análisis de riesgos (amenazas, importancia relativa...).

La auditoría de cuentas se está judicializando –camino que seguirá la Auditoría Informática, práctica importada de Estados Unidos–, ya que aparece en el vigente Código Penal (delitos societarios y otros puntos) con especial énfasis en los administradores. No olvidemos, al respecto, la obligatoriedad de suscribir pólizas de seguro de responsabilidad civil para auditores independientes, individuales y sociedades.

Por prudencia y rectitud, convendrá aclarar al máximo –de ser posible– si el Informe de Auditoría es propiamente de auditoría y no de consultoría o asesoría informática, o de otra materia afín o próxima.

Aunque siempre debe prevalecer el deber de secreto profesional del auditor, conviene recordar que en el caso de detectar fraude durante el proceso de auditoría procede actuar en consecuencia, con la debida prudencia que aconseja episodio tan delicado y conflictivo, sobre todo si afecta a los administradores de la organización objeto de auditoría. Ante un caso así, conviene consultar a la Comisión Deontológica Profesional, al asesor jurídico, y leer detenidamente las normas profesionales, el Código Penal y otras disposiciones; incluso hacer lo propio con las de organismos oficiales tales como el Banco de España, la Dirección General de Seguros, la Comisión Nacional del Mercado de Valores, el organismo regulador del medio ambiente..., que pudieran estar afectados, no debería desestimarse. El asunto podría, incluso, terminar en los Tribunales de justicia.

4.5. LA DOCUMENTACIÓN

En el argot de auditoría se conoce como papeles de trabajo la "totalidad de los documentos preparados o recibidos por el auditor, de manera que, en conjunto,

constituyen un compendio de la información utilizada y de las pruebas efectuadas en la ejecución de su trabajo, junto con las decisiones que ha debido tomar para llegar a formarse su opinión".

El Informe de Auditoría, si se precisa que sea profesional, tiene que estar basado en la **documentación** o **papeles de trabajo,** como utilidad inmediata, previa supervisión.

La documentación, además de fuente de *know how* del Auditor Informático para trabajos posteriores así como para poder realizar su gestión interna de calidad, es fuente en algunos casos en los que la corporación profesional puede realizar un control de calidad, o hacerlo algún organismo oficial. Los papeles de trabajo pueden llegar a tener valor en los Tribunales de justicia.

Por otra parte, no debemos omitir la característica registral del Informe, tanto en su parte cronológica como en la organizativa, con procedimientos de archivo, búsqueda, custodia y conservación de su documentación, cumpliendo toda la normativa vigente, legal y profesional, como mínimo exigible.

Los trabajos utilizados, en el curso de una labor, de otros auditores externos y/o expertos independientes, así como de los auditores internos, se reseñen o no en el Informe de Auditoría Informática, formarán parte de la documentación.

Además, se incluirán:

- El contrato cliente/auditor informático y/o la carta propuesta del auditor informático.
- Las declaraciones de la Dirección.
- Los contratos, o equivalentes, que afecten al sistema de información, así como el informe de la asesoría jurídica del cliente sobre sus asuntos actuales y previsibles.
- El informe sobre terceros vinculados.
- Conocimiento de la actividad del cliente.

4.6. EL INFORME

Se ha realizado una visión rápida de los aspectos previos para tenerlos muy presentes al redactar el Informe de Auditoría Informática, esto es, la comunicación del Auditor Informático al cliente, formal y, quizá, solemne, tanto del alcance de la auditoría; (objetivos, período de cobertura, naturaleza y extensión del trabajo realizado) como de los resultados y conclusiones.

Es momento adecuado de separar lo significativo de lo no significativo, debidamente evaluados por su importancia y vinculación con el factor riesgo, tarea eminentemente de carácter profesional y ético, según el leal saber y entender del Auditor Informático.

Aunque no existe un formato vinculante, sí existen esquemas recomendados con los requisitos mínimos aconsejables respecto a estructura y contenido.

También es cuestión previa decidir si el informe es largo o, por el contrario, corto, por supuesto con otros informes sobre aspectos, bien más detallados, bien más concretos, como el **informe de debilidades del control interno,** incluso de hechos o aspectos; todo ello teniendo en cuenta tanto la legislación vigente como el contrato con el cliente.

En mi modesta opinión, los términos cliente o proveedor/interno o externo, típicos de la Gestión de la Calidad, resultan más apropiados que informático/auditor informático/usuario, ya que este último término tiene una lamentable connotación peyorativa.

En lo referente a su redacción, el Informe deberá ser claro, adecuado, suficiente y comprensible. Una utilización apropiada del lenguaje informático resulta recomendable.

Los puntos esenciales, genéricos y mínimos del Informe de Auditoría Informática, son los siguientes:

1. Identificación del Informe

El título del Informe deberá identificarse con objeto de distinguirlo de otros informes.

2. Identificación del Cliente

Deberá identificarse a los destinatarios y a las personas que efectúen el encargo.

3. Identificación de la entidad auditada

Identificación de la entidad objeto de la Auditoría Informática.

4. Objetivos de la Auditoría Informática

Declaración de los objetivos de la auditoría para identificar su propósito, señalando los objetivos incumplidos.

5. Normativa aplicada y excepciones

Identificación de las normas legales y profesionales utilizadas, así como las excepciones significativas de uso y el posible impacto en los resultados de la auditoría.

6. Alcance de la Auditoría

Concretar la naturaleza y extensión del trabajo realizado: área organizativa, período de auditoría, sistemas de información... señalando limitaciones al alcance y restricciones del auditado.

7. Conclusiones: Informe corto de opinión

Lógicamente, se ha llegado a los resultados y, sobre todo, a la esencia del dictamen, la opinión y los párrafos de salvedades y énfasis, si procede.

El Informe debe contener uno de los siguientes tipos de opinión: **favorable o sin salvedades, con salvedades, desfavorable o adversa,** y **denegada.**

7.1. **Opinión favorable.** La opinión calificada como favorable, sin salvedades o limpia, deberá manifestarse de forma clara y precisa, y es el resultado de un trabajo realizado sin limitaciones de alcance y sin incertidumbre, de acuerdo con la normativa legal y profesional.

Es indudable que entre el informe de recomendaciones al cliente, que incluye lo referente a debilidades de control interno en sentido amplio, y las salvedades, existe o puede existir una zona de gran sensibilidad; tan es así que tendrá que clarificarse al máximo, pues una salvedad a la opinión deberá ser realmente significativa; concretando: ni pasarse, ni no llegar, dicho en lenguaje coloquial; en puridad es un punto de no retorno.

7.2. **Opinión con salvedades.** Se reitera lo dicho en la opinión favorable al respecto de las salvedades cuando sean significativas en relación con los objetivos de auditoría, describiéndose con precisión la naturaleza y razones.

Podrán ser éstas, según las circunstancias, las siguientes:

- Limitaciones al alcance del trabajo realizado; esto es, restricciones por parte del auditado, etc.
- Incertidumbres cuyo resultado no permita una previsión razonable.
- Irregularidades significativas.
- Incumplimiento de la normativa legal y profesional.

7.3. **Opinión desfavorable.** La opinión desfavorable o adversa es aplicable en el caso de:

- Identificación de irregularidades
- Incumplimiento de la normativa legal y profesional, que afecten significativamente a los objetivos de auditoría informática estipulados, incluso con incertidumbres; todo ello en la evaluación de conjunto y reseñando detalladamente las razones correspondientes.

7.4. **Opinión denegada.** La denegación de opinión puede tener su origen en:

- Las limitaciones al alcance de auditoría.
- Incertidumbres significativas de un modo tal que impidan al auditor formarse una opinión.
- Irregularidades.
- El incumplimiento de normativa legal y profesional.

7.5. **Resumen.** El siempre difícil tema de la opinión, estrella del Informe de Auditoría Informática, joven como informática y más todavía como auditoría informática; por tanto, puede decirse que más que cambiante, mutante. Debido a ello, y además con la normativa legal y profesional desacompasadas, la ética se convierte casi en la única fuente de orientación para reducir el desfase entre las expectativas del usuario en general y el informe de los auditores.

No olvidemos que existe la *ingeniería financiera* y la *contabilidad creativa;* tampoco que las entidades que pueden ser auditadas suelen estar sometidas a cambios, como, por ejemplo, la implantación de aseguramiento y gestión de la calidad –vía ISO 9000, vía EFQM (modelo europeo)–, *reingeniería de* procesos y otras transformaciones significativas (adaptaciones al Milenio y al Euro).

8. Resultados: Informe largo y otros informes

Parece ser que, de acuerdo con la teoría de ciclos, el informe largo va a colocar al informe corto en su debido sitio, o sea, como resumen del informe largo (¿quizá

obsoleto?). Los usuarios, no hay duda, desean saber más y desean transparencia como valor añadido.

Es indudable que el límite lo marcan los papeles de trabajo o documentación de la Auditoría Informática, pero existen aspectos a tener en cuenta:

- El secreto de la empresa.
- El secreto profesional.
- Los aspectos relevantes de la auditoría.
- ...

Las soluciones previsibles se orientan hacia un Informe por cada objetivo de la Auditoría Informática, tal como el de **Debilidades de Control Interno** o los informes especiales y/o complementarios que exigen algunos organismos gubernamentales, como, por ejemplo, el Banco de España, la Comisión Nacional del Mercado de Valores y la Dirección General de Seguros, entre otros y por ahora.

9. Informes previos

No es una práctica recomendable, aunque sí usual en algunos casos, ya que el Informe de Auditoría Informática es, por principio, un **informe de conjunto.**

Sin embargo, en el caso de detección de irregularidades significativas, tanto errores como fraudes, sobre todo, se requiere una actuación inmediata según la normativa legal y profesional, independientemente del nivel jerárquico afectado dentro de la estructura de la entidad. Recordemos al respecto el delito societario y la responsabilidad civil del Auditor (Informático).

10. Fecha del Informe

El tiempo no es neutral; la fecha del Informe es importante, no sólo por la cuantificación de honorarios y el cumplimiento con el cliente, sino para conocer la magnitud del trabajo y sus aplicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo, incluso la del cierre del ejercicio, si es que se está realizando **un Informe de Auditoría Informática como herramienta de apoyo a la Auditoría de Cuentas.** En casos conflictivos pueden ser relevantes aspectos tales como los hechos posteriores al fin del período de auditoría, hechos anteriores y posteriores al trabajo de campo...

11. Identificación y firma del Auditor

Este aspecto formal del informe es esencial tanto si es individual como si forma parte de una sociedad de auditoría, que deberá corresponder a un socio o socios legalmente así considerados.

12. Distribución del Informe

Bien en el contrato, bien en la carta propuesta del Auditor Informático, deberá definirse quién o quiénes podrán hacer uso del Informe, así como los usos concretos que tendrá, pues los honorarios deberán guardar relación con la responsabilidad civil.

4.7. CONCLUSIONES

¿Qué es el informe de auditoría informática y qué le diferencia de otro tipo de informes (consultaría, asesoría, servicios profesionales...) de informática?

Resulta básico, antes de redactar el informe de auditoría, que el asunto esté muy claro, no sólo por las expectativas ya citadas, sino porque cada término tiene un contenido usual muy concreto; la etiqueta auditoría es, en esencia, un juicio de valor u opinión con justificación.

Por tanto, habida cuenta que tiene base objetiva –sobre todo con independencia en sentido amplio–, es eminentemente una opinión profesional subjetiva.

Además, como se aplican criterios en términos de probabilidad, hay que evitar la predisposición a algún posible tipo de manipulación, debido a la libertad de elección de pruebas; no se debe elegir una serie de ellas que dé la imagen buscada (prejuicio) como consecuencia de la acumulación de sesgos *ad hoc*.

Esta insistencia en clarificar es quizá excesiva, pero resulta importante emitir el Informe de auditoría informática de acuerdo con la aplicación de la Auditoría Informática con criterios éticamente profesionales y desestimar los procedimientos de Auditoría Informática "creativa" sorteando la posible "contaminación" con la contabilidad "creativa".

En el precitado Libre Verde de Auditoría Legal de la Unión Europea y recordando la Directiva Octava de Derecho de Sociedades, se señala que el auditor debe ser independiente, pero sólo la FEE señala que puede serlo de una manera objetiva.

Es ilustrativo revisar textualmente el punto 4.9 del famoso Libro Verde:

"En años recientes, se ha manifestado preocupación sobre las amenazas que se ciernen sobre la independencia de los auditores. Varias encuestas indican el hecho de que las empresas están cada vez más preparadas a desafiar a los auditores, comprar opiniones, buscar asesoramiento legal sobre las opiniones de los auditores y a cambiar de auditores. Algunos informes concluyen que, dadas las presiones competitivas, sería idealista asumir que todos los auditores actúan en todo momento sin pensar en el riesgo de perder clientes. Se han manifestado críticas de que el profesionalismo se ha disminuido en favor de una actitud más de negocio."

En fin, que como indicio del estado del arte, este párrafo resulta bastante aleccionador.

Navegando entre definiciones y definiciones, encuentro muy explicativa la de ISACF, que dice así:

"La auditoría de sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o alguna sección/área) de los sistemas automatizados de procesamiento de la información, incluyendo procedimientos relacionados no automáticos y las interrelaciones entre ellos."

Creo que precisa lo suficiente sobre el sistema informático, el manual y sus conexiones para delimitar los objetivos de cobertura de un informe de auditoría informática que, ponderados con los objetivos COSO de la Actividad de Tecnologías de la Información (planes estratégicos, información fiable, adecuada y disponible, y sistemas de información disponibles), clarifican en forma razonable las zonas fronterizas con otros temas afines, por ahora.

En mi opinión, Maastricht está acelerando el asunto; tanto es así que si Maastricht no existiera habría que inventarlo, aunque el término auditoría tiene connotaciones no deseables. Espero que el MARC (Maastricht Accounting and Auditing Research Center) sea un factor positivo en la auditoría de los sistemas de información y, por tanto, en los informes y su normativa legal/profesional correspondiente.

4.8. LECTURAS RECOMENDADAS

Emilio del Peso Navarro, Miguel Ángel Ramos González, Carlos Manuel Fernández Sánchez y María José Ignoto Azaustre. *Manual de dictámenes y peritajes informáticos. Ediciones Díaz de Santos, S.A. Madrid, 1995.*

Agustín López Casuso. *Normas de Auditoría: Cómo Interpretarlas para su Aplicación.* Editorial IACJCE. Madrid, 1995.

Luis Muñoz Sabate. *Técnica Probatoria: Estudio sobre las Dificultades de la Prueba en el Proceso.* Editorial Praxis, S.A. Barcelona, 1993, 4ª edición.

Mary C. Bromake. *Los informes de auditoría y su técnica de redacción.* Editorial Deusto, S.A. Bilbao, 1989.

Revista SIC, Seguridad en Informática y Comunicaciones. Ediciones Coda, S.L. Madrid.

4.9. CUESTIONES DE REPASO

1. ¿Qué diferencia existe entre evidencia suficiente y evidencia adecuada?
2. ¿Qué diferencia existe entre prueba de cumplimiento y prueba sustantivo?
3. ¿Las normas IFAC son vinculantes en España?
4. ¿Las normas ISACF son vinculantes en España?
5. ¿Qué diferencia existe entre opinión desfavorable y opinión denegada?
6. ¿Qué significa importancia relativa?, ¿y materialidad?
7. ¿Qué significado tiene la responsabilidad civil del auditor informática emisor del informe de auditoría informática y firmante del mismo?
8. ¿Cuál es la utilidad del documento denominado Declaraciones de la Dirección?
9. ¿Qué diferencia existe entre experto informática y auditor informático?
10. ¿Qué diferencia existe entre auditor interno y auditor externo?

CAPÍTULO 5

ORGANIZACIÓN DEL DEPARTAMENTO DE AUDITORÍA INFORMÁTICA

Rafael Ruano Díez

5.1. ANTECEDENTES

El concepto de auditoría informática ha estado siempre ligado al de auditoría en general y al de auditoría interna en particular, y éste ha estado unido desde tiempos históricos al de contabilidad, control, veracidad de operaciones, etc. En tiempo de los egipcios ya se hablaba de contabilidad y de control de los registros y de las operaciones. Aun algunos historiadores fijan el nacimiento de la escritura como consecuencia de la necesidad de registrar y controlar operaciones (Dale Flesher, *50 Years of Progress).* Hago esta referencia histórica a fin de explicar la evolución de la corta pero intensa historia de la auditoría informática, y para que posteriormente nos sirva de referencia al objeto de entender las diferentes tendencias que existen en la actualidad.

Si analizamos el nacimiento y la existencia de la auditoría informática desde un punto de vista empresarial, tendremos que empezar analizando el contexto organizativo y ambiental en el que se mueve.

Empezaremos diciendo que tanto dentro del contexto estratégico como del operativo de las organizaciones actuales, los sistemas de información y la arquitectura que los soporta desempeñan un importante papel como uno de los soportes básicos para la gestión y el control del negocio, siendo así uno de los requerimientos básicos de cualquier organización. Esto da lugar a los sistemas de información de una organización.

Es evidente que para que dichos sistemas cumplan sus objetivos debe existir una función de gestión de dichos sistemas, de los recursos que los manejan y de las

inversiones que se ponen a disposición de dichos recursos para que el funcionamiento y los resultados sean los esperados. Esto es lo que llamamos el Departamento de Sistemas de Información.

Finalmente, y en función de lo anterior, aunque no como algo no enteramente aceptado aún, debe existir una función de control de la gestión de los sistemas y del departamento de sistemas de información. A esta función la llamamos auditoría informática.

El concepto de la función de auditoría informática, en algunos casos llamada función de control informático y en los menos, llamada y conocida por ambos términos, arranca en su corta historia, cuando en los años cincuenta las organizaciones empezaron a desarrollar aplicaciones informáticas. En ese momento, la auditoría trataba con sistemas manuales. Posteriormente, en función de que las organizaciones empezaron con sistemas cada vez más complejos, se hizo necesario que parte del trabajo de auditoría empezara a tratar con sistemas que utilizaban sistemas informáticos.

En ese momento, los equipos de auditoría, tanto externos como internos, empezaron a ser mixtos, con involucración de auditores informáticos junto con auditores financieros. En ese momento se comenzaron a utilizar dos tipos de enfoque diferentes que en algunos casos convergían:

- Trabajos en los que el equipo de auditoría informática trabajaba bajo un programa de trabajo propio, aunque entroncando sus objetivos con los de la auditoría financiera; éste era el caso de trabajos en los que se revisaban controles generales de la instalación y controles específicos de las aplicaciones bajo conceptos de riesgo pero siempre unido al hecho de que el equipo de auditoría financiera utilizaría este trabajo para sus conclusiones generales sobre el componente financiero determinado.

- Revisiones en las que la auditoría informática consistía en la extracción de información para el equipo de auditoría financiera. En este caso el equipo o función de auditoría interna era un exponente de la necesidad de las organizaciones y departamentos de auditoría de utilizar expertos en informática para proveer al personal de dicho departamento de información extraída del sistema informático cuando la información a auditar estaba empezando a ser voluminosa y se estaba perdiendo la pista de cómo se había creado.

Esta situación convive hoy en día con conceptos más actuales y novedosos de lo que es la función y de lo que son los objetivos de la auditoría informática.

En mi opinión, y es algo que vamos a desarrollar a continuación, la tendencia futura de la auditoría informática radicará en los siguientes principios:

1. Todos los auditores tendrán que tener conocimientos informáticos que les permitan trabajar en el cada vez más fluctuante entorno de las tecnologías de la información dentro de las organizaciones empresariales, culturales y sociales.

2. Este aspecto no eliminará la necesidad de especialistas en auditoría informática; antes al contrario, los especialistas necesitarán cada vez más, unos conocimientos muy específicos, que al igual que sucede en el entorno de los sistemas de información, les permitan ser expertos en las diferentes ramas de la tecnología informática: comunicaciones, redes, ofimática, comercio electrónico, seguridad, gestión de bases de datos, etc.

3. El auditor informática dejará de ser un profesional procedente de otra área, con su consiguiente reciclado, para pasar a ser un profesional formado y titulado en auditoría informática que tendrá a su alcance diferentes medios de formación, externa fundamentalmente, y que tendrá que formar una red de conocimientos compartidos con otros profesionales, tanto en su organización como con profesionales de otras organizaciones.

El futuro de la auditoría informática estará en la capacidad de cubrir adecuadamente, en cuanto a experiencia y especialización, todas las áreas de los sistemas informáticos y de información de una empresa y en saber de forma propia o con ayuda interna y externa, adecuarse a los cambios que sucedan en la Tecnología de la Información. Para adecuarse a estos cambios, el auditor informático, tendrá que autogenerar su propia filosofía de gestión del cambio.

5.2. CLASES Y TIPOS DE AUDITORÍA INFORMÁTICA

Como he tratado de mencionar anteriormente, existe una gran confusión sobre lo que es auditoría informática y la relación que tiene con otras ramas organizativas de las empresas y organizaciones. Aun hoy en día, si preguntásemos a diferentes agentes empresariales y sociales, nos contestarían con diferentes respuestas sobre lo que es y no es auditoría informática.

Voy a tratar de resumir las diferentes acepciones de auditoría informática que existen en nuestro país:

- Auditoría informática como soporte a la auditoría tradicional, financiera, etc.

- Auditoría informática con el concepto anterior, pero añadiendo la función de auditoría de la función de gestión del entorno informático.

- Auditoría informática como función independiente, enfocada hacia la obtención de la situación actual de un entorno de información e informático en aspectos de seguridad y riesgo, eficiencia y veracidad e integridad.
- Las acepciones anteriores desde un punto de vista interno y externo.
- Auditoría como función de control dentro de un departamento de sistemas.

Ante esta situación déjenme expresar cuál es mi visión sobre lo que es y debe ser la función de auditoría informática.

5.3. FUNCIÓN DE AUDITORÍA INFORMÁTICA

5.3.1. Definición

Está claro a estas alturas que la auditoría, revisión, diagróstico y control de los sistemas de información y de los sistemas informativos que soportan éstos deben ser realizados por personas con experiencia en ambas disciplinas, informática y auditoría (en principio llamemos a nuestro amigo el Auditor Informático General: AIG). A esto yo le añado que además nuestro amigo debe completar su formación con conocimientos de gestión del cambio y de gestión empresarial.

¿Cómo definimos entonces a nuestro amigo AIG? Para tratar de definir su perfil, la definición más exacta es quizá que es un profesional dedicado al análisis de sistemas de información e informáticos que está especializado en alguna de las múltiples ramas de la auditoría informática, que tiene conocimientos generales de los ámbitos en los que, ésta se mueve, que tiene conocimientos empresariales generales, y que además:

Posee las características necesarias para actuar como consultor con su auditado, dándole ideas de cómo enfocar la construcción de los elementos de control y de gestión que le sean propios.

Y que puede actuar como consejero con la organización en la que está desarrollando su labor. Un entorno informático bien controlado, puede ser un entorno ineficiente si no es consistente con los objetivos de la organización.

El eterno problema que se ha suscitado durante mucho tiempo es si el auditor informático, al no existir tal formación académica en nuestro país, tenía que ser un auditor convertido en informática, o por el contrario un informático reciclado como auditor informático. En mi larga experiencia, he visto de todo, personal de desarrollo o de explotación convertidos en auditores informáticos en menos de un mes, auditores financieros reciclados, primero como extractores de información, mediante la formación en el adecuado software de interrogación de archivos, y posteriormente convertidos en auditores de la función informática.

En ambos casos, los éxitos y los fracasos se acumulaban por igual. ¿Qué hacer en estos casos? ¿Cuál debe ser el perfil correcto de un auditor informático? Ésta es mi visión y opinión del perfil del futuro auditor informático y consecuentemente de las funciones que la función de auditoría informática debe tener.

5.3.2. Perfiles profesionales de la función de Auditoría Informática

A tenor de lo que hemos dicho hasta ahora, se ve claramente que el auditor informático debe ser una persona con un alto grado de calificación técnica y al mismo tiempo estar integrado en las corrientes organizativas empresariales que imperan hoy en día. De esta forma, dentro de la función de auditoría informática, se deben contemplar las siguientes características para mantener un perfil profesional adecuado y actualizado:

1. La persona o personas que integren esta función deben contemplar en su formación básica una mezcla de conocimientos de auditoría financiera y de informática general. Estos últimos deben contemplar conocimientos básicos en cuanto a:

   - Desarrollo informático; gestión de proyectos y del ciclo de vida de un proyecto de desarrollo.
   - Gestión del departamento de sistemas.
   - Análisis de riesgos en un entorno informático.
   - Sistema operativo (este aspecto dependerá de varios factores, pero principalmente de si va a trabajar en un entorno único –auditor interno– o, por el contrario, va a tener posibilidades de trabajar en varios entornos como auditor externo).
   - Telecomunicaciones.
   - Gestión de bases de datos.
   - Redes locales.
   - Seguridad física.
   - Operaciones y planificación informática; efectividad de las operaciones y del rendimiento de los sistemas.
   - Gestión de la seguridad de los sistemas y de la continuidad empresarial a través de planes de contingencia de la información.
   - Gestión de problemas y de cambios en entornos informáticos.
   - Administración de datos.

- Ofimática.
- Comercio electrónico.
- Encriptación de datos.

2. A estos conocimientos básicos se les deberá añadir una especialización en función de la importancia económica que distintos componentes financieros puedan tener en un entorno empresarial. Así, en un entorno financiero pueden tener mucha importancia las comunicaciones, y será necesario que alguien dentro de la función de auditoría informática tenga esta especialización, pero esto mismo puede no ser válido para un entorno productivo en el que las transacciones EDI pueden ser más importantes.

3. Uno de los problemas que más han incidido en la escasa presencia de auditores informáticos en nuestro país, es quizás la a veces escasa relación entre el trabajo de auditoría informática y las conclusiones con el entorno empresarial donde se ubicaba la "entidad auditada". Esta sensación de que las normas van por sitios diferentes de por donde va el negocio ha sido fruto muchas veces de la escasa comunicación entre el auditado (objetivos empresariales) y el auditor (objetivos de control). Como quiera que la cruda realidad nos está demostrando en la actualidad cada vez más la necesidad de cada vez mayor control en los sistemas de información, se hace necesario para el auditor informático conocer técnicas de gestión empresarial, y sobre todo de gestión del cambio, ya que las recomendaciones y soluciones que se aporten deben estar en la línea de la búsqueda óptima de la mejor solución para los objetivos empresariales que se persiguen y con los recursos que se tienen.

4. El auditor informático debe tener siempre el concepto de Calidad Total. Como parte de un colectivo empresarial, bien sea permanentemente como auditor interno o puntualmente como auditor externo, el concepto de calidad total hará que sus conclusiones y trabajo sea reconocido como un elemento valioso dentro de la organización y que los resultados sean aceptados en su totalidad. Esta aplicación organizativa debe hacer que la propia imagen del auditor informático sea más reconocida de forma positiva por la organización.

5.3.3. Funciones a desarrollar por la función de Auditoría Informática

Se han suscitado múltiples controversias sobre las funciones a desarrollar en cuanto al trabajo de Auditoría Informática que se debe realizar. ¿Cuál es el objetivo de una Auditoría Informática? ¿Qué se debe revisar, analizar o diagnosticar?

¿Puede la función de Auditoría Informática aportar sólo lo que le piden o debe formar parte de un ente organizativo total, lo que le exige una actitud de contribución total al entorno empresarial en el que está realizando su trabajo? En definitiva, ¿qué aspectos debe revisar el auditor informático? Debe revisar la seguridad, el control interno, la efectividad, la gestión del cambio y la integridad de la información.

Si analizamos la realidad más actual, diremos que la función Auditoría Informática debe mantener en la medida de lo posible los objetivos de revisión que le demande la organización, pero como esto es muy general, vamos a precisar algo más lo que sería un entorno ideal que tiene que ser auditado.

Supongamos una organización que produce componentes tecnológicos de audio y vídeo tanto en formato primario como en producto semiterminado y terminado. Esta organización mantiene sus programas y resultados de investigación bajo control informático. Además tiene las características propias de cualquier empresa productora y comercial en cuanto a sistemas de información. Mantiene en Internet un sistema de información de sus productos con la posibilidad de que usuarios de la Red puedan hacer consultas sobre diferentes características de los productos. Gasta anualmente un uno por ciento de su facturación en sus sistemas de información y un diez por ciento en investigación.

¿Cuáles serían los objetivos de revisión de la Auditoría Informática en este ejemplo? Desde luego parece que la Auditoría Informática debería enfocarse hacia aspectos de seguridad, de comercio electrónico y de control interno en general, añadiendo en función de lo expuesto en cuanto al gasto anual que debería realizarse una revisión de la efectividad del departamento.

Esto nos indica que solamente con un ejemplo simple vemos que la Auditoría Informática abarca campos de revisión más allá de los que tradicionalmente se han mantenido; esto es, la revisión del control interno informático de los servicios centrales y de las aplicaciones.

El mundo complejo de las empresas en el que nos movemos, con industrias emergentes y con una tendencia globalizadora en los negocios, hace muy necesario que los sistemas de control interno sean lo más efectivos posibles, pero también conceptos más amplios, como el riesgo de la información, la continuidad de las operaciones, la gestión del centro de información o la efectividad y actualización de las inversiones realizadas son necesarias para poder mantener el nivel competitivo que el mundo empresarial demanda a sus sistemas de información.

Es así que entonces la función de Auditoría Informática debe realizar un amplio abanico de actividades objetivas, algunas de las cuales enumero a continuación:

- Verificación del control interno, tanto de las aplicaciones como de los sistemas informáticos, centrales y periféricos.
- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de la gestión.
- Análisis de la integridad, fiabilidad y certeza de la información a través del análisis de las aplicaciones. Esta función, que la vienen desempeñando los auditores informáticos, están empezando ya a desarrollarla los auditores financieros.
- Auditoría del riesgo operativo de los circuitos de información.
- Análisis de la gestión de los riesgos de la información y de la seguridad implícita.
- Verificación del nivel de continuidad de las operaciones (a realizar conjuntamente con los auditores financieros).
- Análisis del Estado del Arte tecnológico de la instalación revisada y de las consecuencias empresariales que un desfase tecnológico pueda acarrear.
- Diagnóstico sobre el grado de cobertura que dan las aplicaciones a las necesidades estratégicas y operativas de información de la organización.

El papel de la auditoría informática se convierte de esta manera en algo más que la clásica definición del auditor informático:

"... el auditor informático es responsable para establecer los objetivos de control que reduzcan o eliminen la exposición al riesgo de control interno. Después de que los objetivos de la auditoría se hayan establecido, el auditor debe revisar los controles y evaluar los resultados de su revisión para determinar las áreas que requieran correcciones o mejoras."

Aun a riesgo de ser criticado por muchos de mis compañeros, creo que el papel del auditor informático tiene que dejar de ser el de un profesional cuya única meta empresarial sea analizar el grado de implantación y cumplimiento del control interno. Las organizaciones están invirtiendo mucho dinero en sistemas de información, cada vez son más dependientes de ellos y no pueden permitirse el lujo de tener buenos profesionales, que estaban mediatizados por esquemas que eran válidos hace unos años pero que en estos momentos no lo son a tenor de las necesidades empresariales. El concepto de control interno es importantísimo, pero además de verificar dicho control, el auditor interno tiene la obligación de convertirse un poco en consultor y en ayuda del auditado, dándole ideas de cómo establecer procedimientos de seguridad, control interno, efectividad y eficacia y medición del riesgo empresarial.

5.4. ORGANIZACIÓN DE LA FUNCIÓN DE AUDITORÍA INFORMÁTICA

Según lo que hemos comentado hasta ahora, la función de auditoría informática ha pasado de ser una función meramente de ayuda al auditor financiero a ser una función que desarrolla un trabajo y lo seguirá haciendo en el futuro, más acorde con la importancia que para las organizaciones tienen los sistemas informáticos y de información que son su objeto de estudio y análisis. El auditor informático pasa a ser auditor y consultor del ente empresarial, en el que va a ser analista, auditor y asesor en materias de:

- Seguridad
- Control interno operativo
- Eficiencia y eficacia
- Tecnología informática
- Continuidad de operaciones
- Gestión de riesgos

no solamente de los sistemas informáticos objeto de su estudio, sino de las relaciones e implicaciones operativas que dichos sistemas tienen en el contexto empresarial.

Con esta amplitud de miras, ¿cómo se va a organizar la función dentro de la empresa? Está claro que en este caso estamos hablando de una función interna de auditoría informática.

La concepción típica que he visto en las empresas españolas hasta ahora, es la de que la función de auditoría informática está entroncada dentro de lo que es la función de auditoría interna con rango de subdepartamento. Esta concepción se basa en el nacimiento histórico de la auditoría informática y en la dificultad de separar el elemento informático de lo que es la auditoría operativa y financiera, al igual que lo es separar la operativa de una empresa de los sistemas de información que los soportan.

Si volvemos a mi aseveración anterior sobre el papel que debe desempeñar el auditor informático dentro de un contexto empresarial, la organización tipo de la auditoría informática, debe contemplar en mi opinión los siguientes priacipios:

- Su localización puede estar ligada a la localización de la auditoría interna operativa y financiera, pero con independencia de objetivos (aunque haya una coordinación lógica entre ambos departamentos), de planes de formación y de presupuestos.

- La organización operativa tipo debe ser la de un grupo independiente del de auditoría interna, con una accesibilidad total a los sistemas informáticos y de información, e idealmente dependiendo de la misma persona en la empresa que la auditoría interna, que debería ser el director general o consejero delegado. Cualquier otra dependencia puede dar al traste con la imagen del auditor informático y consecuentemente con la aceptación de su trabajo y de sus conclusiones.

La dependencia, en todo caso, debe ser del máximo responsable operativo de la organización, nunca del departamento de organización o del de sistemas (abundan los casos en que esta dependencia existe), ni del departamento financiero y/o administrativo.

La gestión de la función, en la medida de que exista la experiencia, debe ser llevada a cabo por personal que haya o esté trabajando en auditoría informática.

Los recursos humanos con los que debe contar el departamento deben contemplar una mezcla equilibrada entre personas con formación en auditoría y organización y personas con perfil informático. No obstante, este perfil genérico debe ser tratado con un amplio programa de formación en donde se especifiquen no sólo los objetivos de la función, sino también de la persona.

- Este personal debe contemplar entre su titulación la de CISA como un elemento básico para comenzar su carrera como auditor informático.

- La organización interna tipo de la función podría ser:

  - Jefe del departamento. Desarrolla el plan operativo del departamento, las descripciones de los puestos de trabajo del personal a su cargo, las planificaciones de actuación a un año, los métodos de gestión del cambio en su función y los programas de formación individualizados, así como gestiona los programas de trabajo y los trabajos en sí, los cambios en los métodos de trabajo y evalúa la capacidad de las personas a su cargo.

  - Gerente o supervisor de auditoría informática. Trabaja estrechamente con el Jefe del departamento en las tareas operativas diarias. Ayuda en la evaluación del riesgo de cada uno de los trabajos, realiza los programas de trabajo, dirige y supervisa directamente a las personas en cada uno de los trabajos de los que es responsable. Realiza la formación sobre el trabajo. Es responsable junto con su jefe de la obtención del mejor resultado del trabajo para el auditado, entroncando los conceptos de valor añadido y gestión del cambio dentro de su trabajo. Es el que más "vende" la función con el auditado.

- Auditor informático. Son responsables para la ejecución directa del trabajo. Deben tener una especialización genérica, pero también una específica, según se comentó anteriormente. Su trabajo consistirá en la obtención de información, realización de pruebas, documentación del trabajo, evaluación y diagnóstico de resultados.

- El tamaño sólo se puede precisar en función de los objetivos de la función, pero en mi opinión, para una organización tipo, el abanico de responsabilidades debería cubrir:

  - Especialista en el entorno informático a auditar y en gestión de bases de datos.
  - Especialista en comunicaciones y/o redes.
  - Responsable de gestión de riesgo operativo y aplicaciones.
  - Responsable de la auditoría de sistemas de información, tanto en explotación como en desarrollo.
  - En su caso, especialista para la elaboración de programas de trabajo conjuntos con la Auditoría Financiera.

5.5. CUESTIONES DE REPASO

1. ¿Cuáles son las líneas de evolución de la Auditoría Informática?

2. ¿Qué diferentes acepciones existen de la Auditoría Informática?

3. ¿Cuál es el perfil del auditor informático general?

4. ¿Qué formación debe poseer el auditor informático?

5. ¿Cuáles son las funciones de la Auditoría Informática?

6. ¿Qué aspectos pueden hacer más compleja, en la actualidad, la función de Auditoría Informática?

7. ¿Cuál debe ser la localización de la función de Auditoría Informática en la empresa?

8. ¿Cuáles son las tareas del Jefe del Departamento de Auditoría Informática?

9. ¿Qué tamaño debe tener el Departamento de Auditoría Informática?

10. Defina un plan de formación para que un informático pueda desempeñar sin problemas la función de auditor.

CAPÍTULO 6

EL MARCO JURÍDICO DE LA AUDITORÍA INFORMÁTICA

Emilio del Peso Navarro

6.1. INTRODUCCIÓN

Los efectos de la incorporación a nuestra Sociedad en un principio de la Informática, posteriormente de la Telemática y en la actualidad de lo que se viene denominando Nuevas Tecnologías de la Información y las Comunicaciones, han transformado ésta y el futuro que se vislumbra es que el cambio ha de ser aún mayor.

La transformación ha operado en todos los órdenes de la vida tanto públicos como privados, profesionales y particulares. La forma de vida ha cambiado radicalmente y no hemos hecho más que empezar.

Conceptos tan arraigados como el de trabajo tenemos que empezar a contemplarlos de otra manera, e incluso la forma de divertirnos, nuestro ocio, también ha quedado afectado.

Estas nuevas tecnologías han incidido en el Derecho desde dos perspectivas:

1.ª Contemplar estas nuevas tecnologías como una herramienta del operador jurídico de forma parecida a como ayudan a otros profesionales: arquitectos, médicos, etc., lo que da lugar a la Informática Jurídica.

2.ª Estudiar y analizar estas nuevas tecnologías como un objeto más del Derecho, lo que hace emerger una rama nueva del mismo: el Derecho

Informático o Derecho de las Nuevas Tecnologías de la Información y las Comunicaciones.

Esta dicotomía la volveremos a ver después cuando estudiemos la contratación, en la que nos encontraremos con un tipo de contratación, la electrónica o por medios electrónicos, y con otro, la informática.

La Informática Jurídica la podemos contemplar desde tres categorías diferentes[1]:

1. La Informática Jurídica de Gestión que se presenta como un eficaz instrumento en la tramitación de los procedimientos judiciales, en la administración de los despachos de abogados, procuradores, notarios, etc.

2. La Informática Jurídica Documental que es la utilización de la Informática para facilitar el almacenamiento de enormes volúmenes de datos relativos a Legislación, Jurisprudencia y Doctrina, con el fin de permitir posteriormente el acceso a la misma de una forma fácil, rápida y segura.

3. La Informática Jurídica Decisional, por último, es la utilización de la Informática como un instrumento para ayudar a la toma de decisiones. Tal es el caso de los jueces ante las sentencias. Está basada, principalmente, en técnicas de la denominada "inteligencia artificial" con el empleo de sistemas expertos y herramientas similares.

El Derecho Informático, a diferencia de la Informática Jurídica, es aquella parte del Derecho que regula el mundo informático evitando que se convierta en una jungla donde siempre sale ganando el más fuerte. Fruto del mismo son: la protección de datos personales, la protección jurídica de los programas de computador, los delitos informáticos, el documento electrónico, el comercio electrónico, y la contratación electrónica e informática entre otras materias.

El auditor informático, si quiere realizar bien su labor y a la vez evitar situaciones desagradables y un tanto peligrosas, está obligado a conocer esta rama del Derecho, pues es la que regula el objeto de su trabajo. Desconocer las normas que regulan la protección de los datos personales, la piratería de los programas de computador, las obligaciones contractuales, los delitos informáticos, las responsabilidades civiles y penales en que puede incurrir puede tener consecuencias graves si, como es fácil que ocurra, dichas circunstancias se presentan en el entorno en que trabaja.

[1] Para más información: EMILIO DEL PESO NAVARRO y MIGUEL ÁNGEL RAMOS GONZÁLEZ. *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socio-económicas*. Díaz de Santos, Madrid. 1994. págs. 10 y 11.

Si examinamos dichas normas claramente veremos que todas ellas versan sobre un determinado bien jurídico: la información.

La información ha sido un bien valioso en todas las épocas, pero en ninguna había alcanzado la importancia que tiene en el momento actual en el que fácilmente se convierte en conocimiento.

En el pasado no existía la posibilidad, como ocurre ahora, de convertir informaciones parciales y dispersas en informaciones en masa y organizadas.

La aplicación conjunta de la Informática y las Telecomunicaciones, lo que se ha venido en denominar Telemática, en la práctica ha hecho desaparecer los factores tiempo y espacio.

Para DAVARA RODRÍGUEZ[2]: *"La información es un bien que tiene unas características determinadas y determinantes es, no cabe duda, un bien económico, pero diferente a los demás bienes económicos existentes en un mercado tradicional"*. Justifica lo anterior en las siguientes afirmaciones:

1ª Se trata de un bien que no se agota con el consumo.
2ª Es un bien que puede ser utilizado por numerosas personas a la vez.
3ª Es la base del desarrollo de la nueva sociedad.
4ª Es el vehículo que circula por las autopistas de la información.

Para definir este conjunto de circunstancias en el que nos movemos se ha acuñado el término Sociedad de la información.

La información puede ser muy variada, como veremos a continuación, y no toda ella suele tener el mismo valor.

6.2. LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El artículo 18.4 de nuestra Constitución emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de sus ciudadanos y el legítimo ejercicio de sus derechos.

Fruto de este mandato constitucional fue la promulgación de la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal **(LORTAD)**. Se trata de una ley de las que en el Derecho

[2] MIGUEL ÁNGEL DAVARA RODRÍGUEZ. *De las autopistas de la información a la sociedad virtual*. Aranzadi, Pamplona, 1996, pág. 50.

Comparado se vienen denominando leyes de protección de datos, aunque en realidad su objeto no sea la protección de los datos sino la protección de la *intimidad* y la *privacidad* de las personas titulares de esos datos.

En la Exposición de Motivos de la Ley se hace una interesante distinción entre lo que el legislador entiende por *intimidad* y por *privacidad.*

Con independencia de que muchos autores hasta ahora no hacían distinción entre *intimidad* y el anglicismo *privacidad* se empieza a hacer corresponder aquélla con los derechos defendidos en los tres primeros puntos del artículo 18 de la Constitución, y la *privacidad,* entendida como el derecho a la autodeterminación informativa, con el punto 4.

La Ley Orgánica 15/1999, de 13 de enero (LOPD) de Protección de Datos de Carácter Personal, deroga la LORTAD. Tanto la LORTAD como la LOPD se inspiran en los siguientes principios:

Principio de finalidad. Antes de la creación de un archivo de datos de carácter personal[3] ha de conocerse el fin del mismo (art. 4.1).

Este principio, a su vez, engloba otros dos: el principio de pertinencia y el de utilización abusiva.

Principio de pertinencia (art. 4.1). Los datos deben ser pertinentes, es decir estar relacionados con el fin perseguido al crearse el archivo.

Principio de utilización abusiva (art. 4.2). Los datos recogidos no deben ser utilizados para otro fin distinto a aquel para el que fueron recabados.

Principio de exactitud (art. 4.3 y 4.4). El responsable del archivo debe poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día.

Principio de derecho al olvido (art. 4.5). Los datos deberán desaparecer del archivo una vez se haya cumplido el fin para el que fueron recabados.

Principio del consentimiento (art. 6). El tratamiento automatizado de los datos requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa contemplándose algunas excepciones y teniendo el carácter de revocable.

---

[3] Datos de carácter personal son cualquier información concerniente a personas físicas, identificadas o identificables (art. 3 a LOPD y Resolución Agencia Protección de Datos).

El artículo 1.4 del Reglamento amplía esta definición diciendo que es: *"Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier tipo susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable".*

Principio de los datos especialmente protegidos (art. 7). Se debe garantizar de forma especial el tratamiento automatizado de los datos de carácter personal cuando ellos se refieran a ideología, afiliación sindical, religión o creencias del afectado, así como los referentes a su origen racial, salud, vida sexual o a la comisión de infracciones penales o administrativas.

Principio de seguridad (art. 9). El responsable deberá adoptar las medidas necesarias de índole física, organizativa o lógica con objeto de poder garantizar la seguridad de los datos de los archivos.

Principio de acceso individual (art. 14). Cualquier persona tendrá derecho a saber si sus datos son tratados de forma automatizada y a tener una copia de los mismos. En el caso de que éstos sean inexactos o se hubiesen conseguido de forma ilegal tiene derecho a que sean corregidos o destruidos.

Principio de publicidad (art. 38). Es preciso que exista un archivo público en el que figuren los diseños de los archivos de datos de carácter personal, tanto los de titularidad pública como privada.

De estos principios se derivan los siguientes derechos: derecho de oposición (art. 30), derecho de impugnación de valoraciones (art. 13), derecho de consulta al Registro General de Protección de Datos (art. 14), derecho de acceso (art. 15), derecho de rectificación y cancelación (art. 16), derecho de tutela (art. 18) y derecho de indemnización (art. 19).

Como órgano garante de estos derechos en la Ley figura la Agencia de Protección de Datos, ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. El Estatuto de la Agencia de Protección de Datos fue aprobado por Real Decreto 428/1993 de 26 de marzo y declarado subsistente por la disposición transitoria tercera de la LOPD.

Al frente de la Agencia figura un Director y consta de los siguientes órganos: Consejo Consultivo, Registro General, Inspección y Secretaría General.

Las potestades de la Agencia son las siguientes:

Potestad reguladora. Según el artículo 5 del Estatuto colabora con los órganos competentes en el desarrollo normativo así como en la aplicación de la Ley.

Potestad inspectora. Según el artículo 40 de la Ley corresponde a la Agencia la *inspección* de los archivos comprendidos en el ámbito de ésta.

Potestad sancionadora. La Agencia puede imponer multas de hasta cien millones de pesetas para los casos más graves por las infracciones cometidas en el sector

privado. Las sanciones correspondientes al sector público serán las establecidas en la legislación sobre el régimen disciplinario de las Administraciones Públicas.

Potestad inmovilizadora. El Director de la Agencia, según el artículo 49, en los supuestos constitutivos de infracción muy grave podrá, mediante resolución motivada, inmovilizar los archivos automatizados.

La Ley fue desarrollada por un Reglamento aprobado por Real Decreto 1332/1994 de 20 de junio, y el artículo 9 fue desarrollado por RD 994/1999, de 11 de junio que aprobó el Reglamento de Medidas de Seguridad, ambos declarados subsistentes por la Disposición Transitoria Tercera de la LOPD.

6.3. LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE COMPUTADOR

Antes de hablar de su protección jurídica consideramos importante explicar qué se entiende por programas de computador y cuál es su lugar entre las diferentes clases de bienes jurídicos dignos de protección en nuestro ordenamiento jurídico.

En una primera aproximación, un programa de computador se puede considerar como el conjunto de materiales elaborados conceptualmente para la solución de un problema de tratamiento automatizado de datos.

El Texto Refundido de la Ley de la Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996 de 12 de abril, en su artículo 96.1 lo define como: *"toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente en un sistema informático, para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuera su forma de expresión o fijación.*

A los mismos efectos, la expresión programas de computador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de computador".

Entre la categoría de los bienes, los programas de computador presentan peculiaridades que los diferencian de los bienes con una entidad material y susceptibles por tanto de una aprehensión física. Nuestro Código Civil divide los bienes en corporales e incorporales.

Un programa de computador, como una creación de la mente que es, no puede ser incluido en ninguna de estas dos categorías, por lo que hay que acudir a una nueva que es la que se ha creado para este tipo de bienes, la de los bienes inmateriales.

Un bien inmaterial es:

- Fruto o creación de la mente.
- Para que se haga perceptible para el mundo exterior es necesario plasmarlo en un soporte.
- Puede ser disfrutado simultáneamente por una pluralidad de personas.

Por todo ello la apropiación en los bienes inmateriales, por sí sola, no es suficiente para garantizar su goce exclusivo, a diferencia de lo que ocurre con los bienes materiales.

Si queremos que el titular de un bien inmaterial disfrute en exclusiva del mismo es preciso, desde el punto de vista jurídico, que el Derecho prohíba a todos los demás la utilización o la explotación del mismo y otorgue al titular un derecho en exclusiva.

Un programa de computador, como se desprende de lo expuesto, es un bien inmaterial y en función de tal hemos de procurar su protección jurídica.

La protección jurídica de los programas de computador, en principio, se puede instrumentar utilizando las siguientes instituciones jurídicas conocidas: estipulaciones contractuales, secreto comercial, derecho de patentes, derecho de marcas y derecho de autor.

Como fácilmente se desprende las cuatro primeras tienen una eficacia limitada, siendo más amplia la última, por lo que es éste el sistema elegido por considerarlo, a pesar de las dificultades que presenta, el más idóneo. No obstante, la protección que el derecho otorga a los programas de computador es compatible con la protección que se le pudiera otorgar por otra vía.

La protección de los programas de computador está regulada en el Texto Refundido de la Ley de la Propiedad Intelectual (a partir de ahora TRPI).

El artículo 10 del TRPI al referirse al objeto de la propiedad intelectual dice: *"Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte tangible o intangible, actualmente conocido o que se invente en el futuro"*, y al enumerar las obras comprendidas incluye entre ellas los programas de computador.

El TRPI regula la protección de los programas de computador en el Título VII del Libro I (arts. 95 a 104).

El artículo 95 señala que *"el derecho de autor sobre los programas de computador se regirá por los preceptos del presente Título y, en lo que no está específicamente*

previsto en el mismo, por las disposiciones que resulten aplicables de la presente Ley".

El autor por el solo hecho de crear una obra tiene una serie de derechos que se dividen en: morales y patrimoniales o de explotación.

Los derechos morales, enumerados en el artículo 14, son irrenunciables e inalienables.

Por contra los derechos patrimoniales o de explotación pueden ser transferidos libremente. Según el artículo 17 *"corresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizados sin su autorización, salvo en los casos previstos en la presente Ley".*

El artículo 100 fija unos límites a los derechos de explotación en función de las peculiaridades propias de los programas de computador principalmente referidos a la copia de seguridad y la interoperabilidad.

Por reproducción, según el artículo 18, *"se entiende la fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella".*

Distribución, según el artículo 19 es *"la puesta a disposición del público del original o copias de la obra mediante su venta, alquiler o préstamo o de cualquier otra forma".*

Según el artículo 20.1: *"Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas."*

La transformación de la obra, a tenor del artículo 21.1 *"comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente".*

En principio el titular exclusivo de los derechos de explotación es el propio autor (art. 17).

A la titularidad de los derechos sobre los programas de computador dedica el TRPI el artículo 97 presentándose los siguientes casos:

> *"1. Será considerado autor del programa de computador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.*

2. *Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite o divulgue bajo su nombre.*

3. *Los derechos de autor sobre un programa de computador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.*

4. *Cuando un trabajador asalariado cree un programa de computador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de computador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario."*

Cuando exista una relación mercantil se estará a lo pactado en el contrato.

La titularidad de los derechos habrá de demostrarse por alguno de los medios de prueba admitidos en derecho. El artículo 6.1 dice: *"Se presumirá autor, salvo prueba en contrario, a quien aparezca como tal en la obra mediante su nombre, firma o signo que lo identifique."*

La inscripción de un programa de computador en el Registro de la Propiedad Intelectual no es constitutiva de derechos, sino simplemente declarativo de los derechos de propiedad intelectual sobre aquél, no constituyendo una prueba indestructible sobre la titularidad de una obra determinada, sino que constituye una nueva presunción de dicha titularidad.

Las infracciones del derecho de autor pueden ser perseguidas por la vía civil y la vía penal.

El Título I del Libro III está dedicado a las acciones y procedimientos para la protección de los derechos reconocidos en la Ley.

Como medidas de protección figuran:

- Cese de la actividad ilícita (art. 139).
- Indemnización de los daños materiales y morales causados (art. 140).
- Medidas cautelares (arts. 141, 142 y 143).

El artículo 102 está referido a la infracción de los derechos respecto a los programas de computador:

> *"a) Quienes pongan en circulación una o más copias de un programa de computador conociendo o pudiendo presumir su naturaleza ilegítima.*
>
> *b) Quienes tengan con fines comerciales una o más copias de un programa de computador, conociendo o pudiendo presumir su naturaleza ilegítima.*
>
> *c) Quienes pongan en circulación o tengan con fines comerciales cualquier instrumento cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de computador."*

En la vía penal las infracciones del derecho están tipificadas en los artículos 270, 271 y 272 del Código Penal[4] pudiendo llegar las penas de prisión a cuatro años y las multas a veinticuatro meses para los casos más graves.

6.4. LAS BASES DE DATOS Y LA MULTIMEDIA

Una base de datos, como dice DAVARA RODRÍGUEZ, a quien seguiremos en este apartado, es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada para la resolución de un problema planteado en una consulta.

JAMES MARTIN define la base de datos como una colección de datos interrelacionados almacenados en conjunto sin redundancias perjudiciales o innecesarias; su finalidad es la de servir a una aplicación o más, de la mejor manera posible; los datos se almacenan de modo que resulten independientes de los programas que los usan; se emplean métodos bien determinados para incluir datos nuevos y para modificar o extraer los datos almacenados. Dícese que un sistema comprende una colección de bases de datos cuando éstas son totalmente independientes desde el punto de vista estructural.

Una base de datos se compone de un contenido y de una estructura de ese contenido.

El contenido de una base de datos puede ser: textos, gráficos, sonidos, imágenes fijas e imágenes en movimiento.

En lenguaje informático a esto se le suele denominar *media*, a la que nos referiremos específicamente más adelante.

---

[4] Ley Orgánica 10/1995 de 23 de noviembre.

Lógicamente cada uno de estos contenidos tendrá un titular de los derechos de autor sobre los mismos.

Pero con independencia de esto, que es importante y que habrá de tenerse en cuenta a la hora de crear una base de datos, lo que aquí tratamos de buscar es la protección jurídica de esa estructura para la que ha sido necesaria una obra de creatividad al seleccionar, clasificar y ordenar sus respectivos contenidos. En definitiva se trata de una obra de creatividad intelectual y, por tanto, objeto de protección. Hay veces, sin embargo, que no se trata de una creatividad intelectual, y no obstante su valor económico es grande.

Las primeras bases están protegidas por el derecho de autor y las segundas por un derecho *sui generis* al que se refiere la Directiva de la Unión Europea 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996.

Es importante analizar la función de los diferentes autores que participan en la creación, desarrollo y explotación de una base de datos, sus relaciones contractuales y la protección jurídica de la titularidad de las bases de datos.[5]

En un principio en una base de datos participan: el creador o promotor, el distribuidor y el usuario.

Creador o promotor es toda aquella persona física o jurídica que partiendo de una idea selecciona, clasifica y ordena un determinado tipo de información creando una base de datos, la mantiene y la actualiza.

Distribuidor es asimismo toda persona física o jurídica que comercializa el producto.

Por último, usuario es toda persona física o jurídica que utiliza y consulta la base.

Entre creador o promotor y distribuidor existe una relación contractual en la que el primero se compromete a la creación, mantenimiento y actualización de la base y el segundo a su comercialización, aunque en algún caso podría llegar a su distribución gratuita.

Los contratos entre el distribuidor y el usuario suelen ser de los denominados de adhesión, en los que el primero fija las condiciones y el segundo simplemente se adhiere a ellas.

[5] Para ampliar el tema ver: JORGE PÁEZ MAÑÁ. *Bases de Datos Jurídicas*. Cindoc. CSIC, Madrid, 1995.

La protección jurídica en nuestro ordenamiento jurídico viene dada por el vigente Texto Refundido de la Ley de la Propiedad Intelectual de 12 de abril de 1996 y por la Directiva de la Unión Europea, incorporada al ordenamiento jurídico español por la Ley 5/1998 de 6 de marzo.

En definitiva lo que se protege en una base de datos no es simplemente el almacenamiento de obras, su ordenación y recuperación, sino que es todo el procedimiento de creación y el resultado final de la misma, en cuanto a su contenido, análisis, almacenamiento, clasificación, selección. y ordenación que caracteriza a la base de datos en sí.

Como hemos dicho anteriormente, en lenguaje informática se denomina *media* a las diferentes clases de archivos que se pueden utilizar en un sistema:

Siguiendo a MILLÉ éstos pueden ser los siguientes:

a) Archivos de textos. Éstos contienen la descripción numérica de la información redactada mediante signos alfanuméricos.

b) Archivos gráficos. Contienen la descripción numérica de un diseño.

c) Archivos de sonidos. Contienen la descripción numérica de una onda sonora.

d) Archivos de imágenes fijas. Contienen la descripción numérica de una imagen formada por píxeles ordenados en columnas y filas.

e) Archivos de imágenes en movimiento. Contienen la descripción numérica de imágenes en movimiento y se llaman corrientemente vídeos.

Estos archivos se pueden procesar simultáneamente y almacenar en el mismo soporte. Esta combinación de archivos permite producir creaciones multimedia.

Multimedia se puede definir como la combinación de todo tipo de señales de voz, datos, imágenes y escritura. Es un concepto global que abarcará una gran diversidad de servicios.

Entre las obras multimedia encontramos:

a) Videojuegos. Se suele tratar de obras creadas como multimedia y no suelen incorporar elementos de obras ajenas.
b) Educación y entretenimiento. Programas de enseñanza y de entrenamiento.
c) *Edutainment.* Productos que enseñan al usuario mientras juega.
d) Revistas.

e) Publicidad.
f) Simuladores.

Las obras multimedia suelen ser producto de un equipo, se trata de obras colectivas y su titularidad suele tenerla una persona jurídica.

En gran número de casos una obra multimedia será una obra derivada, pues se trabajará sobre una obra ya existente de la que se deberán tener los derechos correspondientes salvo que se trate de obras de dominio público.

Para la creación de obras multimedia se suelen utilizar las llamadas herramientas, por ejemplo: lenguajes de autor. De estas herramientas se deberá tener licencia para su uso.

Igualmente se suelen utilizar gráficos, fotografías, etc. que existen en archivos creados al efecto y también habrá de contratarse su utilización.

Puede suceder también que se incluyan obras de vídeo con interpretación de artistas, con los que habrá que contratar la necesaria autorización.

En resumen, el mundo de la multimedia es un sector en gran auge que como todo lo nuevo plantea problemas en las relaciones entre los intervinientes que el derecho deberá resolver en aquello que aún no esté contemplado en el ordenamiento jurídico.

6.5. LOS DELITOS INFORMÁTICOS

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La definición de delito puede ser más compleja.

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquélla condiciona a ésta.

Según el ilustre penalista CUELLO CALÓN los elementos integrantes del delito son:

a) El delito es un acto humano, es una acción (acción u omisión).
b) Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.
c) Debe corresponder a un tipo legal (figura de delito), definido por la ley, ha de ser un acto típico.

d) El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.
e) La ejecución u omisión del acto debe estar sancionada con una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado con una pena.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la ley, que se realiza en el entorno informático y está sancionado con una pena.

Contemplado el delito informático en un sentido amplio se pueden formar varios grandes grupos de figuras delictivas claramente diferenciadas:

a) Delitos contra la intimidad.
b) Delitos contra el patrimonio.
c) Falsedades documentales.

El Código Penal vigente, al que nos referiremos a partir de ahora, fue aprobado por la Ley Orgánica 10/1995 de 23 de noviembre.

Delitos contra la intimidad

El Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, dedica su Capítulo Primero, que comprende los artículos 197 al 200, al descubrimiento y revelación de secretos.

Este capítulo, aparte de otras materias, viene a regular, en sede penal, las infracciones que se cometan en el ámbito de la Ley Orgánica 5/1992, de 29 de octubre, LORTAD.

El artículo 197, en su punto 1, contempla la figura de quien para descubrir los secretos o vulnerar la intimidad de otro se apodera de mensajes de correo electrónico o cualesquiera otros documentos. Aquí entendemos que, a tenor de lo que dispone el artículo 26 de la Ley, se encuentra comprendido cualquier tipo de documento electrónico.

En el mismo punto también se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de

comunicación. Pensamos que entre lo anterior se encuentra el pinchado de redes informáticas. Es importante advertir que en este punto no se hable para nada de datos de carácter personal ni de datos automatizados, a los que se refiere el mismo artículo en el punto siguiente, sino a secretos y a vulneración de la intimidad en general.

El punto 2 del artículo se refiere específicamente a datos de carácter personal pero abarcando no sólo como actualmente hace la LORTAD, los archivos informáticos, electrónicos o telemáticos, sino también los archivos convencionales.

"Las mismas penas se impondrán a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien sin estar autorizado acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

En los puntos siguientes del artículo las penas se agravan si los datos se difunden, revelan o ceden. Asimismo se sanciona a quien conociendo su origen ilícito y sin haber tomado parte en el descubrimiento los difunda, revele o ceda.

El hecho de que quien cometa el delito sea el encargado o el responsable del archivo agrava la pena.

Existen unas circunstancias agravantes que se dan en función de:

a) El carácter de los datos: ideología, religión, creencias, salud, origen racial y vida sexual.
b) Las circunstancias de la víctima: menor de edad o incapaz.

El hecho de que se persiga un fin lucrativo igualmente eleva la pena.

La condición de autoridad o funcionario público agrava las penas dada la situación de privilegio en que actúa (art. 198).

Delitos contra el patrimonio

Los delitos contra el patrimonio y contra el orden socioeconómico figuran en el Título XIII.

Es importante, en el dominio en que nos movemos, lo que se dice en el artículo 239, al tratar de las llaves falsas, al considerar llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Así las tarjetas magnéticas sustraídas a sus propietarios se considerarán llaves falsas. Es importante esta consideración en relación con el artículo 238 en que para calificar un delito de robo con fuerza en las cosas es necesario que concurra alguna de varias circunstancias entre las que se encuentra el uso de llaves falsas.

Entre los delitos contra el patrimonio se encuentran: la estafa informática, las defraudaciones, los daños informáticos y la propiedad intelectual.

Estafas informáticas (art. 248.2)

La estafa se puede definir[6] como el perjuicio patrimonial realizado con ánimo de lucro mediante engaño.

El engaño es elemento necesario de este delito. Consiste, según CUELLO CALÓN, en aprovecharse del error provocado o mantenido por el agente en la persona engañada.

Hasta la entrada en vigor del nuevo Código Penal ha sido difícil reconducir determinados fraudes informáticos hacia la figura de la estafa debido a la inexistencia del elemento de engaño a una persona.

El punto 2 del artículo 248 dice: *"También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero."*

Defraudaciones (art. 256)

Se considera defraudación el uso, sin consentimiento de su titular, de cualquier equipo terminal de telecomunicación.

---

[6] EUGENIO CUELLO CALÓN. *Derecho Penal II (Parte Especial. Volumen segundo).* Bosch, Barcelona, 1972, pág. 914.

Daños informáticos (art. 264.2)

Según el artículo 264.2 se sanciona *"al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos"*.

Entre esas situaciones se pueden incluir los famosos virus informáticos, bombas lógicas y *hackers*.

Propiedad intelectual (arts. 270, 271 y 272)

Los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores se contemplan en el Capítulo IX.

"Artículo 270. Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinado a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de computador."

Es interesante advertir que no sólo se sanciona la fabricación o puesta en circulación, sino la simple tenencia de un dispositivo para saltarse las llaves lógicas o las famosas "mochilas".

Se elevan las penas si el beneficio obtenido es cuantioso o el daño causado es grave, y además se inhabilita al autor del delito para el ejercicio de la profesión relacionada con el delito cometido (art. 271).

Estos artículos son, en sede penal, la respuesta a esa lacra de nuestro tiempo que es la piratería informática.

Ésta resulta muy dañina para el desarrollo informático, pero entendemos que sólo con la amenaza de una sanción penal no se soluciona el problema. Es necesaria una labor educativa, pues hasta que no hayamos convencido al infractor de que cuando está copiando ilegalmente un programa de computador es como si estuviese robando la cartera a otra persona, difícilmente se hallará solución. Insistimos: resulta vital esa labor educativa.

Delitos de falsedades

Las falsedades se contemplan en el Título XVIII del Código. La asimilación que hace el artículo 387 de las tarjetas de débito y de crédito a la moneda es muy importante de cara a la defensa de éstas frente al ataque criminal de que están siendo objeto.

En el artículo 386 se sanciona su falsificación y puesta en circulación.

A la falsificación de los documentos públicos oficiales y mercantiles y de los despachos transmitidos por los servicios de telecomunicación se dedica la Sección 1ª del Capítulo II de este Título (arts. 390 a 395 y 400). Como decíamos al principio el artículo 26 del Código, al considerar documento todo soporte material que exprese o incorpore datos con eficacia probatoria o cualquier tipo de relevancia jurídica permite que cualquier artículo del Código que se refiera a un documento pueda ser aplicado a éste aunque sea electrónico.

6.6. LOS CONTRATOS INFORMÁTICOS

El contrato informático, según DAVARA RODRÍGUEZ[7] *"es aquel cuyo objeto es un bien o un servicio informático –o ambos– o que una de las prestaciones de las parte tenga por objeto ese bien o servicio informático."*

No existe un *numerus clausus* de los contratos informáticos y pueden seguir multiplicándose, lo que viene sucediendo en función de los avances técnicos y de su mayor utilización por la sociedad.

Los contratos informáticos se suelen dividir en tres grandes grupos: *hardware*, *software* y servicios.

Entendemos que esta división no responde ya a la realidad, y para una mayor clarificación del problema y una mayor homogeneidad esta clasificación se debe ampliar del siguiente modo:

[7] MIGUEL ÁNGEL DAVARA RODRÍGUEZ. *Derecho Informático*. Aranzadi, Pamplona, 1993, pág. 211.

1. Contratación del *hardware*.
2. Contratación del *software*.
3. Contratación de datos.
4. Contratación de servicios.
5. Contratos complejos.

Hasta el presente, el tercer grupo dedicado a los servicios venía siendo una especie de cajón de sastre donde iban a parar todos los contratos que no se referían específicamente al *hardware* o al *software*. Así contemplábamos en ese grupo la comercialización de los datos y una serie de contratos de cierta complejidad que comprendían en sí mismos aspectos de *hardware, de software* y de servicios.

Contratación del *hardware*

El objeto de la contratación en esta clase de contratos es el *hardware*, o sea, la parte física del computador y de sus equipos auxiliares.

Este tipo de contratos no suelen presentar problemas específicos. Los contratos más usuales son los siguientes:

a) Compraventa.
b) Arrendamiento.
c) Arrendamiento financiero *(leasing)*.
d) Mantenimiento.

Contratación del *software*

Ya nos hemos referido a esta categoría de bienes anteriormente y a sus especiales peculiaridades. Los contratos más corrientes son los siguientes:

Desarrollo de software

Se trata del caso en que una persona física, un colectivo o una empresa crean un *software* específico, a medida para otro. El tipo de contrato puede ser: arrendamiento de servicios o de obra, mercantil o laboral.

Licencia de uso

Es el contrato en virtud del cual el titular de los derechos de explotación de un programa de computador autoriza a otro a utilizar el programa, conservando el cedente

la propiedad del mismo. Esta autorización, salvo pacto en contrario, se entiende de carácter no exclusivo e intransferible.

Adaptación de un software producto

Se trata de la contratación de una licencia de uso de un producto estándar que habrá que adaptar a las necesidades del usuario.

Mantenimiento

El contrato de mantenimiento, en principio, tiene por objeto corregir cualquier error detectado en los programas fuera del período de garantía. Se consideran varios tipos de mantenimiento: correctivo, de adaptación, perfectivo y preventivo.

Garantía de acceso al código fuente

Es aquel que tiene por objeto garantizar al usuario el acceso a un programa fuente en el caso de que desaparezca la empresa titular de los derechos de propiedad intelectual. Consiste en el depósito del programa fuente en un fedatario público, que lo custodia, por si en el futuro es preciso acceder al mismo.

Contratación de datos

El valor de la información en esa sociedad del saber a la que nos referíamos antes aumenta cada día. La comercialización de las bases de datos es ya muy importante, y la apertura de esas autopistas de la información, de las que tanto se escribe, hará crecer exponencialmente ese mercado.

Los principales contratos son los siguientes:

Distribución de la información

El contrato de distribución, según PÁEZ MAÑÁ[8] *"consiste en la comercialización de la base de datos, durante un cierto período de tiempo a cambio de un precio, lo que origina la obligación por parte del titular de la base de aportar los datos que deben hacerse accesibles a los futuros usuarios, en una forma adecuada para su tratamiento por el equipo informático del distribuidor, y ceder a este último,*

[8] JORGE PÁEZ MAÑÁ. *Bases de datos jurídicos*. Cindoc. CSIC, Madrid, 1994, pág. 186.

en exclusiva o *compartidos con otros distribuidores, los derechos de explotación que previamente haya adquirido por cesión o transmisión de los autores de las obras".*

Suministro de información

Mediante este contrato el usuario puede acceder, siempre que lo precise, a las bases de datos del distribuidor.

Compra

Es un contrato por el que el titular propietario de una base de datos vende a otro una copia de ésta con la posibilidad de que el adquirente, a su vez, pueda no sólo usarla sino mezclarla con otras propias para después comerciar con ellas. Todo ello, por supuesto, respetando lo dispuesto en la Ley 5/1992.

Cesión

Es un caso parecido al anterior salvo que sólo se permite el uso por el cesionario de la base sin que se le permita la transmisión posterior.

Compra de etiquetas

En este caso no se permite al comprador la reproducción de las etiquetas y sí su empleo para envíos por correo.

Contratación de servicios

Los contratos de servicios informáticos más importantes son los siguientes:

- Consultoría informática.
- Auditoría informática.
- Formación.
- Seguridad informática.
- Contratación de personal informática.
- Instalación.
- Comunicaciones.
- Seguros.
- Responsabilidad civil.

Contratos complejos

Los contratos complejos son aquellos que contemplan los sistemas informáticos como un todo incorporando al objeto del mismo, tanto el *hardware* como el *software* y algunos servicios determinados. Los más usuales son los siguientes:

Contratación global o parcial de servicios informáticos (outsourcing)

Se trata de la subcontratación de todo o de parte del trabajo informático mediante un contrato con una empresa externa que se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes.

Contrato de respaldo (back-up)

Su finalidad es asegurar el mantenimiento de la actividad empresarial en el caso de que circunstancias previstas pero inevitables impidan que siga funcionando el sistema informático.

Contrato de llave en mano (turn-key-package)

En esta clase de contratos el proveedor se compromete a entregar el sistema creado donde el cliente le indique y asume la responsabilidad total de diseño, realización, pruebas, integración y adaptación al entorno informático del cliente tanto lógico como físico.

Contrato de suministro de energía informática

Como señala GETE-ALONSO y CALERA[9] es: *"aquel mediante el que una parte –el suministrador– poseedor de una unidad central que permanece en sus locales, pone a disposición del usuario la misma, lo que le permite el acceso a los 'software', a cambio de un precio"*.

[9] MARÍA DEL CARMEN GETE-ALONSO y CALERA. *La contratación en materia informática*. La Ley núm. 3005, Madrid, mayo 1992, pág. 10.

6.7. EL INTERCAMBIO ELECTRÓNICO DE DATOS

En la época en que vivimos todas las organizaciones, tanto privadas como públicas, deben mejorar su productividad examinando los diferentes factores que pueden influir en los resultados.

Entre estos factores se encuentran algunos de especial importancia como la reducción de costes, la agilización administrativa y la eliminación de errores. Esto se puede mejorar eliminando intermediarios entre el origen y el destino de los datos.

Como fruto de esta necesidad de comunicarse con rapidez y seguridad en el mundo actual nace el Intercambio Electrónico de Datos conocido internacionalmente por sus siglas en inglés EDI *(Electronic Data Interchange)* que es un sistema informático que permite las transacciones comerciales y administrativas directas a través del computador sin necesidad de realizar ningún trámite. Significa ahorro de tiempo y de papel.

Podemos definir el EDI como el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales o administrativas.

Un sistema de este tipo ha de cumplir tres requisitos básicos:

- El intercambio se ha de realizar por medios electrónicos.
- El formato tiene que estar formalizado.
- La conexión ha de ser de computador a computador.

En un sistema EDI son las aplicaciones informáticas de las empresas o de las Administraciones Públicas las que "dialogan" entre sí sin necesidad de intervención humana.

Significa, y esto es lo que nos interesa, el reemplazo del papel como elemento sustancial de la vinculación y comunicación negocial por un soporte informático.

Las razones que se pueden esgrimir para la implantación del EDI son:

- Precisión.
- Velocidad.
- Ahorro.
- Beneficios tangibles.
- Satisfacción del cliente.

El EDI es aplicable en el comercio, la industria, el transporte y las diferentes Administraciones Públicas.

La aceptación legal del EDI es un tema de suma importancia, sin duda detrás de la organización del mismo subyace un entendimiento entre las partes que intervienen que están dispuestas a aceptar una serie de obligaciones y de renunciar a ciertos derechos a efectos del buen funcionamiento del sistema.

Estos derechos y obligaciones se plasman en los correspondientes contratos: el contrato de intercambio de información y el contrato con las compañías de comunicaciones.

6.8. LA TRANSFERENCIA ELECTRÓNICA DE FONDOS

Una Transferencia Electrónica de Fondos (a partir de ahora TEF) puede significar muchas cosas. Si consideramos un concepto amplio de la misma puede abarcar todo tipo de envíos de fondos que se realicen por medios electrónicos.

Se puede definir como la transferencia de fondos que de forma automática es ejecutada inmediata y simultáneamente a la orden dada por el titular de la cuenta bancaria por medio de un sistema electrónico.

Podemos considerar que existen cuatro tipos principales de TEF que han ido apareciendo en el tiempo, conviven y son operativos en la actualidad:

- Transferencias entre entidades financieras.
- Transferencias entre otras organizaciones y las entidades financieras.
- El usuario colabora y, mediante las tarjetas de plástico y los cajeros automáticos, obtiene una serie de servicios bancarios.
- Se potencia el sistema con terminales en los puntos de venta y el banco en casa.

Por su gran trascendencia social nos referiremos a continuación al fenómeno de las tarjetas de plástico.

Las tarjetas de plástico o tarjetas como medio de pago, por ahora las denominaremos así, con su continuo y ascendente desarrollo, se están convirtiendo en un medio de pago cada vez más importante en el tráfico mercantil sustituyendo poco a poco al dinero papel y el cheque.

La Unión Europea siempre sensible a aquellos problemas que puedan tener alguna trascendencia de cara a la creación del mercado único y asimismo a la constitución de la Europa de los ciudadanos, ha dedicado una Comunicación, dos

Recomendaciones y una Directiva a los sistemas de pago electrónico, su normalización e interoperabilidad.

Aunque existen notas comunes entre los diversos tipos de tarjetas, la diferenciación entre ellas viene dada por su contenido contractual (derechos y obligaciones) con independencia de la denominación que les otorgue la entidad emisora.

Tarjetas propiamente de crédito

Son aquellas que, como su nombre indica, proporcionan un crédito al titular de la misma.

Tarjetas de débito

Emitidas por Entidades de Crédito, permiten a sus usuarios realizar compras en los establecimientos comerciales y a la vez ofrecen una gama de operaciones bancarias. En principio no están limitadas a un solo establecimiento comercial vinculando necesariamente la tarjeta a una cuenta corriente bancaria.

Estos dos tipos de tarjetas nos permiten utilizar los cajeros automáticos y los terminales puntos de venta.

El Código Europeo de Buena Conducta en materia de pago electrónico contenido en la Recomendación de 8 de diciembre de 1987 respecto a los contratos dice:

"a) *Los contratos celebrados entre los emisores o su representante y los prestadores o los consumidores revestirán la forma escrita y deberán ser objeto de una petición previa. Definirán con precisión las condiciones generales y específicas del acuerdo.*

b) *Se redactarán en la/s lengua/s oficiales del Estado miembro en que se haya celebrado.*

c) *Cualquier tarifación del baremo de cargas se fijará con transparencia teniendo en cuenta las cargas y riesgos reales y no supondrá ningún obstáculo a la libre competencia.*

d) *Todas las condiciones, siempre que sean conforme a la Ley, serán libremente negociables y se establecerán claramente en el contrato.*

e) Las condiciones específicas de rescisión del contrato se precisarán y comunicarán a las partes de la celebración del contrato."

En síntesis lo que se busca en esta Recomendación es transparencia, y que dadas las condiciones en que se establecen estos contratos, la parte más fuerte no salga beneficiada.

En el mundo empresarial la implantación de estas nuevas tecnologías por parte de las Entidades Financieras ha favorecido una evolución histórica en el concepto de lo que era la tesorería en las empresas, que ha pasado de ser una tesorería puramente administrativa a ser una tesorería de gestión que puede y debe generar beneficios por sí misma.

El conocimiento inmediato de posiciones y operaciones y la transferencia casi instantánea permite reducir provisiones y al mismo tiempo situar el dinero en el lugar donde más produzca.

6.9. LA CONTRATACIÓN ELECTRÓNICA

En una primera aproximación al tema por contratación electrónica o contratación por medios electrónicos se puede entender todo intercambio electrónico de datos o documentos cuyo objeto sea la contratación.

Sin embargo, en todos ellos no se pactan las cláusulas del contrato en el mismo momento del intercambio electrónico. Así vemos en los epígrafes anteriores que tanto el intercambio electrónico de datos (EDI) como la transferencia electrónica de fondos (TEF) son el resultado de un macrocontrato anterior realizado por el sistema tradicional en el que las partes han fijado los términos del mismo y en el que muchas veces lo que hacen es renunciar a una serie de posibles derechos.

En este epígrafe nos referiremos a otro tipo de contratación electrónica; aquella en la que el contrato se establece en el momento de la transacción electrónica sin que se haya pactado nada necesariamente con anterioridad.

M. SCHAUS[10] dice que en la formación del contrato estas nuevas tecnologías influyen desde tres ópticas diferentes:

– Desde el grado de inmediatez.

[10] M. SCHAUS. *Formación de contratos. Comunicación de la oferta y de la aceptación al oferente. La validez de los contratos internacionales negociados por medios electrónicos.* CECO, Madrid, 1988, págs. 21 y ss.

- Desde la calidad del diálogo.
- Desde la seguridad.

Desde el grado de inmediatez

En nuestro derecho existe disparidad de criterios entre el Código Civil y el de Comercio a la hora de determinar en qué momento se perfecciona el contrato.

El artículo 1262 del Código Civil dice: *"El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato. La aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta."*

Por su parte en el artículo 54 del Código de Comercio señala: *"Los contratos que se celebren por correspondencia quedarán perfeccionados cuando los contratantes hubieren aceptado su propuesta."*

Desde la calidad del diálogo

Entre los diferentes procedimientos existentes hoy día el que mayor se asemeja a un diálogo es la videoconferencia. En ella los interlocutores pueden apreciar no sólo el contenido del mensaje, sino también la entonación, gestos y silencios.

El teléfono ofrece idénticas posibilidades excepto que los interlocutores no pueden verse.

Desde la seguridad

Desde el punto de vista jurídico el concepto de seguridad se refiere a la autentificación de la identidad del usuario y a las huellas que deja la transacción y que pueden ser utilizadas como prueba.

Vemos que del grado del cumplimiento de estos tres aspectos, admitiendo que se dan en la contratación electrónica, depende en gran parte su inclusión como una nueva forma de contratación, con sus peculiaridades, pero dentro de una ortodoxia contractual.

A fin de comprobar si existe un acuerdo de voluntades entre las partes contratantes a los efectos del art. 1261 del Código Civil es importante clasificar los

diferentes tipos de contratación electrónica que se pueden presentar en función de cómo actúa la parte contratante emisora y la parte contratante receptora. Para simplificar consideraremos que ambas partes actúan de la misma forma, aunque no supondría ningún problema que esto no fuese así.

Sin desear ser exhaustivos consideramos que se pueden presentar los siguientes casos:

a) Comunicación entre dos computadores personales.
b) Comunicación entre varios computadores personales a través de un Centro de Compensación.
c) Comunicación entre dos sistemas informáticos.
d) Comunicación entre varios sistemas informáticos mediante un Centro de Compensación.
e) Comunicación entre dos Sistemas Expertos.

Los casos b) y d) simplemente los apuntamos para dejar constancia de su existencia.

En los casos a) y b) el computador se limita a transferir una información que contiene una expresión de voluntad contractual.

En principio, salvo que existan problemas de autentificación a los que nos referiremos más adelante, entendemos que esta voluntad transmitida forma parte de un negocio jurídico válido.

El problema se complica en los casos c) y d) cuando los que están en comunicación son dos sistemas informáticos (computadores) y lo que se transmite no se limita a ser sólo una información que incorpora una voluntad contractual, sino que ésta puede, venir alterada por una serie de aspectos que incorpora el propio sistema informático.

Problemas que se nos pueden presentar en la contratación electrónica son: identidad de los contratantes, extensión o no de este tipo de contratación a todos los contratos, ¿cuándo y dónde se concluye el contrato?, autentificación, factor tiempo y confidencialidad.

Los avances tecnológicos y la adaptación del Derecho a estas nuevas situaciones deben superar los obstáculos que la generalización de una forma de contratación presenta.

6.10. EL DOCUMENTO ELECTRÓNICO

Es corriente identificar documento con soporte papel y escritura, pero esto no siempre es así.

Para ROUANET MOSCARDÓ[11] un documento es: *"Un objeto normalmente escrito en el que, por tanto, se plasma algo mediante letras u otros signos trazados o impresos sobre el papel u otra superficie, pero que excepcionalmente puede no ser escrito; y es un objeto en el que puede representarse un hecho natural o un acuerdo de voluntades (hecho voluntario, arte o negocio) o ser el resultado de una actividad o de un procedimiento."*

PRIETO CASTRO define el documento como el objeto o materia en que consta por escrito una declaración de voluntad o de conocimiento o cualquier expresión del pensamiento, según resulta de los preceptos de la legislación positiva.

Los conceptos anteriores tienen en común que hablan de un escrito, aunque el primero admite la excepcionalidad de que no lo sea.

Escribir, según el *Diccionario de la Lengua Española*, es: *"Representar las palabras o las ideas con letras u otros signos trazados en papel u otra superficie."*

Por tanto, el documento no ha de ser siempre papel, sino que puede ser otro objeto o materia y la representación de las palabras o las ideas puede hacerse por otros signos distintos de las letras.

Dichos signos pueden ser la codificación binaria y la superficie distinta del papel puede ser un soporte informático.

De todo ello podemos deducir que el documento electrónico pertenece a la categoría de los documentos en sentido jurídico.

El problema para una aceptación generalizada de este tipo de documento puede estar en la necesidad de la seguridad de que la traducción del lenguaje a máquina a un lenguaje natural sea la correcta y no en la propia esencia del documento.

Coincidimos con DAVARA RODRÍGUEZ cuando dice que el problema de la firma que conlleva, en muchos casos, la autenticación del documento, puede ser, sin duda, el caballo de batalla para una total aceptación a efectos probatorios de este tipo de documentos.

---

[11] JAVIER ROUANET MOSCARDÓ. *Valor probatorio procesal del documento informático*. Congreso sobre Derecho Informático. Facultad de Derecho, Zaragoza, 1989, pág. 116.

Un documento escrito está compuesto de datos y de impresión en un soporte. La impresión comprende, la mayoría de las veces, la representación de un hecho y la firma.

La firma suele tener tres funciones: identificativa, declarativa y probatoria.

Esto significa que sirve para identificar quién es el autor del documento, declarar que el autor de la firma asume el contenido del mismo y permitir verificar si el autor de la firma es efectivamente aquel que ha sido identificado como tal en el caso de la propia firma.

Notas importantes de la firma son la habitualidad y ser autógrafa u ológrafa, puesta de puño y letra por el firmante.

Hasta el presente, éste ha sido uno de los principales sistemas de autentificación, aunque no es el único; pero en el futuro tendrá que ser sustituido en numerosas ocasiones. Los avances tecnológicos están obligando a que la firma manuscrita sea sustituida por otro sistema, en este caso electrónico.

Una firma digital o electrónica es una señal digital representada por una cadena de bits. Este tipo de firma ha de ser secreta, fácil de producir y de reconocer y difícil de falsificar.

En el caso de la firma manuscrita el fedatario público da fe de la autenticidad del documento. El empleo de la firma digital obliga a la aparición de una nueva figura: el fedatario electrónico. Éste ha de ser capaz de verificar la autenticidad de los documentos que circulan a través de las líneas de comunicaciones.

En cualquier caso los avances tecnológicos que se están produciendo quizás en un futuro cercano hagan aconsejable darle un carácter autónomo a este tipo de prueba con todos los problemas que esto pueda conllevar.

6.11. LECTURAS RECOMENDADAS

Davara Rodríguez, Miguel Ángel. *Derecho Informático.* Aranzadi. Pamplona, 1993.

Páez Mañá, Jorge. *Bases de Datos jurídicos.* Cindoc. CSIC. Madrid, 1994.

Peso Navarro, Emilio del y Ramos González, Miguel Ángel. *Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas.* Díaz de Santos. Madrid, 1994.

Peso Navarro, Emilio del; Ramos González, Miguel Ángel; Fernández Sánchez, Carlos Manuel e Ignoto Azaustre, María José. *Manual de Dictámenes y peritajes informáticos*. Díaz de Santos. Madrid, 1995.

Peso Navarro, Emilio del y Ramos González, Miguel Ángel. *LORTAD: Reglamento de Seguridad*. Díaz de Santos. Madrid, 1999.

Peso Navarro, Emilio del. *La Ley de Protección de Datos. La nueva LORTAD*. Díaz de Santos. Madrid, 2000.

6.12. CUESTIONES DE REPASO

1. ¿Cuál es la diferencia entre Informática Jurídica y Derecho Informático?
2. ¿Cuáles son los principios de la LOPD?
3. ¿Cuáles son los derechos patrimoniales en el derecho de autor?
4. ¿Qué es la multimedia?
5. ¿Qué es una estafa informática?
6. Realice una clasificación de los contratos informáticos.
7. ¿Qué es el EDI?
8. ¿Cuál es la diferencia entre una tarjeta de crédito y una de débito?
9. ¿Cuál es la diferencia entre contratación informática y contratación electrónica?
10. ¿Qué es un documento electrónico?

CAPÍTULO 7

DEONTOLOGÍA DEL AUDITOR INFORMÁTICO Y CÓDIGOS ÉTICOS

Jorge Páez Mañá

7.1. INTRODUCCIÓN

En el denominado "nuevo orden mundial", caracterizado por unas directrices económicas, en permanente cambio, estrechamente vinculadas a los continuos avances tecnológicos, tratar temas relacionados con la deontología, la ética o la moral, implica necesariamente hacer un alto en el camino, dejar al lado las múltiples y a menudo absurdas motivaciones económico-profesionales y, sin las premuras derivadas del ritmo de vida que aparentemente esta sociedad impone, reposadamente, con sosiego, adentrarse en el mundo interno subjetivo de la conciencia para observar la concepción humanística que, como personas, ésta pone de manifiesto como máximo exponente de la propia y auténtica identidad.

Una vez realizada dicha prospección interna se estará en condiciones de, dada la intrínseca naturaleza social del hombre, poder atisbar en el mundo externo, donde éste realiza su convivencia, observando los valores morales imperantes, representativos del grado de evolución social de la comunidad que los ha asumido como propios.

La primera observación debería inducir a reflexionar sobre los aspectos más íntimos ligados a la vida interior de cada cual (creencias, sentimientos, finalidad teleológica, proyecto de vida, etc.), que globalmente considerados han de poner de manifiesto la propia e intrínseca realidad individualizada, es decir, la genuina identidad personal.

Esta identidad, inherente a toda persona, debería estar sustentada en los **principios** morales socialmente acusados y preservados a lo largo de los tiempos, principios que, provenientes del espíritu y susceptibles, en virtud del libre albedrío, de servir o no de guía a la conducta exteriormente manifestada de los individuos, permiten diferenciar a éstos del resto de seres vivos, que carecen de esa libertad de conciencia.

Si bien la moral individual está enraizada en forma única y personalizada, la necesidad de relacionarse y convivir unos individuos con otros en comunidad exige una cierta adaptación de las diferentes concepciones morales individuales a unas determinadas normas éticas, socialmente asumidas por los miembros integrantes de la comunidad, que facilitan una convivencia pacífica y enriquecedora común.

Estas normas sociales, reflejo de la idiosincrasia de las diferentes comunidades, ponen de manifiesto los usos y costumbres que regulan mediáticamente las relaciones entre las personas y grupos que las conforman, considerándose, sin precisar su normalización positiva, implícitamente aceptadas por todos, y representativas de los principios sociales básicos reguladores de dichas relaciones (buena fe, cortesía, respeto, solidaridad, etc.).

Conviene, en este punto de la reflexión, resaltar el hecho de que los principios morales, en contraposición con los preceptos normativos materiales, deben ser asumidos individual y colectivamente como propios en forma voluntaria y con independencia de que se haya, o no, establecido expresamente la obligación material de cumplirlos, ayudando a configurar una concepción ética interna de lo que está bien y lo que está mal que constituye la parte fundamental del patrimonio espiritual de las personas y grupos integrantes de la sociedad que los aceptan como suyos.

Es precisamente esa característica de voluntariedad, de íntimo convencimiento de su idoneidad, generada por una previa sensibilización personal y colectiva sobre su validez para el cumplimiento de los fines teleológicos de los individuos y sociedades que los asumen, lo que configura a los principios morales como fuente primordial del derecho positivo y eje genuino y auténtico de la evolución social de la humanidad.

Junto a estas normas éticas inmateriales, coexisten otras positivas que regulan, en forma coactiva, los deberes y derechos de los ciudadanos integrados en cada colectividad. Estas normas positivas, elaboradas en virtud del "contrato social" que los ciudadanos implícitamente suscriben con sus gobernantes, se establecen como reguladores de aquellos aspectos que se considera deben estar clara y expresamente estipulados, a fin de determinar los principios legales que, de obligado cumplimiento, regulan los deberes y derechos que rigen en la sociedad y que, por ende, pueden ser imperativamente exigibles a cada uno de sus miembros.

La complejidad de las relaciones colectivas, la protección de los más débiles contra los abusos de los más fuertes y la necesidad de establecer unas normas de comportamiento precisas que, conocidas por todos, sirvan de cauce idóneo para la solución efectiva de los posibles conflictos personales que puedan generarse en el seno de la comunidad, ha fundamentado el establecimiento y legitimidad de dichos principios legales, si bien se exige de estos que estén imbuidos por los principios morales, colectivamente asumidos, y que respeten los derechos humanos internacionalmente reconocidos como conformadores del derecho mundial.

Ante esta dicotomía de normas morales y materiales, los códigos deontológicos representan un cierto punto de acercamiento y encuentro entre ambas.

Estos códigos toman, de las normas morales, su faceta intrínsecamente ética, y reflejan el sentir mayoritario de los profesionales a los que van dirigidos, de lo que se considera como un adecuado comportamiento ético-profesional, sirviendo de reprobación moral de aquellas conductas contrarias a lo regulado en los mismos.

Debe *tenerse en cuenta que todo código deontológico, entendido como conjunto* de preceptos que establecen los deberes exigibles a aquellos profesionales que ejerciten una determinada actividad, tiene como finalidad teleológico la de incidir en sus comportamientos profesionales estimulando que éstos se ajusten a determinados principios morales que deben servirles de guía.

El hecho de que los códigos deontológicos deban ser elaborados por los propios profesionales en el marco de los colegios, asociaciones o agrupaciones que los representen, y asumidos en forma generalizada como forma de autorregulación ética de su actividad, permite que éstos incidan en algunos aspectos –inaplicables al resto de ciudadanos, ya que fuera de su específico campo de aplicación serían ineficaces e inoperantes–, sobre los que, en beneficio de la propia comunidad, establecen unas determinadas pautas de conducta, a fin de evitar conculcar, por simple desconocimiento o apatía ético-intelectual, derechos de terceras personas.

Los principios contenidos en los códigos deontológicos exigen asimismo, por su especificidad moral, que los propios profesionales coadyuven a su difusión mostrando un comportamiento conforme a los mismos como medio de sensibilización y mejora del prestigio y calidad de su oficio.

A este respecto los auditores han de ser conscientes, dada su alta especialización en un campo habitualmente desconocido por amplios sectores sociales, de la obligación que moralmente deben asumir respecto a advertir a la sociedad sobre los riesgos y dependencias que la informática puede provocar y sobre las medidas que deben adoptarse para prevenirlos, debiendo servir los códigos deontológicos de

ejemplo y cauce idóneo para transmitir, al resto de la sociedad, sus singulares y específicas percepciones, inquietudes y autolimitaciones.

Debe tenerse muy presente que si bien los sistemas informáticos, sometidos a auditorías, son un mero instrumento al servicio de la política empresarial, el estudio de su estructura, y aún más el acceso a la información almacenada en su seno, permite a los auditores obtener una visión y conocimiento tanto de la situación global como de determinadas facetas de la empresa o sus empleados, en ciertos casos superior a las de los propios auditados, razón por la cual el sometimiento de los primeros a unos, en apariencia innecesariamente rígidos y detallados principios deontológicos propios de su oficio, resulta de obligada instauración en favor de los segundos, aun cuando estos últimos desconozcan tan siquiera la existencia de los mismos y se sorprendan de determinadas actitudes de los auditores acordes con ellos.

Los códigos deontológicos toman asimismo, de las normas materiales, las facetas reguladores de determinados comportamientos interpersonales como salvaguardia de derechos individuales y colectivos susceptibles de protección institucional, sirviendo de cauce para coartar, en los ámbitos profesionales correspondientes, aquellas conductas contrarias a lo regulado en sus preceptos mediante la imposición de sanciones, contempladas éstas desde una perspectiva disciplinaria meramente profesional.

Conviene en todo caso matizar el alcance coercitivo de las normas deontológicas.

Ya se ha indicado anteriormente que toda persona debe ceñir su conducta a sus propias normas morales internas, consustanciales a su identidad, y aceptar la imposición de unas normas coactivas externas, impuestas como medio de protección de la sociedad en la que se encuentra integrada.

Sin embargo, estas últimas normas no pueden regular, con total exhaustividad, el complejo mundo de relaciones interpersonales y aún menos profundizar en aspectos puntuales que sólo afectan a un reducido grupo de individuos o actividades, so pena de constituir un corpus jurídico conformado por un número tan elevado de preceptos que, por su gigantismo, resultaría del todo punto inasumible por la sociedad y, por ende, inútil e inaplicable.

Los códigos deontológicos, por el contrario, al restringir su ámbito subjetivo a determinados grupos de personas, los profesionales de áreas concretas, y acotar su ámbito temático a sus específicos campos de actividad, permiten, sin causar perjuicio ni discriminación al resto de integrantes de la comunidad, establecer, para el ejercicio de determinadas actividades, unos mínimos estándares de comportamiento ético y técnico configuradores, a tenor del estado de la ciencia, de la moral colectiva del grupo al que van dirigidos.

Hay que tener presente que, mediante el ejercicio profesional, se pone de manifiesto una de las facetas de la personalidad que más incide en la valoración social de la actividad desarrollada por las personas a través de la realización de su trabajo.

Ciertamente existe un numeroso conjunto de preceptos incluidos en normas materiales provenientes del Derecho Constitucional, Civil, Laboral, Mercantil, etc., que regulan una gran variedad de actos relacionados con la actividad profesional, pero más allá de dichos preceptos, y como fundamento de los mismos, debe existir una "moral profesional" que sirva de guía para determinar cuándo un determinado comportamiento profesional es bueno o malo (moralmente admisible y beneficioso o moralmente inadmisible y perjudicial).

La coercibilidad de los códigos deontológicos debe, por tanto, constreñirse a la imposición de medidas disciplinarias, correctoras de comportamientos contrarios a lo estipulado en los mismos, que pongan de manifiesto el rechazo, por el colectivo profesional correspondiente, de aquellas conductas profesionales indignas.

Estas medidas suelen estar constituidas por apercibimientos, reprensiones públicas o privadas y, en los casos de grave o reiterado incumplimiento, exclusiones temporales o definitivas del infractor, del grupo profesional que las ha asumido como propias.

Con esta perspectiva se hace preciso, en el momento actual, ir planteando, de forma crítica, la necesidad de sensibilizar a los auditores informáticos, integrados en un sector profesional dotado de una cierta autonomía y con unas características muy particulares, de la conveniencia de reflexionar sobre la dualidad de facetas integradoras de su comportamiento profesional (comportamiento técnico cualificado y comportamiento ético) a fin de eliminar el error de creer que su actividad debe valorarse únicamente en función de unos mínimos estándares técnicos de calidad y fiabilidad obviando los condicionantes éticos que, en caso de conflicto con condicionantes técnicos o de cualquier otra índole (científicos, económicos, promocionales, empresariales, etc.), deben ser considerados como prevalentes.

Antes de entrar en una aproximación de los diferentes principios deontológicos que normalmente se asocian a la actividad de los auditores, no está de más recalcar que en tanto en cuanto éstos no estén plenamente asumidos, como configuradores de la dimensión ética de su profesión, sería preferible apelar a los comportamientos morales individuales, como medio de ir incidiendo en la sedimentación de concepciones humanísticas en el entorno profesional en que se desenvuelven, a pretender imponer unilateralmente, a través de agrupaciones, sociedades o colegios profesionales, dichos principios.

7.2. PRINCIPIOS DEONTOLÓGICOS APLICABLES A LOS AUDITORES INFORMÁTICOS

Los principios deontológicos aplicables a los auditores deben necesariamente estar en consonancia con los del resto de profesionales y especialmente con los de aquellos cuya actividad presente mayores concomitancias con la de la auditoría, razón por la cual, en equivalencia con los principios deontológicos adoptados por diferentes colegios y asociaciones profesionales de nuestro entorno socio-cultural, y sin ánimo de exhaustividad, se pueden indicar como básicos, en un orden meramente alfabético y ajeno, por tanto, a cualquier ponderación de importancia, los siguientes:

7.2.1. Principio de beneficio del auditado

El auditor deberá ver cómo se puede conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada, estando obligado a presentar recomendaciones acerca del reforzamiento del sistema y el estudio de las soluciones más idóneas según los problemas detectados en el sistema informático de esta última, siempre y cuando las soluciones que se adopten no violen la ley ni los principios éticos de las normas deontológicas.

En ningún caso está justificado que realice su trabajo el prisma del propio beneficio, sino que por el contrario su actividad debe estar en todo momento orientada a lograr el máximo provecho de su cliente.

Cualquier actitud que anteponga intereses personales del auditor a los del auditado deberá considerarse como no ética, ya que limitará necesariamente la aptitud del primero para prestar al segundo toda la ayuda que, a tenor de su capacitación, puede y debe aportarle.

Para garantizar tanto el beneficio del auditado como la necesaria independencia del auditor, este último deberá evitar estar ligado en cualquier forma, a intereses de determinadas marcas, productos o equipos compatibles con los de su cliente, debiendo eludir hacer comparaciones, entre el sistema o equipos del auditado con los de otros fabricantes, cuando las mismas sólo se realicen con la intención de influir en las decisiones de su cliente y provocar un cambio hacia esos otros sistemas o productos bien por intereses económicos particulares del auditor o bien por el mayor conocimiento que tenga de ellos o desee tener.

La adaptación del auditor al sistema del auditado debe implicar una cierta simbiosis con el mismo, a fin de adquirir un conocimiento pormenorizado de sus características intrínsecas.

A partir de la adquisición de dicho conocimiento, y con el grado de independencia indicado anteriormente, estará en condiciones de indicar, si lo considerase pertinente en forma globalizada o en forma particularizada, las ventajas y desventajas que el sistema ofrece respecto a otros sistemas o marcas, debiendo obtener de dicha comparación una serie de conclusiones que permitan mejorar la calidad y prestaciones del sistema auditado.

Únicamente en los casos en que el auditor dedujese la imposibilidad de que el sistema pudiera acomodarse a las exigencias propias de su cometido o considerase excesivamente onerosos los cambios a introducir para obtener una suficiente fiabilidad a corto y medio plazo, éste podría proponer un cambio cualitativamente significativo de determinados elementos o del propio sistema informático globalmente contemplado.

Una vez estudiado el sistema informático a auditar, el auditor deberá establecer los requisitos mínimos, aconsejables y óptimos para su adecuación a la finalidad para la que ha sido diseñado, determinando en cada caso su adaptabilidad, fiabilidad, limitaciones, posibles mejoras y costes de las mismas, con objeto de presentar al auditado una serie de opciones de actuación en función de dichos parámetros a fin de que éste pueda valorar las relaciones coste-eficacia-calidad-adaptabilidad de las diferentes opciones, facilitándole un abanico de posibilidades de establecer una política a corto, medio y largo plazo acorde con sus recursos y necesidades reales.

El auditor deberá lógicamente abstenerse de recomendar actuaciones innecesariamente onerosas, dañinas o que generen riesgos injustificados para el auditado, e igualmente de proponer modificaciones carentes de base científica contrastada, insuficientemente probadas, o de imprevisible futuro.

Una de las cuestiones más controvertidas, respecto de la aplicación de este principio, es la referente a facilitar el derecho de las organizaciones auditadas a la libre elección del auditor, lo que implica el deber moral de evitar generar dependencias de los primeros respecto de los segundos, aunque dicho condicionante perjudique determinadas expectativas económicas de estos últimos.

Igualmente, si el auditado decidiera encomendar posteriores auditorías a otros profesionales, éstos deberían poder tener acceso a los informes de los trabajos anteriormente realizados sobre el sistema del auditado siempre y cuando con ello no se vulnerasen derechos de terceros protegidos con el secreto profesional que el auditor debe en todo momento guardar.

7.2.2. Principio de calidad

El auditor deberá prestar sus servicios a tenor de las posibilidades de la ciencia y medios a su alcance con absoluta libertad respecto a la utilización de dichos medios y en unas condiciones técnicas adecuadas para el idóneo cumplimiento de su labor.

En los casos en que la precariedad de medios puestos a su disposición impidan o dificulten seriamente la realización de la auditoría, deberá negarse a realizarla hasta que se le garantice un mínimo de condiciones técnicas que no comprometan la calidad de sus servicios o dictámenes.

Cuando durante la ejecución de la auditoría, el auditor considerase conveniente recabar el informe de otros técnicos más cualificados sobre algún aspecto o incidencia que superase su capacitación profesional para analizarlo en idóneas condiciones, deberá remitir el mismo a un especialista en la materia o recabar su dictamen para reforzar la calidad y fiabilidad global de la auditoría.

7.2.3. Principio de capacidad

El auditor debe estar plenamente capacitado para la realización de la auditoría encomendada, máxime teniendo en cuenta que, en la mayoría de los casos, dada su especialización, a los auditados en algunos casos les puede ser extremadamente difícil verificar sus recomendaciones y evaluar correctamente la precisión de las mismas.

Hay que tener muy presente que el auditor, al igual que otros determinados profesionales (médicos, abogados, educadores, etc.), puede incidir en la toma de decisiones de la mayoría de sus clientes con un elevado grado de autonomía, dada la dificultad práctica de los mismos de contrastar su capacidad profesional y el desequilibrio de conocimientos técnicos existentes entre el auditor y los auditados.

Debe, por tanto, ser plenamente consciente del alcance de sus conocimientos y de su capacidad y aptitud para desarrollar la auditoría evitando que una sobreestimación personal pudiera provocar el incumplimiento parcial o total de la misma, aun en los casos en que dicho incumplimiento no pueda ser detectado por las personas que le contraten dadas sus carencias cognitivas técnicas al respecto.

Conviene indicar que en los casos de producirse, por el contrario, una subestimación de su capacidad profesional, esta circunstancia podría afectar negativamente en la confianza del auditado sobre el resultado final de la auditoría, dejándole una innecesaria impresión de inseguridad sobre las propuestas o decisiones a adoptar.

A efectos de garantizar, en la medida de lo posible, la pertinencia de sus conocimientos, el auditor deberá procurar que éstos evolucionen, al unísono con el desarrollo de las tecnologías de la información, en una forma dinámica, evitando una perniciosa estaticidad técnico-intelectual que, en este campo de la ciencia, origina una drástica reducción de las garantías de seguridad y una obsolescencia de métodos y técnicas que pueden inhabilitarle para el ejercicio de su profesión.

Conviene por último llamar la atención sobre la casuística de la acreditación de la capacitación de los auditores con la pregunta clásica, adaptada a las circunstancias de esta profesión, de ¿quién audita a los auditores?

Es deseable que se fortalezca la certificación profesional de la aptitud de los auditores para realizar unos trabajos de índole tan compleja.

Esta certificación que deberá tener un plazo de validez acorde con la evolución de las nuevas tecnologías de la información, debería estar avalada y garantizada por la metodología empleada para acreditar dicha especialización, la independencia de las entidades certificadoras, y la solvencia profesional, objetivamente contrastada, de los órganos, necesariamente colegiados, que en las mismas se creen con la finalidad de apreciar la formación y cualificación profesional de los solicitantes de la misma.

7.2.4. Principio de cautela

El auditor debe en todo momento ser consciente de que sus recomendaciones deben estar basadas en la experiencia contrastada que se le supone tiene adquirida, evitando que, por un exceso de vanidad, el auditado se embarque en proyectos de futuro fundamentados en simples intuiciones sobre la posible evolución de las nuevas tecnologías de la información.

Si bien es cierto que el auditor debe estar al corriente del desarrollo de dichas tecnologías de la información e informar al auditado de su previsible evolución, no es menos cierto que debe evitar la tentación de creer que, gracias a sus conocimientos, puede aventurar, con un casi absoluto grado de certeza, los futuros avances tecnológicos y transmitir, como medio de demostrar su cualificada especialización, dichas previsiones como hechos incontestables incitando al auditado a iniciar ilusorios e insuficientemente garantizados proyectos de futuro.

Debe, por tanto, el auditor actuar con un cierto grado de humildad, evitando dar la impresión de estar al corriente de una información privilegiada sobre el estado real de la evolución de los proyectos sobre nuevas tecnologías y ponderar las dudas que le surjan en el transcurso de la auditoría a fin de poner de manifiesto las diferentes

posibles líneas de actuación en función de previsiones reales y porcentajes de riesgo calculados de las mismas, debidamente fundamentadas.

7.2.5. Principio de comportamiento profesional

El auditor, tanto en sus relaciones con el auditado como con terceras personas, deberá, en todo momento, actuar conforme a las normas, implícitas o explícitas, de dignidad de la profesión y de corrección en el trato personal.

Para ello deberá cuidar la moderación en la exposición de sus juicios u opiniones evitando caer en exageraciones o atemorizaciones innecesarias procurando, en todo momento, transmitir una imagen de precisión y exactitud en sus comentarios que avalen su comportamiento profesional e infundan una mayor seguridad y confianza a sus clientes.

El comportamiento profesional exige del auditor una seguridad en sus conocimientos técnicos y una clara percepción de sus carencias, debiendo eludir las injerencias no solicitadas por él, de profesionales de otras áreas, en temas relacionados o que puedan incidir en el resultado de la auditoría y, cuando precisase del asesoramiento de otros expertos, acudir a ellos, dejando en dicho supuesto constancia de esa circunstancia y reflejando en forma diferenciada, en sus informes y dictámenes, las opiniones y conclusiones propias y las emitidas por los mismos.

El auditor debe asimismo guardar un escrupuloso respeto por la política empresarial del auditado, aunque ésta difiera ostensiblemente de las del resto del sector en las que desarrolla su actividad, evitar comentarios extemporáneos sobre la misma en tanto no estén relacionados o afecten al objeto de la auditoría y analizar pormenorizadamente las innovaciones concretas puestas en marcha por el auditado a fin de determinar sus específicas ventajas y riesgos, eludiendo evaluarlas únicamente a tenor de los estándares medios del resto de empresas de su sector.

Igualmente debe evitar realizar actos que simulen aplicaciones de tratamientos ficticios, encubran comportamientos no profesionales o den publicidad a metodologías propias o ajenas insuficientemente contrastadas y garantizadas.

7.2.6. Principio de concentración en el trabajo

En su línea de actuación, el auditor deberá evitar que un exceso de trabajo supere sus posibilidades de concentración y precisión en cada una de las tareas a él encomendadas, ya que la saturación y dispersión de trabajos suele a menudo, si no está

debidamente controlada, provocar la conclusión de los mismos sin las debidas garantías de seguridad.

A este efecto, el auditor deberá sopesar las posibles consecuencias de una acumulación excesiva de trabajos a fin de no asumir aquellos que objetivamente no tenga tiempo de realizar con las debidas garantías de calidad, debiendo rechazar o posponer los que en dichas circunstancias se le ofrezcan.

Asimismo deberá evitar la desaconsejable práctica de ahorro de esfuerzos basada en la reproducción de partes significativas de trabajos o conclusiones obtenidas de trabajos previos en otros posteriores elaborados como colofón de nuevas auditorías.

Por el contrario, sí es admisible el que, una vez analizados en profundidad los aspectos a tener en cuenta y obtenidas las correspondientes conclusiones, se contrasten las mismas a tenor de la experiencia adquirida y reflejada en anteriores informes, ya que este modo de actuar permite detectar posibles omisiones en el estudio, completar los trabajos sobre el objeto de la auditoría incompletamente ejecutados y cubrir las imprevisiones detectadas por medio de esta comparación.

Este comportamiento profesional permitirá al auditor dedicar a su cliente la mayor parte de los recursos posibles obtenidos de sus conocimientos y experiencias previas con una completa atención durante la ejecución de la auditoría sin injerencias o desatenciones originadas por prestaciones ajenas a la misma.

7.2.7. Principio de confianza

El auditor deberá facilitar e incrementar la confianza del auditado en base a una actuación de transparencia en su actividad profesional sin alardes científico-técnicos que, por su incomprensión, puedan restar credibilidad a los resultados obtenidos y a las directrices aconsejadas de actuación.

Este principio requiere asimismo, por parte del auditor, el mantener una confianza en las indicaciones del auditado aceptándolas sin reservas como válidas, a no ser que observe datos que las contradigan y previa confirmación personal de la inequívoca veracidad de los mismos.

Para fortalecer esa confianza mutua se requiere por ambas partes una disposición de diálogo sin ambigüedades que permita aclarar las dudas que, a lo largo de la auditoría, pudieran surgir sobre cualesquiera aspectos que pudieran resultar conflictivos, todo ello con la garantía del secreto profesional que debe regir en su relación.

El auditor deberá, en consonancia con esta forma de actuar, adecuar su lenguaje al nivel de comprensión del auditado, descendiendo y detallando cuanto haga falta en su explicación debiendo solicitar, cuando lo considere necesario, la presencia de alguno de los colaboradores de confianza de su cliente que pudiera apreciar determinados aspectos técnicos cuando precise informarle sobre cuestiones de una especial complejidad científica.

7.2.8. Principio de criterio propio

El auditor durante la ejecución de la auditoría deberá actuar con criterio propio y no permitir que éste esté subordinado al de otros profesionales, aun de reconocido prestigio, que no coincidan con el mismo.

En los casos en que aprecie divergencias de criterio con dichos profesionales sobre aspectos puntuales de su trabajo, deberá reflejar dichas divergencias dejando plenamente de manifiesto su propio criterio e indicando, cuando aquél esté sustentado en metodologías o experiencias que difieran de las corrientes profesionales mayoritariamente asumidas, dicha circunstancia.

La defensa a ultranza del propio criterio no es óbice para respetar las críticas adversas de terceros, aunque el auditor debe evitar que, si una vez analizadas continúa discrepando de las mismas, éstas puedan seguir influyendo en su trabajo, ya que la libertad de criterio impone al auditor la obligación ética de actuar en todo momento en la forma que él considere personalmente más beneficiosa para el auditado, aun cuando terceras personas le inciten a desarrollar líneas diferentes de actuación.

Este principio exige asimismo del auditor una actitud cuasibeligerante en los casos en que llegue al convencimiento de que la actividad que se le solicita, presuntamente para evaluar y mejorar un sistema informático, tiene otra finalidad ajena a la auditoría, en cuyo caso deberá negarse a prestar su asistencia poniendo de manifiesto el porqué de dicha negativa.

De igual forma cuando el auditor observe que, de forma reiterada, el auditado se niega, sin justificación alguna, a adoptar sus propuestas, deberá plantearse la continuidad de sus servicios en función de las razones y causas que considere puedan justificar dicho proceder.

7.2.9. Principio de discreción

El auditor deberá en todo momento mantener una cierta discreción en la divulgación de datos, aparentemente inocuos, que se le hayan puesto de manifiesto durante la ejecución de la auditoría.

Este cuidado deberá extremarse cuando la divulgación de dichos datos pudiera afectar a derechos relacionados con la intimidad o profesionalidad de las personas concernidas por los mismos o a intereses empresariales, y mantenerse tanto durante la realización de la auditoría como tras su finalización.

7.2.10. Principio de economía

El auditor deberá proteger, en la medida de sus conocimientos, los derechos económicos del auditado evitando generar gastos innecesarios en el ejercicio de su actividad.

En cumplimiento de este principio deberá procurar evitar dilaciones innecesarias en la realización de la auditoría. Esta economía de tiempos permitirá al auditado reducir los plazos de actuación tendentes a solventar los problemas detectados o a la adecuación a los nuevos métodos propuestos aportando un determinado valor añadido al trabajo del auditor.

De igual forma, el auditor deberá tener en cuenta la economía de medios materiales o humanos, eludiendo utilizar aquellos que no se precisen, lo que redundará en reducciones de gastos no justificados.

Conviene, en virtud de este principio, delimitar en la forma más concreta posible *ab initio* el alcance y límites de la auditoría a efectos de evitar tener que realizar estudios sobre aspectos colaterales no significativos, que detraen tiempo y medios para su análisis, y emitir informes sobre temas circunstanciales o ajenos a la finalidad perseguida.

El auditor deberá rechazar las ampliaciones del trabajo en marcha, aun a petición del auditado, sobre asuntos no directamente relacionados con la auditoría, dejando que de ellos se encarguen los profesionales *ad hoc*, y evitará entrar en discusiones, comentarios, visitas de cortesías, etc. que no estén justificadas con la ejecución de la misma.

En las recomendaciones y conclusiones realizadas en base a su trabajo deberá asimismo eludir, incitar o proponer actuaciones que puedan generar gastos innecesarios o desproporcionados.

7.2.11. Principio de formación continuada

Este principio, íntimamente ligado al principio de capacidad y vinculado a la continua evolución de las tecnologías de la información y las metodologías relacionadas con las mismas, impone a los auditores el deber y la responsabilidad de

mantener una permanente actualización de sus conocimientos y métodos a fin de adecuarlos a las necesidades de la demanda y a las exigencias de la competencia de la oferta.

La progresiva especialización de sus clientes exige asimismo de los auditores, para poder mantener el grado de confianza que se precisa para dejar en sus manos el análisis de las prestaciones de los sistemas informáticos, un continuo plan de formación personal que implique un seguimiento del desarrollo y oportunidades de las nuevas tecnologías de la información para poder incorporar dichas innovaciones, una vez consolidadas, a los sistemas de sus clientes, evitando de esta forma su obsolescencia.

7.2.12. Principio de fortalecimiento y respeto de la profesión

La defensa de los auditados pasa por el fortalecimiento de la profesión de los auditores informáticos, lo que exige un respeto por el ejercicio, globalmente considerado, de la actividad desarrollada por los mismos y un comportamiento acorde con los requisitos exigibles para el idóneo cumplimiento de la finalidad de las auditorías.

En consonancia con el principio de defensa de la profesión de los auditores, éstos deberán cuidar del reconocimiento del valor de su trabajo y de la correcta valoración de la importancia de los resultados obtenidos con el mismo.

En cuanto a la remuneración por su actividad profesional ésta debería estar acorde con la preparación del auditor y con el valor añadido que aporta al auditado con su trabajo, siendo rechazable el establecimiento de acuerdos que impliquen remuneraciones al auditor manifiestamente desproporcionadas tanto por insuficientes como por abusivas, ya que a largo plazo, tanto las unas como las otras redundan en un debilitamiento del reconocimiento y aprecio de la profesión.

El auditor deberá, por tanto, en prestigio de su profesión, evitar competir deslealmente con sus compañeros rebajando sus precios a límites impropios del trabajo a realizar con la finalidad de eliminar competidores y reducir la competencia profesional, e igualmente evitar abusar de su especialización para imponer una remuneración como contrapartida a su actividad profesional que manifiestamente exceda del valor objetivo de su trabajo.

Como integrante de un grupo profesional, deberá promover el respeto mutuo y la no confrontación entre compañeros. Este respeto no está reñido, sin embargo, con la denuncia de comportamientos indebidos, parasitarios o dolosos en los casos en que éstos le hayan quedado patentes, ya que estas denuncias deben contemplarse en el marco de la defensa de la propia profesión como forma de elevar su reconocimiento.

En sus relaciones profesionales deberá exigir asimismo una reciprocidad en el comportamiento ético de sus colegas y facilitar las relaciones de confraternidad y mutuo apoyo cuando así se lo soliciten. Este mutuo apoyo no debe entenderse en ningún caso como contraprestación gratuita de asesoramiento, sino como cauce de colaboración en temas puntuales que precisen de una cierta especialización o contrastación de opiniones.

7.2.13. Principio de independencia

Este principio, muy relacionado con el principio de criterio propio, obliga al auditor, tanto si actúa como profesional externo o con dependencia laboral respecto a la empresa en la que deba realizar la auditoría informática, a exigir una total autonomía e independencia en su trabajo, condición ésta imprescindible para permitirle actuar libremente según su leal saber y entender.

La independencia del auditor constituye, en su esencia, la garantía de que los intereses del auditado serán asumidos con objetividad; en consecuencia el correcto ejercicio profesional de los auditores es antagónico con la realización de su actividad bajo cualesquiera condiciones que no permitan garantizarla.

Esta independencia implica asimismo el rechazo de criterios con los que no esté plenamente de acuerdo, debiendo reflejar en su informe final tan sólo aquellos que considere pertinentes, evitando incluir en el mismo aquellos otros con los que disienta aunque sea impelido a ello.

El auditor igualmente deberá preservar su derecho y obligación de decir y poner de manifiesto todo aquello que según su ciencia y conciencia considere necesario, y abstenerse de adoptar métodos o recomendar líneas de actuación que, según su entender, pudieran producir perjuicios al auditado, aunque éste así se lo solicite.

A efectos de salvaguardar su independencia funcional, deberá eludir establecer dependencias con firmas que la limiten a fin de evitar que, aun subjetivamente, pueda producirse una reducción de su libertad de actuación profesional.

Conviene, sin embargo, diferenciar esta independencia en su trabajo de la exigencia de utilizar el resultado del mismo, lo que obviamente entra en el campo competencial de la potestad de actuación del auditado, el cual puede seguir o ignorar, por las razones que estime convenientes, sus informes, recomendaciones, orientaciones o consejos sin que ello suponga merma alguna en la independencia del auditor.

7.2.14. Principio de información suficiente

Este principio de primordial interés para el auditado, obliga al auditor a ser plenamente consciente de su obligación de aportar, en forma pormenorizadamente clara, precisa e inteligible para el auditado, información tanto sobre todos y cada uno de los puntos relacionados con la auditoría que puedan tener algún interés para él, como sobre las conclusiones a las que ha llegado, e igualmente informarle sobre la actividad desarrollada durante la misma que ha servido de base para llegar a dichas conclusiones.

Dicha información deberá estar constituida por aquella que el auditor considere conveniente o beneficiosa para los intereses o seguridad de su cliente y estar en consonancia con la utilidad que pueda tener, en el presente o en el futuro, para el mismo. Junto a dicha información deberá asimismo facilitar cualquier otra que le sea requerida por el auditado, aunque la considere intranscendente o poco significativa, siempre y cuando ésta tenga una relación directa y no meramente circunstancial con el objeto de la auditoría y no afecte a datos nominativos cuyo deber de secreto le sea exigible.

En dichas informaciones deberá evitar aportar datos intrascendentes para su cliente (datos que sólo afecten a su propia imagen comercial o profesional del auditor –autopropaganda–, datos comerciales no pertinentes, etc.), que sólo persigan incrementar el volumen del informe o justificar la ausencia de determinadas precisiones de singular importancia mediante la aportación de otras de menor interés y de más fácil elaboración para el auditor.

El auditor deberá asimismo comprometerse con sus conclusiones, debiendo indicar en ellas los defectos observados en el sistema informático, las líneas de actuación que recomienda y las dudas que respecto a las mismas se le plantean, indicando en este último caso si la causa excepcional que las produce se deriva de una insuficiencia de datos sobre el propio sistema, de una falta de conocimientos técnicos del propio auditor que le impide decidirse, con una mínima garantía de fiabilidad, sobre la conveniencia de inclinarse preferentemente por alguna de ellas, o de una incertidumbre sobre posibles evoluciones a medio o largo plazo de los avances tecnológicos.

Ciertamente el auditor debe ser consciente de que la explicitación de sus dudas afectará a la confianza del auditado, pero en cualquier caso es preferible transmitir una información veraz, entendida ésta como la que es exigible a todo buen profesional en el ejercicio de su actividad a tenor de sus conocimientos, que trasmitir, como opinión experta, una información de la que no pueda garantizar personalmente su exactitud.

Es importante asimismo que la información trasmitida al auditado ponga de manifiesto una prudencia y sentido de la responsabilidad, características estas que nunca deben estar reñidas con los principios de suficiencia informativa y de veracidad, evitando recrear los aspectos negativos o los errores humanos detectados que deben quedar reflejados con un cierto tacto profesional.

El auditor debe evitar hacer recaer la totalidad de inadaptaciones del sistema sobre algunos elementos singulares (personales o materiales), ignorando aquellos otros que pudieran tener incidencia en los fallos o anomalías detectadas, por simple comodidad en la elaboración de sus informes, y huir del secretismo en cuanto a la explicitación de los métodos utilizados siendo inadmisible que se aproveche para ello de la buena fe del auditado.

La labor informativa del auditor deberá, por tanto, estar basada en la suficiencia, autonomía y máximo aprovechamiento de la misma por parte de su cliente, debiendo indicar junto a sus juicios de valor, la metodología que le ha llevado a establecerlos para, de esta forma, facilitar el que, en futuras auditorías, puedan aprovecharse los conocimientos extraídos de la así realizada, eludiendo monopolios fácticos y dependencias generadas por oscurantismo en la trasmisión de la información.

7.2.15. Principio de integridad moral

Este principio, inherentemente ligado a la dignidad de persona, obliga al auditor a ser honesto, leal y diligente en el desempeño de su misión, a ajustarse a las normas morales, de justicia y probidad, y a evitar participar, voluntaria o inconscientemente, en cualesquiera actos de corrupción personal o de terceras personas.

El auditor no deberá, bajo ninguna circunstancia, aprovechar los conocimientos adquiridos durante la auditoría para utilizarlos en contra del auditado o de terceras personas relacionadas con el mismo.

Durante la realización de la auditoría, el auditor deberá emplear la máxima diligencia, dedicación y precisión, utilizando para ello todo su saber y entender.

7.2.16. Principio de legalidad

En todo momento el auditor deberá evitar utilizar sus conocimientos para facilitar, a los auditados o a terceras personas, la contravención de la legalidad vigente.

En ningún caso consentirá ni colaborará en la desactivación o eliminación de dispositivos de seguridad ni intentará obtener los códigos o claves de acceso a sectores restringidos de información generados para proteger los derechos, obligaciones o intereses de terceros (derecho a la intimidad, secreto profesional, propiedad intelectual, etc.).

De igual forma los auditores deberán abstenerse de intervenir líneas de comunicación o controlar actividades que puedan generar vulneración de derechos personales o empresariales dignos de protección.

La primacía de esta obligación exige del auditor un comportamiento activo de oposición a todo intento, por parte del auditado o de terceras personas, tendente a infringir cualquier precepto integrado en el derecho positivo.

7.2.17. Principio de libre competencia

La actual economía de mercado exige que el ejercicio de la profesión se realice en el marco de la libre competencia, siendo rechazables, por tanto, las prácticas colusorias tendentes a impedir o limitar la legítima competencia de otros profesionales y las prácticas abusivas consistentes en el aprovechamiento en beneficio propio, y en contra de los intereses de los auditados, de posiciones predominantes.

En la comercialización de los servicios de auditoría informática deben evitarse tanto los comportamientos parasitarios como los meramente desleales, entendidos los primeros como aprovechamientos indebidos del trabajo y reputación de otros en beneficio propio, y los segundos como intentos de confundir a los demandantes de dichos servicios mediante ambigüedades, insinuaciones o puntualizaciones que sólo tengan por objetivo enmascarar la calidad y fiabilidad de la oferta.

7.2.18. Principio de no discriminación

El auditor en su actuación previa, durante y posterior a la auditoría, deberá evitar inducir, participar o aceptar situaciones discriminatorias de ningún tipo, debiendo ejercer su actividad profesional sin prejuicios de ninguna clase y con independencia de las características personales, sociales o económicas de sus clientes.

Deberá evitar cualquier tipo de condicionantes personalizados y actuar en todos los casos con similar diligencia con independencia de los beneficios obtenidos del auditado, de las simpatías personales que tenga hacia éste o de cualquier otra circunstancia.

Su actuación deberá asimismo mantener una igualdad de trato profesional con la totalidad de personas con las que en virtud de su trabajo tenga que relacionarse con independencia de categoría, estatus empresarial o profesional, etc.

7.2.19. Principio de no injerencia

El auditor, dada la incidencia que puede derivarse de su tarea, deberá evitar injerencias en los trabajos de otros profesionales, respetar su labor y eludir hacer comentarios que pudieran interpretarse como despreciativos de la misma o provocar un cierto desprestigio de su cualificación profesional, a no ser que, por necesidades de la auditoría, tuviera que explicitar determinadas inidoneidades que pudieran afectar a las conclusiones o el resultado de su dictamen.

Deberá igualmente evitar aprovechar los datos obtenidos de la auditoría para entrar en competencia desleal con profesionales relacionados con ella de otras áreas del conocimiento. Esa injerencia es mayormente reprobable en los casos en los que se incida en aquellos campos de actividad para los que el auditor no se encuentre plenamente capacitado.

7.2.20. Principio de precisión

Este principio estrechamente relacionado con el principio de calidad exige del auditor la no conclusión de su trabajo hasta estar convencido, en la medida de lo posible, de la viabilidad de sus propuestas, debiendo ampliar el estudio del sistema informático cuanto considere necesario, sin agobios de plazos (con la excepción de lo ya indicado anteriormente respecto al principio de economía) siempre que se cuente con la aquiescencia del auditado, hasta obtener dicho convencimiento.

En la exposición de sus conclusiones deberá ser suficientemente crítico, no eludiendo poner de manifiesto aquellos aspectos concretos que considere puedan tener una cierta incidencia en la calidad y fiabilidad de la auditoría, ni quedándose en generalidades o indefiniciones que por su amplitud o ambigüedad sólo pretendan cubrir al auditor de los riesgos derivados de toda concreción en detrimento de los derechos e intereses del auditado.

Es exigible asimismo del auditor que indique como evaluado únicamente aquello que directamente, o por medio de sus colaboradores, haya comprobado u observado de forma exhaustiva, eludiendo indicar como propias y contrastadas las observaciones parciales o incompletas o las recabadas de terceras personas.

7.2.21. Principio de publicidad adecuada

La oferta y promoción de los servicios de auditoría deberán en todo momento ajustarse a las características, condiciones y finalidad perseguidas, siendo contraria a

la ética profesional la difusión de publicidad falsa o engañosa que tenga como objetivo confundir a los potenciales usuarios de dichos servicios.

La defensa del prestigio de la profesión obliga asimismo a los auditores informáticos a evitar las campañas publicitarias que, por su contenido, puedan desvirtuar la realidad de sus servicios, enmascaren los límites de los mismos, oscurezcan sus objetivos o prometan resultados de imprevisible, cuando no imposible, consecución.

7.2.22. Principio de responsabilidad

El auditor deberá, como elemento intrínseco de todo comportamiento profesional, responsabilizarse de lo que haga, diga o aconseje, sirviendo esta forma de actuar como cortapisa de injerencias extraprofesionales.

Si bien este principio aparentemente puede resultar especialmente gravoso en auditorías de gran complejidad, que por otra parte son las habitualmente encomendadas a los auditores informáticos, es preciso tenerlo presente a fin de poder garantizar su responsabilidad en los casos en que, debido a errores humanos durante la ejecución de la auditoría, se produzcan daños a su cliente que le pudieran ser imputados.

Por ello es conveniente impulsar la formalización y suscripción de seguros, adaptados a las peculiares características de su actividad, que cubran la responsabilidad civil de los auditores con una suficiente cobertura a fin de acrecentar la confianza y solvencia de su actuación profesional.

Obviamente las compañías aseguradoras podrán introducir determinados módulos correctores del coste de suscripción de las correspondientes pólizas a tenor de las garantías que los auditores puedan aportar (certificaciones profesionales, años de experiencia, etc.), lo que avalaría una más racional estructuración de la oferta.

La responsabilidad del auditor conlleva la obligación de resarcimiento de los daños o perjuicios que pudieran derivarse de una actuación negligente o culposa, si bien debería probarse la conexión causa-efecto originaria del daño, siendo aconsejable estipular *a priori* un tope máximo de responsabilidad sobre los posibles daños acorde con la remuneración acordada como contraprestación por la realización de la auditoría.

7.2.23. Principio de secreto profesional

La confidencia y la confianza son características esenciales de las relaciones entre el auditor y el auditado e imponen al primero la obligación de guardar en secreto los

hechos e informaciones que conozca en el ejercicio de su actividad profesional. Solamente por imperativo legal podrá decaer esa obligación.

Este principio, inherente al ejercicio de la profesión del auditor, estipulado en beneficio de la seguridad del auditado, obliga al primero a no difundir a terceras personas ningún dato que haya visto, oído, o deducido durante el desarrollo de su trabajo que pudiera perjudicar a su cliente, siendo nulos cualesquiera pactos contractuales que pretendieran excluir dicha obligación.

El mantenimiento del secreto profesional sobre la información obtenida durante la auditoría se extiende a aquellas personas que, bajo la potestad organizadora del auditor, colaboren con él en cualesquiera de las actividades relacionadas con la misma.

Si se produjese una dejación, por parte de las personas que dependen del auditor, de la obligación de mantener secreto sobre los datos obtenidos de la auditoría, recaerá sobre ellos la correspondiente obligación de resarcimiento por los daños materiales o morales causados como consecuencia de la misma, obligación que compartirán solidariamente con el auditor en virtud de la responsabilidad *in eligendo* o *in vigilando* que éste asume por los actos de sus colaboradores.

Este deber de secreto impone asimismo al auditor el establecimiento de las medidas y mecanismos de seguridad pertinentes para garantizar al auditado que la información documentada, obtenida a lo largo de la auditoría, va a quedar almacenada en entornos o soportes que impidan la accesibilidad a la misma por terceras personas no autorizadas. El auditor tan sólo deberá permitir el acceso y conocimiento de la misma a los profesionales que, bajo su dependencia organizativa, estén igualmente sujetos al deber de mantener el secreto profesional y en la medida en que, por las necesidades de información de los mismos, sea preciso.

No debe considerarse, por el contrario, como vulneración del secreto profesional, la transmisión de datos confidenciales del auditado a otros profesionales cuando esta circunstancia se origine por expresa petición del mismo; la conservación de los informes durante un plazo prudencial, siempre y cuando se cuente con las medidas de seguridad adecuadas; la difusión, con una finalidad científica, o meramente divulgativa, de los problemas detectados en la auditoría y las soluciones a los mismos si previamente se disgregan los datos de forma tal que no puedan asociarse en ningún caso los mismos a personas o empresas determinadas; ni, por último, la revelación del secreto por imperativo legal siguiendo los cauces correspondientes, debiéndose, aun así, mantener al máximo la cautela que impone dicho levantamiento del secreto.

En los casos en que el auditor actúe por cuenta ajena en el marco contractual establecido con la empresa por medio de la cual presta sus servicios al auditado, la transmisión de la información recogida durante la auditoría a su empresa deberá

circunscribirse únicamente a los datos administrativos reguladores de su actividad (precio de la auditoría, gastos generados, tiempo empleado, medios de la empresa utilizados, etc.), excluyendo de dicha información los datos técnicos observados en el sistema informático o los relacionados con cualesquiera otros aspectos, a no ser que el auditado consienta fehacientemente en que dichos datos sean entregados a los responsables de la empresa que, en este caso, quedarán a su vez obligados a mantener el secreto profesional sobre los mismos.

7.2.24. Principio de servicio público

La aplicación de este principio debe incitar al auditor a hacer lo que esté en su mano y sin perjuicio de los intereses de su cliente, para evitar daños sociales como los que pueden producirse en los casos en que, durante la ejecución de la auditoría, descubra elementos de *software* dañinos (virus informáticos) que puedan propagarse a otros sistemas informáticos diferentes del auditado. En estos supuestos el auditor deberá advertir, necesariamente en forma genérica, sobre la existencia de dichos virus a fin de que se adopten las medidas sociales informativas pertinentes para su prevención, pero deberá asimismo cuidar escrupulosamente no dar indicios que permitan descubrir la procedencia de su información.

El auditor deberá asimismo tener presente la ponderación entre sus criterios éticos personales y los criterios éticos subyacentes en la sociedad en la que presta sus servicios, debiendo poner de manifiesto sus opciones personales cuando entren en contradicción con la ética social que el auditado pueda presumir que está implícitamente aceptada por el auditor.

Este principio de adaptabilidad u oposición constructiva tanto a los principios éticos sociales, asumidos como válidos por la comunidad, como a las costumbres dimanantes de los mismos, facilita la necesaria y permanente crítica social sobre dichos principios y costumbres, permitiendo su adaptación a las nuevas necesidades y perspectivas abiertas con el progreso tecnológico regional o mundial.

La consideración del ejercicio profesional de los auditores como servicio público globalmente considerado, exige igualmente una continua elevación del arte de la ciencia en el campo de la auditoría informática, lo que únicamente puede lograrse con la participación activa de los profesionales de dicho sector en la definición de las características y exigencias de su actividad profesional y, por ende, en la elaboración de los códigos deontológicos reguladores del ejercicio responsable de dicha actividad.

7.2.25. Principio de veracidad

El auditor en sus comunicaciones con el auditado deberá tener siempre presente la obligación de asegurar la veracidad de sus manifestaciones con los límites impuestos por los deberes de respeto, corrección y secreto profesional.

El principio de veracidad no debe, sin embargo, considerarse como constreñido a expresar únicamente aquello sobre lo que se tenga una absoluta y total certeza, sino que implica, con el grado de subjetividad que esto conlleva, poner de manifiesto aquello que, a tenor de sus conocimientos y de lo considerado como "buena práctica profesional", tenga el suficiente grado de fiabilidad como para ser considerado comúnmente como veraz mientras no se aporten datos o pruebas que demuestren lo contrario.

Es conveniente tener presentes los criterios expuestos por nuestro Tribunal Constitucional al respecto, generalmente asociado con la actividad de los profesionales de la comunicación, que indican que la obligación de veracidad impone un específico deber de diligencia que se puede y debe exigir al profesional en la transmisión de la información sobre hechos que deben haber sido necesariamente contrastados con datos objetivos, excluyendo por tanto de dicha calificación de veracidad a aquella información basada en "conductas negligentes" del profesional y aún más a aquella otra proveniente "de quien comunique como hechos simples rumores o, peor aún, meras invenciones o insinuaciones insidiosas", considerando como admisible y presuntamente veraz "la información rectamente obtenida y difundida, aun cuando su total exactitud sea controvertible" (STC de 21 de enero de 1988), ya que, como la citada sentencia indica, "las afirmaciones erróneas son inevitables en un debate libre, de tal forma que de imponerse la verdad como condición para reconocimiento del derecho protegido por el artículo 20.1.d) de la Constitución (a comunicar y recibir información veraz) la única garantía de la seguridad jurídica sería el silencio".

Los criterios del Tribunal Constitucional sobre el alcance de la obligación de veracidad han sido reiterados asimismo en sucesivas sentencias en las que se expresa que "información veraz, en el sentido del artículo 20.1.d) significa información comprobada según los cánones de la profesionalidad informativa, excluyendo invenciones, rumores o meras insidias", y que "una cosa es efectuar una evaluación personal, por desfavorable que sea, de una conducta y otra muy distinta es emitir expresiones, afirmaciones o calificativos claramente vejatorios desvinculados de esa información, y que resultan proferidos, gratuitamente, sin justificación alguna" (STC 105/1990 de 6 de junio); que el derecho a la información "no puede restringirse a la comunicación objetiva y aséptica de los hechos, sino que incluye también la investigación de la causación de hechos, la valoración probabilística de estas hipótesis y la formulación de conjeturas sobre esa posible causación" (STC 171/1990 de 12 de noviembre); que "la descripción de hechos y opiniones que ordinariamente se produce en las informaciones determina que la veracidad despliegue sus efectos legitimadores

en relación con los hechos, pero no respecto de las opiniones que los acompañen o valoraciones que de los mismos se hagan, puesto que las opiniones, creencias personales o juicios de valor no son susceptibles de verificación, y ello determina que el ámbito de protección del derecho de información quede delimitado, respecto de esos elementos valorativos, por la ausencia de expresiones injuriosas que resulten innecesarias para el juicio crítico" (STC 172/1990 de 12 de noviembre); y que "la regla constitucional de la veracidad de la información no va dirigida tanto a la exigencia de la total exactitud en la información cuanto a negar la garantía o protección constitucional a quienes, defraudando el derecho de todos a recibir información veraz, actúan con menosprecio de la veracidad o falsedad de lo comunicado, comportándose de manera negligente o irresponsable" (STC 40/1992 de 30 de marzo).

Así pues, la aplicación de este principio exige que el auditor, en el marco de su obligación de informar al auditado sobre el trabajo realizado, comunique a este último sus conclusiones, diferenciando los hechos constatados de las opiniones, propuestas y valoraciones personales, debiendo actuar en la comprobación de los primeros y en la fundamentación de las restantes con una suficiente diligencia profesional para garantizar el cumplimiento de su obligación de informar verazmente.

7.3. CONCLUSIONES

El auditor informático debe ser plenamente consciente de que su comportamiento profesional presenta dos facetas, íntimamente ligadas, que configuran el régimen de su responsabilidad frente a terceros.

La primera corresponde a la aplicación de sus conocimientos técnicos con la finalidad de determinar, en base a los mismos, las condiciones de seguridad, fiabilidad y calidad de los medios, elementos o productos que conforman el sistema informático auditado y recomendar las medidas que estime convenientes para su mejora o adaptación a los objetivos para los que ha sido diseñado o que, a tenor de la coyuntura actual y previsible a medio plazo, constituyan sus perspectivas de futuro.

La segunda debe poner de manifiesto la aplicación de los fundamentos humanísticos que como persona y como profesional le son éticamente exigibles para, en función de los mismos, coadyuvar al desarrollo integral de la sociedad en la prestación de sus servicios y de la cual ha tomado, para la formación de sus conocimientos y desarrollo de su propia personalidad, las ideas integradas en el patrimonio cultural común aportado por sus antecesores.

Es, por tanto, inexcusable tener presente dicha dualidad de facetas a efectos de no ignorar ninguna de ellas so pretexto de que condicionamientos contractuales, jurídicos, sociales o morales, le obliguen a excluir de su comportamiento profesional alguna de

ellas debiendo tener siempre presente, que si bien la aplicación de sus conocimientos técnicos ayuda al desarrollo tecnológico de la sociedad, la aplicación de sus fundamentos humanísticos ayuda a la configuración de la conciencia moral de la misma, sirviendo como elemento de formación de los usos y costumbres que constituyen una de las fuentes del derecho regulador de la convivencia entre las personas que la integran.

En los casos de producirse algún conflicto entre ambas facetas, la ponderación de los derechos en juego deberá dar primacía a los valores morales sobre los materiales, ya que el fundamento íntimo de las personas descansa en los primeros como manifestación de su propio *ítem vital*, y que asimismo su transposición al entorno social debe imponer su prevalencia sobre los segundos, evitando que el desarrollo tecnológico pueda desvirtuar el desarrollo social que es, en suma, el máximo exponente del grado de evolución de la humanidad.

Como colofón a esos planteamientos cabe reflejar, como ejemplos representativos de la Normalización y aplicación de códigos de deontología profesional, el "Código de ética profesional" de la ISACF (Information Systems Audit and Control Foundation) para orientar la conducta de los auditores informáticos miembros de dicha asociación, y el "Código de Conducta" de The British Computer Society, que establece los estándares profesionales de competencia, conducta y ética de la práctica informática en el Reino Unido.

La ISACF propone el siguiente Código de Ética Profesional para orientar a la conducta profesional, personal de los miembros de la Information Systems Audit and Control Association y/o de los poseedores del Certified Information Systems Auditor (CISA).

"Los Auditores Certificados de Sistemas de Información deberán:

1. Apoyar el establecimiento y cumplimiento de normas, procedimientos y controles de las auditorías de sistemas de información.

2. Cumplir con las Normas de Auditoría de Sistemas de Información, según las adopte la Information Systems Audit and Control Foundation.

3. Actuar en interés de sus empleadores, accionistas, clientes y público en general en forma diligente, leal y honesta, y no contribuir a sabiendas en actividades ilícitas o incorrectas.

4. Mantener la confidencialidad de la información obtenida en el curso de sus deberes. La información no deberá ser utilizada en beneficio propio o divulgada a terceros no legitimados.

5. Cumplir con sus deberes en forma independiente y objetiva y evitar toda actividad que comprometa o parezca comprometer su independencia.

6. Mantener su capacidad en los campos relacionados con la auditoría y los sistemas de información mediante la participación en actividades de capacitación profesional.

7. Ejercer sumo cuidado al obtener y documentar material suficiente sobre el cual basar sus conclusiones y recomendaciones.

8. Informar a las partes involucradas del resultado de las tareas de auditoría que se hayan realizado.

9. Apoyar la entrega de conocimientos a la gerencia, clientes y al público en general para mejorar su comprensión de la auditoría y los sistemas de información.

10. Mantener altos estándares de conducta y carácter tanto en las actividades profesionales como en las privadas."

The British Computer Society por su parte establece un Código de Conducta cuyos principios se esquematizan a continuación.

1. Conducta Profesional: La conducta de los miembros de la Asociación mantendrá la dignidad, reputación y alta evaluación social de la profesión.

2. Integridad profesional: Ningún miembro intentará, en forma desleal, realizar actos en detrimento de la reputación, interés o perspectivas de otros miembros, y actuará, en todo momento, en forma íntegra con la Asociación, sus miembros y los miembros de otras profesiones con los que pueda relacionarse en su ejercicio profesional.

3. Interés Público: Todo miembro en cumplimiento y/o exoneración de su responsabilidad para con sus empleadores o clientes cuidará adecuadamente los intereses públicos y los derechos de terceras personas y, en particular, se asegurará de que los derechos de propiedad intelectual de terceros no se vean perjudicados por sus actos.

4. Fidelidad: Los miembros cumplirán sus obligaciones con sus empleadores o clientes con una completa fidelidad para con los mismos. Asimismo evitarán divulgar la información confidencial relacionada con dichas personas.

5. Competencia Técnica: Todo miembro deberá ofertar únicamente aquellos servicios para los que se considere competente e informará a sus empleadores o clientes sobre el nivel de preparación y capacitación que él posee cuando sus servicios hayan sido solicitados.

6. Imparcialidad: Los miembros, cuando trabajen para un determinado cliente, deberán informarle fehacientemente y por escrito sobre aquellos intereses que tengan y que puedan perjudicar o incidir en la imparcialidad de su dictamen u originar conflictos de interés entre ambos.

7.4. LECTURAS RECOMENDADAS

Davara Rodríguez, Miguel Ángel. *Derecho informático.* Edit. Aranzadi. Pamplona, 1993.

Peso Navarro, Emilio del. *Deontología y seguridad en el mundo informático.* Revista Base informática, n.º 15, junio, 1991.

Peso Navarro, Emilio del y Ramos González, Miguel Ángel: *Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas.* Ediciones Díaz de Santos. Madrid, 1994.

Ramos González, Miguel Ángel. *Contribución a la mejora de las técnicas de auditoría Informática mediante la aplicación de métodos y herramientas de Ingeniería del Conocimiento.* Tesis doctoral. Facultad de Informática de la Universidad Politécnica de Madrid, septiembre, 1990.

Vázquez, Jesús María y Barroso, Porfirio. *Deontología de la informática (Esquemas).* Instituto de Sociología Aplicada. Madrid, 1993.

7.5. CUESTIONES DE REPASO

1. Principios deontológicos aplicables a los auditores informativos.

2. Principio de calidad.

3. Principio de criterio propio.

4. ¿Qué significa el principio de economía?
5. Importancia de la formación continua del auditor informático.
6. Grado de independencia del auditor informático.
7. ¿Qué es el principio de legalidad?
8. Responsabilidad del auditor informático.
9. ¿A qué obliga el secreto profesional?
10. Facetas que configuran el régimen de responsabilidad frente a terceros.

CAPÍTULO 8

LA AUDITORÍA FÍSICA

Gabriel Desmonts Basilio

8.1. INTRODUCCIÓN

Lo físico en Informática, hasta ahora, ha tenido una importancia relativa; no en vano se ha visto siempre como algo que soporta lo que, en realidad, es la Informática, y que ocupa un lugar en la mesa.

La UCP (enorme), la pantalla, el teclado, la impresora, cables... y, además, el ratón con su alfombrilla que impiden extender libros y papeles sobre un espacio que, incomprensiblemente, por grande que sea, no existe.

Pero lo físico en Informática no se reduce únicamente a lo expuesto, esto es: dar un soporte tangible, un continente o vehículo a lo etéreo del software, verdadera esencia informática. Todo cuanto rodea o se incluye en el computador, también este mismo, son lo físico como tal, así como otros conceptos o virtualidades que, de una u otra forma, influyen o toman su razón de ser en el Entorno Físico del computador como generalidad o en el del CPD como Unidad Física Informática.

Si se ha dicho que lo físico es algo tangible que proporciona un continente, medio o vehículo y que, además, acoge al CPD dentro de su entorno, una vez conseguido y establecido debería dejar de preocupar. El paso siguiente es asegurarse de que va a seguir dando servicio siempre que se le necesite y de una manera segura ya que, como en toda actividad, se mezcla lo físico con lo funcional y con lo humano.

La Auditoría es el medio que va a proporcionar la evidencia o no de la Seguridad Física en el ámbito en el que se va a desarrollar la labor profesional. Es por tanto, necesario asumir que la Auditoría Física no se debe limitar a comprobar la existencia

de los medios físicos, sino también su funcionalidad, racionalidad y seguridad, palabra esta última que puede resumir o incluir a las anteriores y llevar a un subtítulo de este capítulo que prolongue el ya establecido de Auditoría Física con el de *Auditoría de la Seguridad Física.*

8.2. LA SEGURIDAD FÍSICA

No están muy claras las fronteras que delimitan, si es que lo hacen, los dominios y responsabilidades de los tres tipos de seguridad que a los usuarios de la Informática deben interesar: seguridad lógica, seguridad física y seguridad de las Comunicaciones. Quizá fuera más práctico aunarlas y obtener una seguridad integral, aunque hay que reconocer las diferencias que, evidentemente, existen entre *soft, hard, hard-soft, hard* que soporta al *soft y soft* que mueve al *hard.*

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un CPD. Si se entiende la contingencia o proximidad de un daño como la definición de Riesgo de Fallo, local o general, tres serían las medidas a preparar para ser utilizadas en relación con la cronología del fallo:

8.2.1. Antes

Obtener y mantener un Nivel adecuado de Seguridad Física sobre los activos.

El Nivel adecuado de Seguridad Física, o grado de seguridad, es un conjunto de acciones utilizadas para evitar el Fallo o, en su caso, aminorar las consecuencias que de él se puedan derivar.

Es un concepto general aplicable a cualquier actividad, no sólo informática, en la que las personas hagan uso particular o profesional de entornos físicos.

- Ubicación del edificio.
- Ubicación del CPD dentro del edificio.
- Compartimentación.
- Elementos de construcción.
- Potencia eléctrica.
- Sistemas contra incendios.
- Control de accesos.
- Selección de personal.
- Seguridad de los medios.
- Medidas de protección.
- Duplicación de medios.

8.2.2. Durante

Ejecutar un Plan de Contingencia adecuado.

En general, *desastre* es cualquier evento que, cuando ocurre, tiene la capacidad de interrumpir el normal proceso de una empresa.

La probabilidad de que ocurra un desastre es muy baja, aunque, si se diera, el impacto podría ser tan grande que resultara fatal para la organización. Como, por otra parte, no es corriente que un negocio responda por sí mismo ante un acontecimiento como el que se comenta, se deduce la necesidad de contar con los medios necesarios para afrontarlo. Estos medios quedan definidos en el Plan de Recuperación de Desastres que, junto con el Centro Alternativo de Proceso de Datos, constituye el *Plan de Contingencia* que coordina las necesidades del negocio y las operaciones de recuperación del mismo.

El Plan de Contingencia inexcusablemente debe:

- Realizar un Análisis de Riesgos de Sistemas Críticos que determine la Tolerancia de los Sistemas.
- Establecer un Período Crítico de Recuperación en el cual los procesos deben ser reanudados antes de sufrir pérdidas significativas o irrecuperables.
- Realizar un Análisis de Aplicaciones Críticas por el que se establecerán las Prioridades de Proceso.
- Determinar las Prioridades de Proceso, por días del año, que indiquen cuáles son las Aplicaciones y Sistemas Críticos en el momento de ocurrir el desastre y el orden de proceso correcto.
- Establecer Objetivos de Recuperación que determinen el período de tiempo (horas, días, semanas) entre la declaración de Desastre y el momento en que el Centro Alternativo puede procesar las Aplicaciones Críticas.
- Designar, entre los distintos tipos existentes, un Centro Alternativo de Proceso de Datos.
- Asegurar la Capacidad de las Comunicaciones y
- Asegurar la Capacidad de los Servicios de Back-up.

8.2.3. Después

Los Contratos de Seguros vienen a compensar, en mayor o menor medida, las pérdidas, gastos o responsabilidades que se pueden derivar para el CPD una vez detectado y corregido el Fallo.

De entre la gama de seguros existentes, se pueden señalar:

- *Centros de proceso y equipamiento*: Se contrata cobertura sobre daño físico en el CPD y el equipo contenido en él.

- *Reconstrucción de medios software*: Cubre el daño producido sobre medios *soft* tanto los que son propiedad del tomador del seguro como aquellos que constituyen su responsabilidad.

- *Gastos extra*: Cubre los gastos extra que se derivan de la continuidad de las operaciones tras un *desastre* o daño en el CPD. Es suficiente para compensar los costos de ejecución del Plan de Contingencia.

- *Interrupción del negocio*: Cubre las pérdidas de beneficios netos causadas por las caídas de los medios informáticos o por la suspensión de las operaciones.

- *Documentos y registros valiosos*: Se contrata para obtener una compensación en valor metálico real por la pérdida o daño físico sobre documentos y registros valiosos no amparados por el seguro de Reconstrucción de Medios Software.

- *Errores y omisiones*: Proporciona protección legal ante la responsabilidad en que pudiera incurrir un profesional que cometiera un acto, error u omisión que ocasione una pérdida financiera a un cliente.

- *Cobertura de fidelidad*: Cubre las pérdidas derivadas de actos deshonestos o fraudulentos cometidos por empleados.

- *Transporte de medios*: Proporciona cobertura ante pérdidas o daños a los medios transportados.

- *Contratos con proveedores y de mantenimiento*: Proveedores o fabricantes que aseguren la existencia de repuestos y consumibles, así como garantías de fabricación.

Contratos de mantenimiento que garanticen la asistencia técnica a los equipos e instalaciones una vez extinguidas las garantías de fabricación.

No son realmente Seguros, ya que:

- Los primeros se ubicarían en Nivel adecuado de Seguridad Física (el **antes).**
- Los segundos pueden localizarse tanto en el Nivel adecuado (el **antes**) como en el Plan (el **durante).**

No obstante, dada su forma y su control administrativo, se les puede considerar como Seguros.

8.3. ÁREAS DE LA SEGURIDAD FÍSICA

Se ha expuesto, hasta el momento, un estudio de las tres medidas a preparar para ser utilizadas según el momento del Fallo; riesgo de que se produzca, si se está produciendo y cuando ha pasado. Todo ello partiendo, como primer paso, de la ubicación del edificio y las circunstancias externas e internas que le afectan.

Nada se ha dicho del edificio en sí mismo: ¿sería capaz el Auditor Informático de revisar la construcción y el estado actual de su infraestructura con sus defectos, vicios y posibles enfermedades? Más aún: ¿es capaz de diagnosticar en este tema? Evidentemente, como tal auditor, carece de la capacidad y preparación necesarias para ello. Por tanto, debe considerarse al edificio como la primera de las áreas a tener en cuenta en una Auditoría Física y prever para ella el auxilio de Peritos independientes que den respuestas a las preguntas a plantear durante la Fase 2 del Procedimiento de Auditoría *Adquisición de Información General* y certificaciones que puedan ser incluidas como pruebas, en uno o en otro sentido, en la Fase 9 *Informe Final* tras la *Discusión con los Responsables* si hubiera lugar.

Las áreas en las que el Auditor ha de interesarse personalmente, una vez que la parte del edificio ha sido encargada al juicio del Perito, tendrán relación directa con el hecho informático, siempre considerando el aspecto físico de la seguridad, y que serán tales como:

Organigrama de la empresa

Por él se conocerán las dependencias orgánicas, funcionales y jerárquicas de los departamentos y de los distintos cargos y empleos del personal pudiendo analizar, con

ayuda de documentación histórica, las apropiadas Separación de Funciones y Rotación en el Trabajo.

Da la primera y más amplia visión de conjunto del Centro de Proceso.

Auditoría interna

Departamento independiente o subordinado al de Auditoría Financiera, si existe, y colaborador de éste en cualquier caso, debe guardar las auditorías pasadas, las Normas, Procedimientos y Planes que sobre la Seguridad Física y su Auditoría haya emitido y distribuido la Autoridad competente dentro de la Empresa.

Administración de la seguridad

Vista desde una perspectiva general que ampare las funciones, dependencias, cargos y responsabilidades de los distintos componentes:

- Director o Responsable de la Seguridad Integral.
- Responsable de la Seguridad Informática.
- Administradores de Redes.
- Administradores de Bases de Datos.
- Responsables de la Seguridad activa y pasiva del Entorno físico.

Normas, Procedimientos y Planes que, desde su propia responsabilidad haya emitido, distribuido y controlado el departamento.

Centro de proceso de datos e instalaciones

Entorno en el que se encuentra incluso el CPD como elemento físico y en el que debe realizar su función informática.

Las instalaciones son elementos accesorios que deben ayudar a la realización de la mencionada función informática y, a la vez, proporcionar seguridad a las personas, al soft y a los materiales.

- Sala del Host.
- Sala de Operadores.
- Sala de Impresoras.
- Cámara Acorazada.
- Oficinas.

- Almacenes.
- Sala de aparamenta eléctrica.
- Sala de Aire Acondicionado.
- Área de descanso y servicios...

Equipos y comunicaciones

Son los elementos principales del CPD: Host, terminales, computadores personales, equipos de almacenamiento masivo de datos, impresoras, medios y sistemas de telecomunicaciones...

El Auditor debe inspeccionar su ubicación dentro del CPD así como el Control de Acceso a los mismos como elementos restringidos.

Computadores personales

Especialmente cuando están en red, son elementos muy potentes e indiscretos que pueden acceder a prácticamente cualquier lugar donde se encuentren los Datos *(primer objetivo de toda seguridad)*, por lo que merecerán especial atención tanto desde el punto de vista de acceso a los mismos como a la adquisición de copias *(hard y soft)* no autorizadas. Es especialmente delicada su conexión a los medios de telecomunicaciones.

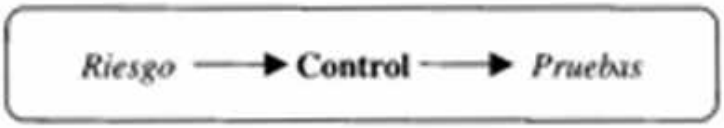
Seguridad física del personal

Accesos y salidas seguras así como medios y rutas de evacuación, extinción de incendios y medios utilizados para ello (agua en lugares con conducciones y aparatos eléctricos, gases asfixiantes...), sistemas de bloqueo de puertas y ventanas, zonas de descanso y de servicios...

Normas y Políticas emitidas y distribuidas por la Dirección referentes al uso de las instalaciones por el personal.

8.4. DEFINICIÓN DE AUDITORÍA FÍSICA

La Auditoría Física, interna o externa, no es sino una auditoría parcial, por lo que no difiere de la auditoría general más que en el Alcance de la misma.



8.5. FUENTES DE LA AUDITORÍA FÍSICA

Ya se ha comentado, brevemente en los párrafos anteriores, cuáles pueden ser algunas de las Fuentes donde la Auditoría va a encontrar la información necesaria para organizar y desarrollar la Fase 4 del Procedimiento o Ciclo de Vida de la Auditoría *"Plan de Auditoría"* que le llevará a realizar las pertinentes Pruebas de Cumplimiento y Sustantivas.

Un CPD, en esencia, sigue un modelo organizativo más o menos estándar, aunque debido a diferentes causas, como puede ser el tipo de empresa a la que pertenece, situación económica, disponibilidades de espacio, actitud de la Dirección, etc. hacen que, en realidad, los CPD's difieran bastante los unos de los otros.

Se señalan a continuación algunas Fuentes que deben estar accesibles en todo Centro de Proceso de Datos.

- *Políticas, Normas y Planes* sobre Seguridad emitidos y distribuidos tanto por la Dirección de la empresa en términos generales como por el Departamento de Seguridad siguiendo un enfoque más detallado.

- *Auditorías anteriores,* generales y parciales, referentes a la Seguridad Física o a cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la Seguridad Física.

- *Contratos de Seguros, de Proveedores y de Mantenimiento.*

- *Entrevistas* con el personal de seguridad, personal informático y de otras actividades, responsables de seguridad de otras empresas dentro del edificio y de la seguridad general del mismo, personal contratado para la limpieza y mantenimiento de locales, etc.

- *Actas e Informes* de técnicos y consultores. Peritos que diagnostiquen el estado físico del edificio, electricistas, fontaneros, técnicos del aire acondicionado, especialistas en electrónica que informen sobre la calidad y estado de operatividad de los sistemas de seguridad y alarma, agencias de seguridad que proporcionan a los Vigilantes jurados, bomberos, etc.

- *Plan de Contingencia y valoración de las Pruebas.*

- *Informes sobre accesos y visitas.* Existencia de un sistema de control de entradas y salidas diferenciando entre áreas Perimetral, Interna y Restringida.

  Informes sobre pruebas de evacuación ante diferentes tipos de amenaza: incendio, catástrofe natural, terrorismo, etc.

  Informes sobre evacuaciones reales.

- *Políticas de Personal.* Revisión de antecedentes personales y laborales, procedimientos de cancelación de contratos y despidos, rotación en el trabajo, planificación y distribución de tareas, contratos fijos y temporales.

- *Inventarios de Soportes* (papel y magnéticos): cintoteca, back-up, procedimientos de archivo, controles de salida y recuperación de soportes, control de copias, etc.

8.6. OBJETIVOS DE LA AUDITORÍA FÍSICA

Más arriba, en Áreas de la Seguridad Física párrafo Computadores Personales, se decía que los Datos son el primer objetivo de toda seguridad. Bien entendido que hacía referencia a toda seguridad informática, la Seguridad Física es más amplia y alcanza otros conceptos entre los que puede haber alguno que supere en importancia a los propios datos.

Sin otro ánimo más que el mero orden basado en una lógica *"de fuera adentro"*, quedan indicados estos Objetivos como sigue:

- Edificio.
- Instalaciones.
- Equipamiento y telecomunicaciones.
- Datos.
- Personas.

8.7. TÉCNICAS Y HERRAMIENTAS DEL AUDITOR

Como se verá, no se diferencian de las técnicas y herramientas básicas de toda auditoría y, como en ellas, su fin es obtener la Evidencia física.

Técnicas:

- *Observación* de las instalaciones, sistemas, cumplimiento de Normas y Procedimientos, etc. no sólo como espectador sino también como actor, comprobando por sí mismo el perfecto funcionamiento y utilización de los conceptos anteriores.

- Revisión analítica de:

  - Documentación sobre construcción y preinstalaciones.
  - Documentación sobre seguridad física.
  - Políticas y Normas de Actividad de Sala.
  - Normas y Procedimientos sobre seguridad física de los datos.
  - Contratos de Seguros y de Mantenimiento.

- *Entrevistas* con directivos y personal, fijo o temporal, que no dé la sensación de interrogatorio para vencer el natural recelo que el auditor suele despertar en los empleados.

- *Consultas* a técnicos y peritos que formen parte de la plantilla o independientes contratados.

Herramientas:

- *Cuaderno de campo / grabadora de audio*
- *Máquina fotográfica / cámara de vídeo*

Su uso debe ser discreto y siempre con el consentimiento del personal si éste va a quedar identificado en cualquiera de las máquinas.

8.8. RESPONSABILIDADES DE LOS AUDITORES

El Auditor Informático, en especial el Interno, no debe desarrollar su actividad como una mera *función policial* dando la impresión a los usuarios informáticos y al resto de empleados de que se encuentran permanentemente vigilados. Esto crea un ambiente tenso y desagradable que en nada favorece ni a las relaciones personales ni al buen desarrollo del trabajo.

El auditor debe esforzarse más en dar una imagen de colaborador que intenta ayudar que en la de fiscalizador o caza-infractores. Para ello es necesario que en las Normas y Procedimientos emitidos por la Dirección figuren las funciones y responsabilidades de los auditores y que ambas sean distribuidas y conocidas por toda la plantilla de la empresa.

Dentro del campo de responsabilidades de los auditores, las referentes a Seguridad Física, quedan establecidas las siguientes para cada tipo de auditor:

Auditor informático interno

- Revisar los controles relativos a Seguridad Física.
- Revisar el cumplimiento de los Procedimientos.
- Evaluar Riesgos.
- Participar sin perder independencia en:
  - Selección, adquisición e implantación de equipos y materiales.
  - Planes de Seguridad y de Contingencia, seguimiento, actualización, mantenimiento y pruebas de los mismos.
- Revisión del cumplimiento de las Políticas y Normas sobre Seguridad Física así como de las funciones de los distintos Responsables y Administradores de Seguridad.
- Efectuar auditorías programadas e imprevistas.
- Emitir informes y efectuar el seguimiento de las recomendaciones.

Auditor informática externo

- Revisar las funciones de los auditores internos.
- Mismas responsabilidades que los auditores internos.
- Revisar los Planes de Seguridad y Contingencia. Efectuar Pruebas.
- Emitir informes y recomendaciones.

8.9. FASES DE LA AUDITORÍA FÍSICA

Siguiendo la Metodología EDPAA y sin perjuicio de alguna pequeña diferencia, más que nada en el orden o el ámbito de las fases, el Ciclo de Vida quedaría:

Fase 1: Alcance de la Auditoría
Fase 2: Adquisición de Información General
Fase 3: Administración y Planificación
Fase 4: Plan de Auditoría
Fase 5: Resultado de las Pruebas
Fase 6: Conclusiones y Comentarios
Fase 7: Borrador del Informe
Fase 8: Discusión con los Responsables de Área
Fase 9: Informe Final

- Informe
- Anexo al Informe
- Carpeta de Evidencias

Fase10: Seguimiento de las Modificaciones acordadas.

8.10. DESARROLLO DE LAS FASES DE LA AUDITORÍA FÍSICA

Resulta clara la práctica identidad entre el Ciclo de Vida de la Auditoría Física con cualquier otro de una auditoría diferente.

Con la intención de ofrecer algo práctico dentro de tanta teoría, se expone a continuación el desarrollo de la Fase 2 *Adquisición de Información* referente a un Plan de Contingencia, siguiendo la técnica del *check-list* para un mejor entendimiento de los conceptos.

La lista es, naturalmente, orientativa y en ningún caso se puede considerar completa.

Auditoría del plan de contingencia

Fase 2 Adquisición de Información

Acuerdo de Empresa para el Plan de Contingencia

- ¿Hay algún acuerdo oral o escrito por parte de la Dirección?
- ¿Ha emitido y distribuido la empresa Políticas o Normas dirigidas al Plan de Contingencia?
- ¿Qué persona o departamento tiene la responsabilidad del Plan?
- ¿Están las responsabilidades de Planeamiento bien definidas, difundidas y entendidas por todo el personal?
- ¿Se mantiene una estrategia corporativa en el Plan? Todos los departamentos deben cooperar en el Plan desde su propia especialidad o responsabilidad.

- ¿Incluyen los presupuestos empresariales fondos destinados al desarrollo y mantenimiento del Plan de Contingencia?

Acuerdo de un Proceso Alternativo

- ¿Está el Acuerdo obligado e impuesto legalmente cuando se produce un desastre?
- ¿Es compatible el equipamiento del Proceso de Datos en el Certro Alternativo con el equipamiento en el CPD?
- ¿Proporciona el Centro Alternativo suficiente capacidad?
- ¿Cuándo fue la última vez que se probó el Centro Alternativo?
- ¿Cuáles fueron los objetivos y el alcance de la prueba?
- ¿Cuáles fueron los resultados de la prueba?, ¿quedaron los resultados bien documentados?
- ¿Han sido implementadas acciones correctivas o están previstas para una futura implementación?
- ¿Está prevista una próxima prueba de uso del Centro Alternativo?
- ¿Utiliza la empresa algún equipamiento de proceso que pueda no estar soportado por el Centro Alternativo?

Protección de Datos

- ¿Tiene la empresa un Centro Externo para el almacenamiento de los *back-up?*
- ¿Se ha realizado alguna vez una auditoría de las cintas y discos almacenados en el Centro Back-up Externo?
- ¿Cuál es el Procedimiento de Acceso al Centro Externo para la obtención de los back-up en el caso de un desastre?
- ¿Cuál es el Procedimiento de Transporte de los back-up desde el Centro Externo al Centro de Proceso Alternativo?

- ¿Cuál es la estrategia para la Restauración de programas?, ¿serán almacenadas las aplicaciones simultáneamente o en fases basadas en prioridades?
- ¿Ha sido asignada prioridad de restauración a cada aplicación?
- ¿Han sido identificados todos los archivos críticos?
- ¿Se han creado los back-up de los archivos críticos según una base metódica?
- ¿Existe un mínimo de tres ciclos de copias de back-up en el Centro Externo?
- ¿Existen copias actualizadas de los Informes del Sistema de Gestión de Cintas almacenadas en el Centro Back-up Externo?

Manual del Plan de Contingencia

- ¿Cómo está estructurado el Plan?
- ¿Es fácil de seguir el Plan en el caso de un desastre?
- ¿Indica el Plan quién es el responsable de desarrollar tareas específicas?
- ¿Cómo se activa el Plan ante un desastre?
- ¿Cómo están contenidos estos procedimientos de activación en los procedimientos de emergencia normales de la empresa?
- ¿Han sido probados estos procedimientos en un test de desastre simulado?
- ¿Contiene el Plan procedimientos que fijen los daños en las etapas iniciales de las Operaciones de Recuperación?
- ¿Incluye el Plan procedimientos para trasladar el proceso desde el Centro Alternativo al Centro Restaurado o Nuevo?
- ¿Contiene el Plan listados del Inventario del proceso de datos y *hard* de comunicaciones, software, formularios preimpresos y stock de papel y accesorios?
- ¿Están actualizados los listines telefónicos del personal de Recuperación así como empleados del Proceso de Datos, alta dirección, usuarios finales y vendedores y suministradores?

- ¿Cómo está mantenido el Plan?
- ¿Quién es el responsable de actualizar el Plan?
- ¿Se mantiene el *Log* de distribución del Plan?
- ¿Cuándo fue actualizado el Plan por última vez?
- ¿Existe una copia del Plan en el Centro Externo de *Back-up?*

8.11. LECTURAS RECOMENDADAS

Thomas, A. J. y Douglas, I. J. *Auditoría Informática.* Paraninfo, Madrid, 1987.
Contingency Planning. Auerbach Publishers.

8.12. CUESTIONES DE REPASO

1. Diferencie entre seguridad lógica, seguridad física y seguridad de las comunicaciones, poniendo varios ejemplos de cada tipo.
2. Explique el concepto de "nivel adecuado de seguridad física".
3. ¿Cómo definiría lo que constituye un "desastre"?
4. ¿Qué tipos de seguros existen?
5. ¿Qué medios de extinción de fuego conoce?
6. ¿Por qué es importante la existencia de un sistema de control de entradas y salidas?
7. ¿Qué técnicas cree que son las más adecuadas para la auditoría física?
8. ¿Cuáles suelen ser las responsabilidades del auditor informático interno respecto a la auditoría física?
9. ¿Qué aspectos considera más importantes a la hora de auditar el plan de contingencia desde el punto de vista de la auditoría física?
10. ¿Qué riesgos habría que controlar en el centro de proceso alternativo?

CAPÍTULO 9

AUDITORÍA DE LA OFIMÁTICA

Manuel Gómez Vaz

9.1. INTRODUCCIÓN

El término ofimática, comúnmente utilizado en diferentes ámbitos profesionales, no aparece definido, sin embargo, en el diccionario de la Real Academia Española de la Lengua. Aunque el objetivo de este capítulo no consiste en determinar el concepto de ofimática ni en profundizar sobre el mismo, resulta imprescindible disponer de una definición que sirva de punto de partida para el desarrollo del tema que nos ocupa. A tales efectos, partiremos de la definición realizada por Schill, entendiendo ofimática como el sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina.

El concepto de ofimática nace a comienzos de la pasada década y las primeras aplicaciones se desarrollan sobre los computadores centrales de las organizaciones. Aunque las oficinas siempre han sido consideradas como pioneras en la utilización de herramientas informáticas para el desarrollo de sus actividades; desde comienzos de los noventa se ha producido un espectacular crecimiento en la demanda de sistemas ofimáticos que todavía continúa acrecentándose. Ejemplos de ello son: las aplicaciones específicas para la gestión de tareas, como hojas de cálculo o procesadores de textos; herramientas para la gestión de documentos, como control de expedientes o sistemas de almacenamiento óptico de información; agendas y bases de datos personales; sistemas de trabajo en grupo como el correo electrónico o el control de flujos de trabajos; etc.

La evolución sufrida en el entorno microinformático ha condicionado el desarrollo de los sistemas ofimáticos actuales. El aumento de la potencia de cálculo, la alta calidad de los productos y la reducción de costes de los computadores

personales y las estaciones de trabajo, ha desplazado el desarrollo de aplicaciones ofimáticas a plataformas microinformáticas y redes de área local. Hoy en día, parece incuestionable que los productos desarrollados en plataformas microinformáticas ofrecen unas prestaciones y una relación coste/beneficio muy superior a las soluciones sobre computadores centralizados. Este desarrollo de sistemas ofimáticos ha mantenido dos paradigmas fundamentales: el escritorio virtual y el trabajo cooperativo (CSCW, *Computed Supported Cooperative Work*).

Podemos aproximar el concepto de escritorio virtual como un único panel, representado por la pantalla del computador, que sustituya la mesa de trabajo tradicional, y donde se encuentren disponibles todas las herramientas necesarias para desarrollar las actividades del oficinista. La interfaz debe parecer natural al usuario y debe ser fácil de aprender y utilizar. Las diversas aplicaciones, además de realizar las tareas para las que han sido diseñadas de un modo eficaz y eficiente, deben integrarse perfectamente entre sí.

El CSCW podría considerarse como una extensión del concepto de integración de aplicaciones. De acuerdo con Kraemer, podríamos definirlo como una multiplicidad de actividades coordinadas, desarrolladas por un conjunto de participantes y soportadas por un sistema informático. Por consiguiente, el entorno ofimático, además de posibilitar la realización del trabajo personal de cada empleado, debe permitir intercambiar la información necesaria en los diversos procesos de la organización, así como posibles interacciones con otras organizaciones.

La práctica totalidad de los paquetes ofimáticos presentes en el mercado se han desarrollado siguiendo el paradigma del escritorio virtual alcanzando un grado de desarrollo aceptable incluso facilitando la integración con otros productos de diferentes fabricantes. Asimismo, durante los últimos años se ha incrementado la oferta de aplicaciones CSCW, debido principalmente al desarrollo espectacular sufrido en las comunicaciones. Este tipo de aplicaciones han incrementado sus funcionalidades y están avanzando en la implantación de estándares para la integración entre sistemas ofimáticos de distintas organizaciones.

9.2. CONTROLES DE AUDITORÍA

La mayoría de los problemas que se producen en la informatización de oficinas no difieren sustancialmente de los encontrados en otros ámbitos de la organización. Sin embargo, existen dos características peculiares de los entornos ofimáticos: la distribución de las aplicaciones por los diferentes departamentos de la organización en lugar de encontrarse en una única ubicación centralizada; y el traslado de la responsabilidad sobre ciertos controles de los sistemas de información a usuarios

finales no dedicados profesionalmente a la informática, que pueden no comprender de un modo adecuado la importancia de los mismos y la forma de realizarlos.

Como consecuencia de los dos factores enunciados, se ha generado una problemática propia en este tipo de entornos: adquisiciones poco planificadas; desarrollos ineficaces e ineficientes, incluso en procesos críticos para el correcto funcionamiento de la organización; falta de conciencia de los usuarios acerca de la seguridad de la información; utilización de copias ilegales de aplicaciones; procedimientos de copias de seguridad deficientes; escasa formación del personal; ausencia de documentación suficiente; etc.

Considerando los problemas expuestos y dejando al margen los conceptos desarrollados en el capítulo correspondiente a la auditoría de redes para evitar solapamientos, hemos elaborado una relación de controles de auditoría básicos. Los controles seleccionados, sin conformar una relación exhaustiva, han sido descritos de tal modo que puedan ser de aplicación a cualquier organización, adaptándolos a las características de la misma. En algunos entornos será necesario algún control adicional que no se encuentre entre los propuestos y en otros entornos alguno de los controles puede no resultar adecuado.

Los controles, que se presentan agrupados siguiendo criterios relacionados con aspectos de economía, eficacia y eficiencia; seguridad y condicionantes legales, son lo suficientemente generales para servir de base en la elaboración del guión de trabajo de la labor del equipo auditor.

9.2.1. Economía, eficacia y eficiencia

Determinar si el inventario ofimático refleja con exactitud los equipos y aplicaciones existentes en la organización.

A causa del bajo coste de muchos componentes, resulta difícil mantener un registro fiable de todas las compras que realiza la organización. Con frecuencia algunos departamentos sortean los procedimientos de autorizaciones de compra establecidos dentro de la organización, por ejemplo, utilizando facturas de adquisición de material no inventariable.

Un inventario poco fiable puede repercutir en el balance de la organización, posibilitando que no se detecten sustracciones de equipamiento informático o de licencias de programas contratadas. Hemos seleccionado este control en primer lugar, ya que la fiabilidad del inventario resultará indispensable para auditar otros controles presentados posteriormente.

El equipo auditor comprobará que se han definido mecanismos para garantizar que todos los equipos adquiridos en la organización son debidamente inventariados.

Después, constatará la conciliación realizada en la última auditoría financiera entre el inventario oficial y las adquisiciones efectuadas. Más tarde, revisando todas las dependencias, almacenes y archivos, elaborará una relación exhaustiva de los equipos informáticos y de las aplicaciones y archivos que residen en los mismos. En esta relación debe quedar reflejada también la versión correspondiente a cada una de las aplicaciones instaladas.

Finalmente, identificará las diferencias reales entre la relación elaborada por el equipo auditor y el inventario oficial para proceder a la subsanación de los errores detectados.

Determinar y evaluar el procedimiento de adquisiciones de equipos y aplicaciones.

Una política de adquisiciones descentralizada en la que cada departamento se encargue de realizar sus compras, ofrece ventajas en cuanto a flexibilidad y capacidad de reacción de los mismos, pero podría acarrear significativas pérdidas económicas para el conjunto de la organización.

El equipo auditor comprobará que en el procedimiento de adquisición se valoran aspectos relativos a la necesidad real de los equipos solicitados y a la integración de dichos equipos con el sistema existente. En el caso de compra de paquetes o de contratación de desarrollos externos, determinará si las prestaciones ofrecidas por el producto solicitado se ajustan a las actividades que se pretenden desarrollar con él; si las plataformas en las que van a ser instaladas las aplicaciones tienen suficiente capacidad para soportarlas de un modo eficiente; si los nuevos productos pueden configurarse, en caso de necesidad, para obtener suficientes pistas de auditoría que permitan efectuar un seguimiento de las anomalías producidas durante su ejecución; y la experiencia y solvencia del proveedor.

Partiendo, del inventario debidamente actualizado, analizará los procedimientos para la adquisición de los productos seguidos en los diversos departamentos de la organización y determinará la existencia de equipos y aplicaciones similares. En caso de que los diversos departamentos de la compañía realicen pedidos sobre equipos y complementos de manera independiente, estudiará si se está desaprovechando la posibilidad de negociar descuentos mediante la aplicación de una política centralizada de compras. Del mismo modo, considerará otros mecanismos que pudieran reducir los costes de la organización como podría ser la negociación centralizada de compra de licencias de aplicaciones.

Determinar y evaluar la política de mantenimiento definida en la organización.

Los procedimientos descentralizados han propiciado que, en ocasiones, los equipos adquiridos no sean incluidos ni en el inventario ni en los contratos de mantenimiento. Incluso podría llegar a suceder que el personal de la organización encargado del mantenimiento no dispusiera de los conocimientos recesarios para llevarlo a cabo.

El equipo auditor examinará la utilización de las garantías de los productos adquiridos, comprobando que no se realizan pagos innecesarios por asistencias de equipos y aplicaciones que se encuentren en garantía. Para ello, deberá verificar que los usuarios finales conocen el estado de las garantías de cada uno de los productos que utilizan y los mecanismos para hacerlas efectivas.

Por lo que respecta a productos cuya garantía haya caducado, determinará cuáles disponen de contratos de mantenimiento vigentes con empresas externas y cuáles son aquellos en los que la responsabilidad del mantenimiento recae en la propia organización. En las contrataciones de mantenimiento con empresas externas, verificará si se han incluido en el contrato aspectos como el tiempo máximo de respuesta, recambios y mano de obra, mantenimiento preventivo, etc. También comprobará que el personal, tanto interno como externo, asignado en tareas de mantenimiento tiene suficientes conocimientos de las plataformas que debe mantener, y que recibe la formación adecuada sobre los nuevos productos instalados en la organización.

En relación con la gestión de incidencias producidas, el equipo auditor comprobará la existencia de un registro de las mismas, los procedimientos establecidos para asignar recursos para solucionarlas, los guiones preparados para solventar las incidencias más frecuentes y el seguimiento de las mismas hasta su resolución. También valorará si el tiempo empleado para atender las solicitudes y resolver las incidencias producidas puede llegar a afectar al funcionamiento de la organización.

Evaluar la calidad de las aplicaciones del entorno ofimático desarrollada por personal de la propia organización.

La utilización de herramientas ofimáticas por los usuarios finales ha propiciado el desarrollo de aplicaciones, en muchos casos sin las debidas garantías de fiabilidad, cuyo mal funcionamiento puede repercutir significativamente en la actividad de la organización cuando se trate de aplicaciones que gestionen procesos críticos. Por otra parte, también es común que los desarrollos en estos entornos no hayan seguido los controles de calidad y seguridad suficientes, posibilitando que algún programador haya introducido "puertas traseras", bombas lógicas o cualquier otro mecanismo que pudiera perturbar el buen funcionamiento de la aplicación desarrollada.

El equipo auditor determinará la existencia de un departamento responsable de controlar el desarrollo de aplicaciones de toda la organización, y que se han definido procedimientos generales de petición, autorización, asignación de prioridades, programación y entrega de aplicaciones, o bien si los departamentos han desarrollado aplicaciones de uso interno, bajo sus propios criterios, sin control de un departamento responsable. En el caso de desarrollos realizados por personal de los propios departamentos, el equipo auditor tendrá que determinar si la metodología empleada y los test de pruebas se ajustan a lo dispuesto en la organización.

Al igual que en el caso de las aplicaciones adquiridas o desarrolladas fuera de la organización, comprobará que las aplicaciones desarrolladas internamente pueden configurarse para obtener las suficientes pistas de auditoría que permitan efectuar un seguimiento de las anomalías producidas durante su ejecución. Asimismo, verificará que los desarrollos se realizan sobre un entorno de desarrollo, evitando operar directamente sobre los datos reales de explotación.

También es tarea del equipo auditor examinar el *reporte* de incidencias de las aplicaciones, así como las reclamaciones manifestadas por los clientes y usuarios como indicios para detectar aquellas aplicaciones que podrían estar funcionando de un modo anómalo.

Evaluar la corrección del procedimiento existente para la realización de los cambios de versiones y aplicaciones.

Los cambios de aplicaciones o de versiones pueden producir situaciones de falta de integración y de incompatibilidad entre los nuevos productos instalados y los existentes con anterioridad. Prácticamente la totalidad de las nuevas versiones son capaces de manejar los formatos utilizados por versiones anteriores, pero no siempre ocurre en sentido contrario.

El equipo auditor determinará la existencia de procedimientos formalmente establecidos para la autorización, aprobación, adquisición de nuevas aplicaciones y cambios de versiones. Asimismo, comprobará que las aplicaciones instaladas y los cambios de versiones han seguido todos los trámites exigidos en el procedimiento establecido.

También se ocupará de determinar si se han analizado los problemas de integración y las incompatibilidades que pueden plantear los nuevos productos previamente a su implantación; si se ha establecido algún plan para la formación de los usuarios finales que vayan a utilizar estos nuevos productos; y si los encargados de mantenerlos han adquirido los conocimientos suficientes para que los cambios que van a producirse no impacten negativamente en el funcionamiento de la organización.

Determinar si los usuarios cuentan con suficiente formación y la documentación de apoyo necesaria para desarrollar sus tareas de un modo eficaz y eficiente.

Un conocimiento deficiente de las funcionalidades de las aplicaciones por parte de los usuarios finales o de los encargados del mantenimiento, puede ocasionar pérdida de eficacia y eficiencia en la utilización de las mismas. No debemos olvidar que carecer de los conocimientos necesarios puede ser debido tanto a que los usuarios no han sido formados como a que no han aprovechado debidamente los cursos de formación recibidos.

El equipo auditor determinará la existencia de un plan de formación para garantizar que todo el personal conoce los productos que tiene que utilizar, incluyendo las nuevas aplicaciones y las versiones instaladas. También comprobará que tras la realización de los cursos, se aplica algún mecanismo para determinar el aprovechamiento conseguido por los alumnos, y si se entrega a los usuarios documentación básica de la operativa del producto, o si pueden acceder a ella fácilmente en caso de necesidad.

Igualmente, comprobará que los empleados utilizan las posibilidades que ofrece el producto y no simulan procedimientos utilizados en versiones previas o en aplicaciones utilizadas con anterioridad. Asimismo, evaluará los mecanismos y circuitos establecidos para solucionar las dudas y problemas planteados, determinando si la responsabilidad de solucionarlos corresponde a un equipo de soporte común a toda la organización, o bien, recae sobre el propio departamento.

Determinar si el sistema existente se ajusta a las necesidades reales de la organización.

La existencia de equipos obsoletos o infrautilizados puede ocasionar situaciones que, por mala distribución de los equipos a las necesidades de la organización, repercutan en el correcto funcionamiento de la misma.

El equipo auditor valorará el uso que se realiza de los equipos existentes, elaborando una relación de aquellos computadores que no se encuentren operativos. Asimismo, revisará las actividades que se ejecutan en cada equipo, determinando aquellos puestos de trabajo que, por las tareas que desempeñan, necesitan ser automatizados o precisan actualizar los equipos existentes; así como aquellos puestos que, debido a su escasa actividad, se encuentran sobredimensionados.

A la vista de los resultados obtenidos, elaborará una relación con recomendaciones sobre descatalogación de productos obsoletos, redistribuciones y adquisiciones de nuevos equipos y aplicaciones.

9.2.2. Seguridad

Determinar si existen garantías suficientes para proteger los accesos no autorizados a la información reservada de la empresa y la integridad de la misma.

Las aplicaciones ofimáticas gestionan información reservada como agendas de contactos, informes sobre temas confidenciales, estadísticas obtenidas con información extraída de la base de datos corporativa, etc. Los accesos no autorizados o las inconsistencias en este tipo de información pueden comprometer el buen funcionamiento de la organización.

Al margen de los requerimientos que, en un futuro, disponga el reglamento de seguridad en desarrollo del artículo 9 de la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter personal, pendiente de aprobación, la organización ha de establecer las políticas y procedimientos de seguridad necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada.

Las funcionalidades en materia de seguridad de las aplicaciones ofimáticas y los sistemas operativos de los computadores personales se han incrementado significativamente en los últimos años, ofreciendo un nivel de seguridad aceptable. No obstante, garantizar el cumplimiento de algunas de las medidas de seguridad expuestas a continuación exigirá recurrir a la adquisición de paquetes adicionales y, sobre todo, la adopción de medidas organizativas.

El equipo auditor examinará la documentación en materia de seguridad existente en la organización y comprobará que han sido definidos, al menos, procedimientos de clasificación de la información, control de acceso, identificación y autenticación, gestión de soportes, gestión de incidencias y controles de auditoría. Con posterioridad, pasará a comprobar si las medidas de seguridad definidas se encuentran realmente operativas.

En primer lugar, determinará si el procedimiento de clasificación de la información establecido ha sido elaborado atendiendo a la sensibilidad e importancia de la misma, y comprobará que toda la información se ha clasificado en función de los criterios establecidos.

Tras verificar que las funciones, obligaciones y responsabilidades, en materia de seguridad, de cada puesto de trabajo están claramente definidas y documentadas, comprobará que se han adoptado las medidas necesarias para que todo el personal conozca tanto aquellas que afecten al desempeño de su actividad como las responsabilidades en que pudiera incurrir en caso de incumplirlas.

Examinando la relación actualizada de usuarios del sistema y de derechos de acceso establecidos, comprobará que cada usuario tiene autorización para acceder únicamente a aquellos datos y recursos informáticos que precisa para el desarrollo de sus funciones.

El equipo auditor deberá comprobar si se han establecido procedimientos de identificación y autenticación para el acceso al sistema. Cuando el mecanismo de autenticación se base en contraseñas, determinará si el procedimiento de creación, almacenamiento, distribución y modificación de las mismas garantiza su confidencialidad. También, determinará si los usuarios desconectan sus puestos de trabajo al finalizar la jornada, y si existe algún mecanismo que produzca la desconexión automática de un usuario tras un período de inactividad determinado, o bien, que precise introducir una contraseña para poder reanudar el trabajo.

En ningún caso olvidará verificar el cumplimiento de los procedimientos establecidos para solicitar nuevos accesos o modificaciones sobre los derechos definidos para un usuario, y que, exclusivamente, el personal autorizado se ocupará de conceder, alterar o anular los derechos de acceso sobre los datos y recursos informáticos.

El equipo auditor analizará el procedimiento de notificación y gestión de incidencias definido en la autorización, determinando cuáles son las incidencias registradas, el momento en que se producen, la persona que realiza la notificación, a quién le son comunicadas, el responsable asignado para revisarla y corregirla, los efectos producidos y las actuaciones que ha provocado.

Finalmente, comprobará que todos los soportes informáticos permiten identificar la información que contienen, son inventariados y se almacenan en un lugar con acceso restringido únicamente al personal autorizado. Igualmente, verificará que la salida de soportes informáticos fuera de la organización es debidamente autorizada.

Determinar si el procedimiento de generación de las copias de respaldo es fiable y garantiza la recuperación de la información en caso de necesidad.

La información generada por el sistema debe estar disponible en todo momento. La no disponibilidad de datos, especialmente de aquellos procedimientos críticos para la organización, además de las consabidas pérdidas económicas, podría llevar, en el extremo, a la paralización del departamento.

El equipo auditor examinará el procedimiento de copias de seguridad seguido en la organización, verificando la suficiencia de la periodicidad, la correcta asignación de responsabilidades y el adecuado almacenamiento de los soportes.

En primer lugar, comprobará que la responsabilidad de realizar las copias de seguridad está asignada y que cada responsable realiza copias de la información que se encuentra bajo su responsabilidad, de tal forma que todos los datos son salvaguardados. A continuación, verificará la existencia de un inventario de los soportes que contienen las copias de seguridad y de la información salvaguardada.

Posteriormente, determinará si la seguridad implementada para garantizar la confidencialidad e integridad de las copias de salvaguarda ofrece garantías equivalentes a las definidas para la información que contienen, tanto en los soportes que se mantienen en los locales de la empresa como en aquellos que se trasladan a una ubicación externa.

Finalmente, controlará la eficacia del procedimiento definido para la recuperación de las copias de seguridad, determinando si los soportes contienen la información que está previsto que contengan, y si es posible la recuperación de la misma, de forma que el resultado final sea un fiel reflejo de la situación anterior.

Determinar si está garantizado el funcionamiento ininterrumpido de aquellas aplicaciones cuya caída podría suponer pérdidas de integridad de la información y aplicaciones.

En las organizaciones se desarrollan procesos en los que una caída de tensión podría ocasionar pérdidas de integridad de la información y aplicaciones manejadas, en ocasiones irrecuperables.

El equipo auditor determinará la existencia de sistemas de alimentación ininterrumpida, y si éstos cubren el funcionamiento de aquellos equipos en los que se ejecutan procesos cuya interrupción podría ocasionar graves repercusiones.

Asimismo, debe ocuparse de similar una caída de tensión, verificar si los equipos de alimentación ininterrumpida entran en funcionamiento y comprobar si el tiempo de actividad proporcionado por el sistema de alimentación ininterrumpida es suficiente, para la finalización de los procesos críticos y la desconexión del sistema.

Determinar el grado de exposición ante la posibilidad de intrusión de virus.

Los costes derivados de la intrusión de virus informáticos se han multiplicado en los últimos años: pérdida de la información y empleo de recursos y tiempo para restablecer el sistema, llegando en algunos casos a la paralización temporal del departamento.

El equipo auditor analizará la protección establecida en cada uno de los puntos del sistema por los que podrían introducirse virus: disqueteras, módem, accesos a

redes, etc.; y revisará la normativa para la instalación y actualización periódica de productos antivirus, prestando especial atención a aquellos casos en que la información manejada puede ser crítica para el funcionamiento de la organización.

Asimismo, analizará la configuración de los equipos y la instalación de programas que permitan detectar la existencia de virus, evitar su irtrusión en el sistema y eliminar aquellos que se hayan introducido.

En caso de que detectara algún virus en alguno de los equipos, el equipo auditor informará inmediatamente al responsable autorizado sugiriendo las medidas que estime pertinentes para evitar la propagación del mismo.

9.2.3. Normativa vigente

Determinar si en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en la Ley Orgánica 51/1999, de protección de datos de carácter personal (LOPD).

La LOPD establece una serie de principios y derechos de los ciudadanos en relación con sus datos de carácter personal incluidos en archivos automatizados.

Además, aquellos afectados que sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la LOPD, pueden reclamar la correspondiente indemnización ante los Tribunales de Justicia.

El equipo auditor deberá comprobar la existencia de un inventario de archivos que manejan datos de carácter personal y constatar que este inventario contiene todos los archivos gestionados en los entornos ofimáticos. Aunque en la mayoría de los casos estos entornos gestionan archivos que se constituyen como meramente auxiliares de otros existentes en la organización, en algún supuesto podrían tratarse datos personales que no se encontraran incluidos en ninguno de los archivos o bases de datos corporativas. La tarea del equipo auditor consistirá en determinar que los archivos que gestionan datos personales en entornos ofimáticos se encuentran bajo control y que han sido notificados al Registro General de la Agencia de Protección de Datos.

Los controles para verificar que los archivos existentes cumplen los preceptos establecidos en la LOPD no pueden excluirse de los procedimientos generales para toda la organización, excediendo, por consiguiente, del alcance del presente capítulo.

Baste recordar que el equipo auditor deberá comprobar la adecuación y validez de los procedimientos establecidos en la organización para garantizar el cumplimiento de los principios (calidad de los datos, información en la recogida, consentimiento del afectado para el tratamiento y la cesión, seguridad de datos, deber de secreto, etc.) y derechos (acceso, rectificación y cancelación) recogidos en la mencionada Ley.

Determinar si en el entorno ofimático se producen situaciones que puedan suponer infracciones a lo dispuesto en el Real Decreto Legislativo 1/1996, de 12 de abril, sobre la propiedad intelectual.

La mayoría de las copias ilegales utilizadas en las organizaciones corresponden a aplicaciones microinformáticas, en especial a aplicaciones ofimáticas. Este hecho puede provocar que aquellos afectados que sufran algún tipo de daño o perjuicio como consecuencia del incumplimiento de lo dispuesto en el Real Decreto Legislativo sobre la propiedad intelectual, presenten reclamaciones ante los Tribunales de Justicia que puedan derivar incluso causas criminales.

El equipo auditor deberá elaborar una relación exhaustiva de las aplicaciones residentes en equipos ofimáticos, que precisen licencia para su utilización. Esta relación se contrastará con el inventario de la organización para verificar que coinciden, y, en caso contrario, deberá averiguar cuáles son las copias ilegalmente utilizadas.

El equipo auditor se ocupará de verificar la definición y aplicación de medidas con carácter preventivo, tales como: la existencia de un régimen disciplinario que sea conocido por todos los empleados, la inhabilitación de las disqueteras y otros puertos de entrada y salida, y las limitaciones en el acceso a redes externas a la organización.

Igualmente, verificará las medidas detectivas existentes tales como: la asignación de responsables que se ocupen de efectuar exploraciones periódicas de las aplicaciones contenidas en cada computador y de analizar los niveles de utilización de las aplicaciones compartidas en la red.

Finalmente, comprobará la definición de medidas correctivas tales como: la eliminación de las copias ilegales que se localicen; los procedimientos para determinar el modo de intrusión y, en consecuencia, definir medidas para evitar que esta situación se repita; y adoptar las acciones disciplinarias pertinentes.

9.3. CONCLUSIONES

La mayoría de las aplicaciones de auditoría en entornos ofimáticos no difiere sustancialmente de las actuaciones necesarias para auditar sistemas centralizados. En ambos casos, la experiencia profesional del auditor supone el elemento fundamental

para la selección de los controles objeto de verificación y la adecuación de los mismos al sistema a auditar, teniendo presente en todo momento que la evolución sufrida por los entornos ofimáticos exigirá conocimientos específicos y técnicas novedosas.

La presentación de los controles muestra una secuencia en las actuaciones a realizar en la auditoría. Como paso previo al inicio de la auditoría propiamente dicha, el equipo auditor debe comprender en profundidad el funcionamiento del sistema y del uso que se hace del mismo, así como analizar los riesgos a los que está expuesto. Para cada uno de los aspectos a revisar, debe comprobar la definición de controles preventivos, detectivos y correctivos. Acto seguido, debe verificar si los controles definidos son realmente aplicados por los usuarios durante el desarrollo de sus actividades. Finalmente, deberá emitir una valoración acerca de la suficiencia y adecuación de los controles definidos e implantados para la prevención de los riesgos a los que se encuentra sometido el sistema.

Durante la exposición de los controles, nos hemos referido con frecuencia a documentos, procedimientos y políticas de actuación definidas e implantadas en la organización; sin embargo, es un hecho habitual que algunos de ellos no hayan sido definidos. Es labor del auditor, además de constatar tales deficiencias en su informe, participar en la elaboración de los mismos. Es decir, el auditor debe ocuparse de detectar las deficiencias presentes en el funcionamiento de la organización, pero, además, debe contribuir con su experiencia y conocimientos en la elaboración de los procedimientos y recomendaciones que permitan subsanarlas.

Como consideración final, recomendar que la auditoría ofimática no debe realizarse de un modo independiente. Nos parece más adecuada la integración de los controles ofimáticos dentro de un plan de auditoría de mayor alcance, principalmente por motivos de eficacia y eficiencia en la preparación y desarrollo de la misma.

9.4. LECTURAS RECOMENDADAS

Thomas, A. J., Douglas, I. J. *Auditoría informática.* Paraninfo, 1987.

Ron Weber *EDP auditing. Conceptual foundations and practice.* McGraw Hill, 1988.

Kraemer, K. L., King, J. L. *Computer-Based systems for Cooperative Work and Group Decisions Making.* ACM Comp. Surveys, vol. 20, n.º 2, junio 1988, pp. 115-146.

Auerbach Publicactions. *EDP Auditing.* 1993. Capítulos 74-01-01, 74-01-05, 74-0174-01-30, 74-01-65, 74-01-71 y 75-01-15.

Schill, Alexander. *Cooperative office systems: Concepts.* Prentice Hall, 1995.

9.5. CUESTIONES DE REPASO

1. ¿Qué elementos de un sistema informático se contemplan dentro de la ofimática?

2. Explique el paradigma de escritorio virtual.

3. ¿Qué distingue la auditoría de ofimática de la de otros entornos informáticos?

4. Analice las repercusiones que puede tener en una empresa un inventario poco fiable bajo las perspectivas de la economía, la eficacia y la eficiencia.

5. ¿Cómo debería ser un procedimiento para la realización de cambios de versiones de paquetes ofimáticos?

6. Calcule el coste real de un computador personal para una empresa (tenga en cuenta el hardware, software, mantenimiento, formación, etc.).

7. ¿Qué mecanismos de seguridad de los que conoce se pueden aplicar a los computadores personales?

8. Escriba un procedimiento para la utilización de equipos ofimáticos que pueda ser entendido por usuarios finales.

9. Analice las principales "vacunas" existentes en el mercado contra virus que afecten a computadores personales.

10. ¿Qué consideraciones al entorno ofimático se encuentran en la LOPD?

CAPÍTULO 10

AUDITORÍA DE LA DIRECCIÓN

Juan Miguel Ramos Escobosa

10.1. INTRODUCCIÓN

Siempre se ha dicho que una organización es un reflejo de las características de su dirección. Los modos y maneras de actuar de aquélla están influenciados por la filosofía y la personalidad de la segunda.

Obviamente, los departamentos informáticos no son una excepción. Aunque puede argumentarse con razón, que, a su vez, estos departamentos están integrados en organizaciones mayores y que, por tanto, son destinatarios de un sinfín de estímulos de las mismas, qué duda cabe de que, dado el ámbito tecnológico tan particular de la informática, la principal influencia que dichos departamentos reciben viene inducida desde la propia dirección de informática. En cualquier caso, es en lo que se centra este capítulo: en la auditoría de la Dirección entendida como *gestión* (en el resto del capítulo se intercambiarán los dos términos) de la Informática.

Las enormes sumas que las empresas dedican a las tecnologías de la información en un crecimiento del que no se vislumbra el final y la absoluta dependencia de las mismas al uso correcto de dicha tecnología hacen muy necesaria una evaluación independiente de la función que la gestiona. Ello constituye, de hecho, la razón principal de este libro. La dirección de informática no debe quedar fuera: es una pieza clave del engranaje.

Sin entrar en discusiones profundas sobre el alcance y significado detrás del verbo *dirigir* (no es el objetivo de este libro y existen multitud de plumas más preparadas que la mía para disertar adecuadamente sobre este apartado), de una

manera general, se podría decir que algunas de las actividades básicas de todo proceso de dirección son:

- Planificar
- Organizar
- Coordinar
- Controlar

10.2. PLANIFICAR

En grandes líneas, se trata de prever la utilización de las tecnologías de la información en la empresa. Existen varios tipos de planes informáticos. El principal, y origen de todos los demás, lo constituye el Plan Estratégico de Sistemas de Información.

10.2.1. Plan Estratégico de Sistemas de Información

Es el marco básico de actuación de los Sistemas de Información en la empresa. Debe asegurar el alineamiento de los mismos con los objetivos de la propia empresa.

Desgraciadamente, la transformación de los objetivos de la empresa en objetivos informáticos no es siempre una tarea fácil. Mucho se ha escrito sobre el contenido y las ventajas e inconvenientes de las diversas metodologías de realización de este tipo de planes. No se trata en estos breves apuntes de terciar en dicha polémica. El lector encontrará abundante bibliografía sobre la materia. El auditor deberá evaluar si tales metodologías se están utilizando y/o pueden ser de utilidad para su empresa.

Estrictamente hablando, estos planes no son responsabilidad exclusiva de la Dirección de Informática. Su aprobación final probablemente incumbe a otros estamentos de la empresa: Comité de Informática (ver más abajo) e incluso en último término de la Dirección General. Sin embargo, la Dirección de Informática debe ser el permanente impulsor de una planificación de Sistemas de Información adecuada y a tiempo.

Aunque se suele definir la vigencia de un plan estratégico como de 3 a 5 años, de hecho tal plazo es muy dependiente del entorno en el que se mueve la empresa. Hay muchos factores que influyen: la cultura de la propia empresa, el sector de actividad, es decir, si la empresa se encuentra en un sector en el que el uso adecuado de la tecnología informática es un factor estratégico –el sector financiero, por ejemplo–, las acciones de la competencia, etc. Cada empresa tiene su equilibrio natural y el auditor deberá evaluar si los plazos en uso en su empresa son los adecuados.

En cualquier caso, independientemente de la metodología, los plazos y las acciones concretas llevadas a cabo, debe existir un proceso, con participación activa de los usuarios, que regularmente elabore planes estratégicos de Sistemas de Información a largo plazo, cualquiera que sea ese *largo*, y el auditor deberá evaluar su adecuación.

Guía de auditoría

El auditor deberá examinar el proceso de planificación de sistemas de información y evaluar si razonablemente se cumplen los objetivos para el mismo. Entre otros aspectos, deberá evaluar si:

- Durante el proceso de planificación se presta adecuada atención al plan estratégico de la empresa, se establecen mecanismos de sincronización entre sus grandes hitos y los proyectos informáticos asociados y se tienen en cuenta aspectos como cambios organizativos, entorno legislativo, evolución tecnológica, organización informática, recursos, etc., y sus impactos están adecuadamente recogidos en el Plan Estratégico de Sistemas de Información. Igualmente, el auditor deberá evaluar si se presta adecuada consideración a nuevas tecnologías informáticas, siempre desde el punto de vista de su contribución a los fines de la empresa y no como experimentación tecnológica.

- Las tareas y actividades presentes en el Plan tienen la correspondiente y adecuada asignación de recursos para poder llevarlas a cabo. Asimismo, si tienen plazos de consecución realistas en función de la situación actual de la empresa, de la organización informática, del estado de la tecnología, etc.

Entre las acciones a realizar, se pueden describir:

- Lectura de actas de sesiones del Comité de Informática dedicadas a la planificación estratégica.
- Identificación y lectura de los documentos intermedios prescritos por la metodología de planificación.
- Lectura y comprensión detallada del Plan e identificación de las consideraciones incluidas en el mismo sobre los objetivos empresariales, cambios organizativos, evolución tecnológica, plazos y niveles de recursos, etc.
- Realización de entrevistas al Director de Informática y a otros miembros del Comité de Informática participantes en el proceso de elaboración del Plan Estratégico. Igualmente, realización de entrevistas a representantes de los usuarios con el fin de evaluar su grado de participación y sintonía con el contenido del Plan.

- Identificación y comprensión de los mecanismos existentes de seguimiento y actualización del Plan y de su relación con la evolución de la empresa.

10.2.2. Otros planes relacionados

Como se ha comentado más arriba, normalmente, deben existir otros planes informáticos, todos ellos nacidos al amparo del Plan Estratégico. Entre otros, los más habituales suelen ser:

- Plan operativo anual
- Plan de dirección tecnológica
- Plan de arquitectura de la información
- Plan de recuperación ante desastres

Algunos de ellos (Plan tecnológico, Plan de arquitectura) aparecen a veces integrados en el propio Plan Estratégico. En este capítulo, se tratarán sólo dos de estos planes, los más comunes y que, además, siempre tienen vida propia: Plan operativo y Plan de recuperación.

Plan operativo anual

El Plan operativo se establece al comienzo de cada ejercicio y es el que marca las pautas a seguir durante el mismo. Debe estar, obviamente, alineado con el Plan Estratégico. Asimismo, debe estar precedido de una recogida de necesidades de los usuarios.

El Plan operativo de Sistemas de Información describe las actividades a realizar durante el siguiente ejercicio natural. Entre otros aspectos, debe señalar los sistemas de información a desarrollar, los cambios tecnológicos previstos, los recursos y los plazos necesarios, etc.

El auditor deberá evaluar la existencia del Plan y su nivel de calidad. Deberá estudiar su alineamiento con el Plan Estratégico, su grado de atención a las necesidades de los usuarios, sus previsiones de los recursos necesarios para llevar a cabo el Plan, etc. Deberá analizar si los plazos descritos son realistas teniendo en cuenta, entre otras cosas, las experiencias anteriores en la empresa, etc.

Plan de recuperación ante desastres

Una instalación informática puede verse afectada por desastres de variada naturaleza: incendio, inundación, fallo de algún componente crítico de hardware, robo, sabotaje, acto de terrorismo, etc., que tengan como consecuencia inmediata la indisponibilidad de un servicio informático adecuado. La Dirección debe prever esta posibilidad y, por tanto, planificar para hacerle frente.

En otro capítulo de este libro se cubren los aspectos relativos a la auditoría de un Plan de recuperación ante desastres. Sin embargo, se quiere señalar aquí que dicho Plan es responsabilidad directa de la Dirección y no del responsable de la seguridad.

10.3. ORGANIZAR Y COORDINAR

El proceso de organizar sirve para estructurar los recursos, los flujos de información y los controles que permitan alcanzar los objetivos marcados durante la planificación.

10.3.1. Comité de Informática

Una de las acusaciones más comúnmente lanzadas contra la informática y los informáticos es la falta de comunicación y entendimiento que se establece entre el departamento de informática en la empresa y el resto de la misma. El Comité de Informática es el primer lugar de encuentro dentro de la empresa de los informáticos y sus usuarios: es el lugar en el que se debaten los grandes asuntos de la informática que afectan a toda la empresa y permite a los usuarios conocer las necesidades del conjunto de la organización –no sólo las de su área– y participar en la fijación de prioridades. Se evitan así acusaciones de favoritismo entre unas áreas y otras, en cuanto al trato recibido de informática, y, en definitiva, se atiende a la mejor utilización de los recursos informáticos, tradicionalmente escasos.

Si bien estrictamente el nombramiento, la fijación de funciones, etc. del Comité de Informática no son responsabilidades directas de la Dirección de Informática, sino de la Dirección General fundamentalmente, la Dirección de Informática se ha de convertir en el principal impulsor de la existencia de dicho Comité.

Aunque no existe regla fija, el Comité debería estar formado por pocas personas y presidido por el director más senior, dentro de la empresa, responsable en último término de las tecnologías de la información. El Director de Informática debería actuar como secretario del Comité y las grandes áreas usuarias deberían estar representadas al nivel de sus directores más senior. Asimismo, el director de Auditoría Interna debería ser miembro del Comité. Otras personas de la organización

también pueden integrarse en el Comité como miembros temporales cuando se trate asuntos de su incumbencia o de su especialidad.

Se ha escrito mucho sobre las funciones que debe realizar un Comité de Informática y parece existir un cierto consenso en, al menos, los siguientes aspectos:

- Aprobación del Plan Estratégico de Sistemas de Información.
- Aprobación de las grandes inversiones en tecnología de la información.
- Fijación de prioridades entre los grandes proyectos informáticos.
- Vehículo de discusión entre la Informática y sus usuarios.
- Vigila y realiza el seguimiento de la actividad del Departamento de Informática.

Guía de auditoría

Al tratarse del máximo órgano decisorio sobre el papel de las tecnologías de la información en la empresa, ninguna auditoría de la Dirección de Informática debería soslayar su revisión. El auditor deberá asegurar que el Comité de Informática existe y cumple su papel adecuadamente.

Para ello, deberá conocer, en primer lugar, las funciones encomendadas al Comité. En este punto, difieren las acciones concretas que el auditor deberá emprender ya que dependerán, en gran manera, del grado de Normalización imperante en la empresa. En unos casos, existirá una normativa interna explicando los objetivos, responsabilidades, componentes, etc. del Comité y en otros no existirá nada de eso y no habrá más que reuniones aperiódicas del mismo.

Entre las acciones a realizar, figuran:

- Lectura de la normativa interna, si la hubiera, para conocer las funciones que debería cumplir el Comité de Informática.
- Entrevistas a miembros destacados del Comité con el fin de conocer las funciones que en la práctica realiza dicho Comité.
- Entrevistas a los representantes de los usuarios, miembros del Comité, para conocer si entienden y están de acuerdo con su papel en el mismo.

Una vez establecida la existencia del Comité de Informática, habrá que evaluar la adecuación de las funciones que realiza. Para ello, el auditor, mediante un conjunto de entrevistas, lecturas de documentación interna del Comité, etc., deberá establecer un juicio sobre la validez, adecuación, etc. de las actuaciones del Comité. Uno de los

aspectos, fundamentales que deberá revisar es el que hace referencia a la presencia y participación efectiva de las áreas usuarias.

Entre las acciones a realizar, figuran:

Lectura de las actas del Comité y entrevistas a los miembros del mismo, con especial incidencia en los representantes de los usuarios para comprobar que:

- El Comité cumple efectivamente con las funciones enunciadas más arriba.
- Los acuerdos son tomados correctamente y los puntos de vista de los representantes de los usuarios son tenidos en cuenta.

10.3.2. Posición del Departamento de Informática en la empresa

El segundo aspecto importante a tener en cuenta a la hora de evaluar el papel de la informática en la empresa, es la ubicación del Departamento de Informática en la estructura organizativa general de la misma. El Departamento debería estar suficientemente alto en la jerarquía y contar con masa crítica suficiente para disponer de autoridad e independencia frente a los departamentos usuarios.

Tradicionalmente, la informatización en las empresas comenzó por el departamento financiero o de administración y, por tanto, el esquema tradicional era encontrar al departamento de informática integrado dentro del financiero o administrativo. Hoy en día, la informática da soporte a un conjunto mucho mayor de áreas empresariales y, por ello, cada vez es más habitual encontrar a departamentos de informática dependiendo directamente de Dirección General. Incluso, en las grandes organizaciones, el Director de Informática es miembro de derecho del Comité de Dirección u órgano semejante. Siempre que el departamento de informática esté integrado en algún departamento usuario, pueden surgir dudas razonables sobre su ecuanimidad a la hora de atender las peticiones del resto de departamentos de la empresa.

Una vez más, estrictamente hablando, la posición del Departamento de Informática no incumbe su Dirección sino a otros estamentos empresariales, probablemente, la Dirección General. Sin embargo, se trae a colación en este capítulo, porque el auditor debe evaluar si las necesidades de los diferentes departamentos de la empresa son tratadas equitativamente por Informática y no existe un sesgo demasiado alto hacia un departamento de la misma. Si esto último ocurriera, una de las primeras razones para ello puede ser la ubicación incorrecta de dicho Departamento.

Guía de auditoría

El auditor deberá revisar el emplazamiento organizativo del Departamento de Informática y evaluar su independencia frente a departamentos usuarios. Para este proceso, será muy útil realizar entrevistas con el Director de Informática y directores de algunos departamentos usuarios para conocer su percepción sobre el grado de independencia y atención del Departamento de Informática.

10.3.3. Descripción de funciones y responsabilidades del Departamento de Informática. Segregación de funciones

Es necesario que las grandes unidades organizativas dentro del Departamento de Informática tengan sus funciones descritas y sus responsabilidades claramente delimitadas y documentadas. Igualmente, es necesario que este conocimiento se extienda a todo el personal perteneciente a Informática: todos ellos deben conocer sus funciones y responsabilidades en relación con los sistemas de información. Y todo ello es una labor que compete, en gran medida, a la Dirección de Informática.

Por otro lado, es de todo punto esencial para tener un entorno controlado que exista una división de funciones y responsabilidades. La filosofía básica que debe orientar esta separación de papeles es impedir que un solo individuo pueda trastornar un proceso crítico. Además, se debería asegurar que el personal de Informática actúa únicamente dentro de la descripción de las funciones existente para su puesto de trabajo concreto.

En particular, se debería asegurar la segregación entre las funciones de desarrollo de sistemas de información, la de producción o explotación y los departamentos de usuarios. Además, la función de administración de la seguridad debería estar claramente separada de la de producción.

Aseguramiento de la Calidad

La calidad de los servicios ofrecidos por el Departamento de Informática debe estar asegurada mediante el establecimiento de una función organizativa de Aseguramiento de la Calidad. Cada vez más hoy en día, se asiste, en las *organizaciones informáticas evolucionadas, a la aparición de esta función de control* de calidad de los servicios informáticos, a imagen y semejanza de las organizaciones en el mundo industrial. Esta función de control ha de ser independiente de la actividad diaria del departamento y ha de depender directamente de la Dirección de Informática.

Es muy importante que esta función, de relativa nueva aparición en el mundo de las organizaciones informáticas, tenga el total respaldo de la Dirección y sea percibido así por el resto del Departamento.

Guía de auditoría

No es propósito de este capítulo describir las funciones de un departamento de informática. Ello se describe en otros capítulos de este libro, además de que existe una amplísima bibliografía sobre la materia. El aspecto fundamental que queremos resaltar aquí es que el auditor deberá comprobar que las descripciones están documentadas y son actuales y que las unidades organizativas informáticas las comprenden y desarrollan su labor de acuerdo a las mismas.

Entre las tareas que el auditor podrá realizar, figuran:

- Examen del organigrama del Departamento de Informática e identificación de las grandes unidades organizativas.
- Revisión de la documentación existente para conocer la descripción de las funciones y responsabilidades.
- Realización de entrevistas a los directores de cada una de las grandes unidades organizativas para determinar su conocimiento de las responsabilidades de su unidad y que éstas responden a las descripciones existentes en la documentación correspondiente.
- Examen de las descripciones de las funciones para evaluar si existe adecuada segregación de funciones, incluyendo la separación entre desarrollo de sistemas de información, producción y departamentos usuarios. Igualmente, será menester evaluar la independencia de la función de seguridad.
- Observación de las actividades del personal del Departamento para analizar, en la práctica, las funciones realizadas, la segregación entre las mismas y el grado de cumplimiento con la documentación analizada.

Aseguramiento de la Calidad

El auditor deberá evaluar la independencia de la función frente al resto de áreas operativas del Departamento de Informática, su dotación de recursos humanos, la experiencia de los mismos, la existencia de métodos y procedimientos formales de

actuación, las posibilidades reales de realizar su trabajo, el contenido de los informes elaborados por la función, etc.

Entre las acciones a llevar a cabo, se pueden considerar:

- Conocimiento de la posición de la Función en el organigrama del Departamento de Informática.

- Análisis del grado de cumplimiento de las actividades del Departamento en relación con las políticas, estándares y procedimientos existentes tanto generales del Departamento como específicos de sus funciones organizativas. De particular importancia es el grado de cumplimiento de la metodología del ciclo de vida de los sistemas de información, de los procedimientos que gobiernan la explotación del computador y de la investigación de la calidad de los datos que se envían a los usuarios.

- Revisión de algunos informes emitidos por la Función con el fin de evaluar si su estructura y contenido son adecuados. Analizar la existencia de acciones de seguimiento basadas en dichos informes.

10.3.4. Estándares de funcionamiento y procedimientos. Descripción de los puestos de trabajo

Deben existir estándares de funcionamiento y procedimientos que gobiernen la actividad del Departamento de Informática por un lado, y sus relaciones con los departamentos usuarios por otro. Estos estándares son el vehículo ideal para transmitir al personal de Informática la filosofía, mentalidad y actitud hacia los controles necesarios con la finalidad de crear y mantener un entorno controlado para la vida de los sistemas de información de la empresa.

De particular importancia son los aspectos relacionados con la adquisición de equipos o material para el Departamento, con el diseño y el desarrollo/modificación de sistemas de información y con la producción o explotación.

Además, dichos estándares y procedimientos deberían estar documentados, actualizados y ser comunicados adecuadamente a todos los departamentos afectados. La Dirección de Informática debe promover la adopción de estándares y procedimientos y dar ejemplo de su uso.

Por otro lado, deben existir documentadas descripciones de los puestos de trabajo dentro de Informática delimitando claramente la autoridad y responsabilidad en cada

caso. Las descripciones deberían incluir los conocimientos técnicos y/o experiencia necesarios para cada puesto de trabajo.

Guía de auditoría

El auditor deberá evaluar la existencia de estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados.

Entre las acciones a realizar, se pueden citar:

- Evaluación del proceso por el que los estándares, procedimientos y puestos de trabajo son desarrollados, aprobados, distribuidos y actualizados.
- Revisión de los estándares y procedimientos existentes para evaluar si transmiten y promueven una filosofía adecuada de control. Evaluación de su adecuación, grado de actualización, y nivel de cobertura de las actividades informáticas y de las relaciones con los departamentos usuarios.
- Revisión de las descripciones de los puestos de trabajo para evaluar si reflejan las actividades realizadas en la práctica.

10.3.5. Gestión de recursos humanos: selección, evaluación del desempeño, formación, promoción, finalización

La gestión de los recursos humanos es uno de los elementos críticos en la estructura general informática. La calidad de los recursos humanos influye directamente en localidad de los sistemas de información producidos, mantenidos y operados por el Departamento de Informática. Además, parte de los recursos humanos necesarios en una instalación informática son grandes expertos técnicos. Seleccionarlos, mantenerlos y motivarlos adecuadamente puede ser crucial para la buena marcha de la informática y su papel en la empresa.

Guía de auditoría

Entre otros aspectos, el auditor deberá evaluar que:

- La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad anteriores.

- El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos y responsabilidades específicas del puesto de trabajo.

- Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia, puesto de trabajo, responsabilidad y desarrollo futuro personal y tecnológico de la instalación. Se planifica la cobertura ordenada de estas necesidades y se lleva a la práctica.

- Existen procesos para la promoción del personal que tienen en cuenta su desempeño profesional.

- Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática.

Además, el auditor deberá evaluar que todos los aspectos anteriores están en línea con las políticas y procedimientos de la empresa.

Entre las acciones a realizar, se pueden citar:

- Conocimiento y evaluación de los procesos utilizados para cubrir vacantes en el Departamento de Informática, bien sea por promoción interna, búsqueda directa de personal externo, utilización de empresas de selección de personal o de trabajo temporal.

- Análisis de las cifras de rotación de personal, niveles de absentismo laboral y estadísticas de proyectos terminados fuera de presupuesto y de plazo. Si los números son anormales (muy altos), podrían constituir una señal de falta de liderazgo por parte de la Dirección de Informática y/o de motivación por parte del personal.

- Realización de entrevistas a personal del Departamento para determinar su conocimiento de las responsabilidades asociadas a su puesto de trabajo y de los estándares de rendimiento, y analizar si los resultados de sus evaluaciones de desempeño han sido comunicadas de una manera acorde con los procedimientos establecidos.

- Revisión del calendario de cursos, descripciones de los mismos, métodos y técnicas de enseñanza, para determinar que los cursos son consistentes con los conocimientos, experiencia, responsabilidades, etc. asignadas al personal y con la estrategia tecnológica marcada para los sistemas de información de la empresa.

- Revisión de los procedimientos para la finalización de contratos. Evaluar si dichos procedimientos prevén que los identificadores de usuario, passwords y prevén otros dispositivos necesarios para tener acceso a los locales y sistemas

informáticos son cancelados, devueltos, etc., con efectividad inmediata tras la finalización del contrato de un empleado.

10.3.6. Comunicación

Es necesario que exista una comunicación efectiva y eficiente entre la Dirección de Informática y el resto del personal del Departamento. Entre los aspectos que es importante comunicar se encuentran: actitud positiva hacia los controles, integridad, ética, cumplimiento de la normativa interna –entre otras, la de seguridad informática–, compromiso con la calidad, etc.

Guía de auditoría

El auditor deberá evaluar las características de la comunicación entre la Dirección y el personal de Informática. Para ello se podrá servir de tareas formales como las descritas hasta ahora y de otras, por ejemplo, a través de entrevistas informales con el personal del Departamento.

10.3.7. Gestión económica

Este apartado de las responsabilidades de la Dirección de Informática tiene varias facetas: presupuestación, adquisición de bienes y servicios y medida y reparto de costes.

10.3.7.1. Presupuestación

Como todo departamento de la empresa, el de Informática debe tener un presupuesto económico, normalmente en base anual. Los criterios sobre cuáles deben ser los componentes del mismo varían grandemente. Un ejemplo típico son los costes de las comunicaciones: en unos casos es el propio Departamento quien corre con ellos y, en otros casos, puede ocurrir que la política de la empresa indique que sean pagados por los departamentos usuarios. En otro ejemplo, también puede ocurrir que los terminales (pantallas e impresoras) sean costeados por los usuarios en vez de serlo por Informática. Sea cual sea la política seguida en la empresa, el Departamento de Informática debe seguirla para elaborar su presupuesto anual.

No vamos a entrar aquí en los diversos métodos existentes de presupuestación, pero el auditor deberá juzgar si son apropiados. Lo que sí debería darse en todo proceso de presupuestación de un Departamento de Informática es una previa petición de necesidades a los departamentos usuarios. Adicionalmente, el Departamento tendrá

sus propias necesidades: cambio o ampliación del computador o de los discos, instalación de un robot manejador de cartuchos, de una unidad de comunicaciones, etc. que se deberán integrar en el presupuesto. Lo más lógico es elaborar al mismo tiempo el presupuesto económico y el Plan operativo anual.

Guía de auditoría

El auditor deberá constatar la existencia de un presupuesto económico, de un proceso para elaborarlo –que incluya consideraciones de los usuarios– y aprobarlo, y que dicho proceso está en línea con las políticas y procedimientos de la empresa y con los planes estratégico y operativo del propio Departamento.

10.3.7.2. Adquisición de bienes y servicios

Los procedimientos que el Departamento de Informática siga para adquirir los bienes y servicios descritos en su plan operativo anual y/o que se demuestren necesarios a lo largo del ejercicio han de estar documentados y alineados con los procedimientos de compras del resto de la empresa. Aquí, la variedad es infinita, con lo que es imposible dar reglas fijas.

Guía de auditoría

Una auditoría de esta área no debe diferenciarse de una auditoría tradicional del proceso de compras de cualquier otra área de la empresa, con lo que el auditor deberá seguir básicamente las directrices y programas de trabajo de auditoría elaborados para este proceso.

10.3.7.3. Medida y reparto de costes

La Dirección de Informática debe en todo momento gestionar los costes asociados con la utilización de los recursos informáticos: humanos y tecnológicos. Y ello, obviamente, exige medirlos.

Un aspecto muy relacionado es el reparto de los costes del Departamento entre los usuarios. Esta medida no está implantada en todas las empresas y, además, tiene sus ventajas e inconvenientes que, también, se encuentran fuera del alcance de este libro. Normalmente, la existencia o ausencia de un sistema de este tipo suele estar muy asociada a la propia cultura de la empresa. En cualquier caso, es cierto que, de estar presente, se da en general, con mayor frecuencia, en grandes organizaciones con

grandes centros de proceso de datos centralizados. Es raro encontrar un sistema de reparto de costes en centros informáticos de departamentos.

Guía de auditoría

El reparto de costes suele ser un tema delicado. En realidad, el asunto espinoso suele ser el llamado precio de transferencia, o sea el coste interno que el Departamento de Informática repercute a los departamentos usuarios por los servicios que les presta.

El auditor deberá evaluar la conveniencia de que exista o no un sistema de reparto de costes informáticos y de que éste sea justo, incluya los conceptos adecuados y de que el precio de transferencia aplicado esté en línea o por debajo del disponible en el mercado.

Entre las acciones a llevar a cabo, se pueden mencionar:

- Realización de entrevistas a la dirección de los departamentos usuarios para evaluar su grado de comprensión de los componentes de coste utilizados en la fórmula de cálculo del precio de transferencia.

- Análisis de los componentes y criterios con los que está calculado el precio de transferencia para evaluar su ecuanimidad y consistencia, y acudir al mercado externo y a ofertas de centros de proceso de datos independientes para compararlas con dichos costes internos.

- Conocimiento de los diversos sistemas existentes en el Departamento para recoger y registrar la actividad del mismo (consumo de recursos de máquina, número de líneas impresas, horas de programación, de *help-desk*, etc.), para procesarla y obtener la información de costes y para presentarla de una manera apropiada.

10.3.8. Seguros

La Dirección de Informática debe tomar las medidas necesarias con el fin de tener suficiente cobertura de seguros para los sistemas informáticos. Aquí se incluyen no sólo las coberturas más tradicionales como la de los equipos (el hardware) o la de infidelidad de los empleados, sino también otro tipo de coberturas normalmente más asociadas a la repentina interrupción del servicio informático por causa de algún desastre. Estas coberturas amparan riesgos tales como la posible pérdida de negocio derivada de dicha interrupción, los costes asociados al hecho de tener que ofrecer servicio informático desde un lugar alternativo por no estar disponible el sitio primario

los costes asociados a la regeneración de datos por pérdida o inutilización de los datos originales, etc.

Guía de auditoría

El auditor deberá estudiar las pólizas de seguros y evaluar la cobertura existente, analizando si la empresa está suficientemente cubierta o existen huecos en dicha cobertura. Por ejemplo, algunas pólizas sólo cubren el reemplazo del equipo, pero no los otros costes mencionados, etc.

10.4. CONTROLAR

La tarea de *dirigir* no puede considerarse completa sin esta faceta que forma parte indisoluble de tal responsabilidad.

10.4.1. Control y seguimiento

Un aspecto común a todo lo que se ha dicho hasta el momento es la obligación de la Dirección de controlar y efectuar un seguimiento permanente de la distinta actividad del Departamento. Se ha de vigilar el desarrollo de los planes estratégico y operativo y de los proyectos que los desarrollan, la ejecución del presupuesto, la evolución de la cartera de peticiones de usuario pendientes, la evolución de los costes, los planes de formación, la evolución de la carga del computador y de los otros recursos (espacio en disco, comunicaciones, capacidad de las impresoras...), etc.

En esta labor, es muy conveniente que existan estándares de rendimiento con los que comparar las diversas tareas. Son aplicables a las diversas facetas de la actividad del Departamento: consumo de recursos del equipo, desarrollo, operaciones, etc.

Guía de auditoría

Entre las acciones a realizar, se pueden mencionar:

- Conocimiento y análisis de los procesos existentes en el Departamento para llevar a cabo el seguimiento y control. Evaluación de la periodicidad de los mismos. Analizar igualmente los procesos de represupuestación.

- Revisión de planes, proyectos, presupuestos de años anteriores y del actual para comprobar que son estudiados, que se analizan las desviaciones y que se toman las medidas correctoras necesarias.

10.4.2. Cumplimiento de la normativa legal

La Dirección de Informática debe controlar que la realización de sus actividades se lleva a cabo dentro del respeto a la normativa legal aplicable. En particular, se consideran fundamentales los relativos a la seguridad e higiene en el trabajo, normativa laboral y sindical, protección de datos personales, propiedad intelectual del software, requisitos definidos en la cobertura de seguros, contratos de comercio electrónico, transmisión de datos por líneas de comunicaciones, así como normativa emitida por órganos reguladores sectoriales.

Asimismo, deben existir procedimientos para vigilar y determinar permanentemente la legislación aplicable.

Guía de auditoría

El auditor deberá evaluar si la mencionada normativa aplicable se cumple.

Para ello, deberá, en primer lugar, entrevistarse con la Asesoría Jurídica de la empresa, la Dirección de Recursos Humanos y la Dirección de Informática con el fin de conocer dicha normativa.

A continuación, evaluará el cumplimiento de las normas, en particular en los aspectos más críticos mencionados más arriba. Si el auditor no es un técnico en los distintos aspectos legales, deberá buscar asesoramiento adecuado interno a la empresa o externo.

10.5. RESUMEN

La auditoría de la Dirección de Informática es una tarea difícil. Sin embargo, la contribución que dicha Dirección de Informática realiza (o debe realizar) al ambiente de control de las operaciones informáticas de una empresa es esencial. Desde un punto de vista de auditoría, la calidad del marco de controles impulsado e inspirado por la Dirección de Informática tiene una gran influencia sobre el probable comportamiento de los sistemas de información. Por parte del auditor, son más necesarias las capacidades, de evaluar la *gestión* que las capacidades técnicas muy profundas.

10.6. LECTURAS RECOMENDADAS

EDP Auditing, Conceptual Foundations and Practice. Ron Weber. McGraw-Hill, 1993.

Control Objectives for Information and Related Technology. Information Systems and Control Foundation, 1996.

Control Objectives. EDP Auditors Association, 1992.

Systems Auditability and Control. The Institute of Internal Auditors Research Foundation, 1991.

10.7. CUESTIONES DE REPASO

1. Descríbanse las actividades a realizar por un auditor para evaluar un plan estratégico de sistemas de información.

2. Descríbanse las funciones de un comité de informática. Elabórese una lista con las funciones empresariales que deberían estar representadas en dicho comité. ¿Qué objetivo tiene para los usuarios su presencia en el comité?

3. Descríbanse las ventajas de tener procedimientos. Elabórese un guión de lo que podrían ser procedimientos de: a) diseño de sistemas b) programación.

4. ¿Qué evidencias deberá buscar el auditor para poder evaluar si las necesidades de los usuarios son tenidas en cuenta adecuadamente?

5. Identifíquense las actividades incompatibles desde un punto de vista de control en un departamento de informática. Razónese.

6. ¿Qué ventajas de control aporta la existencia de la función de aseguramiento de la calidad?

7. Descríbanse los objetivos de control a ser evaluados por el auditor en el apartado de gestión de recursos humanos.

8. ¿Qué tareas debe realizar un auditor para evaluar el plan de formación del departamento de informática? ¿Cómo puede juzgar si dicho plan es acorde con los objetivos de la empresa?

9. Relaciónense las actividades a realizar por un auditor para la evaluación del precio de transferencia de reparto de costes entre el departamento de informática y los usuarios.

10. ¿Cuáles son las áreas legales cuyo cumplimiento es el más importante de auditar?

CAPÍTULO 11

AUDITORÍA DE LA EXPLOTACIÓN

Eloy Peña Ramos

11.1. INTRODUCCIÓN

El nivel de competencia que existe, hoy en día, entre las empresas les obliga a tomar decisiones rápidas y acertadas. Es necesario, para ello, el funcionamiento adecuado de los sistemas informáticos (mediante la incorporación de las *nuevas tecnologías)* y su continua actualización. De esta forma, es decir, combinando esas tecnologías con una adecuada organización y una gestión eficiente, las empresas podrán alcanzar sus objetivos de manera satisfactoria.

La auditoría informática periódica es uno de los instrumentos más eficaces con que cuentan las empresas para asegurar su existencia y superar a sus competidores. La detección oportuna de las debilidades del sistema permite mejorarlo racionalizando los recursos.

En este artículo se pretende elaborar el esquema de un procedimiento (Figura 11.1) para llevar a cabo las auditorías de la explotación de los sistemas de información[1] siguiendo la clasificación de los controles que hace el Proyecto CobiT.

[1] En este capítulo se utilizarán con el mismo significado las expresiones Sistema Informático y Sistema de Información, aunque esta última tiene un contenido más amplio, pues incluye los sistemas manuales y los informáticos.

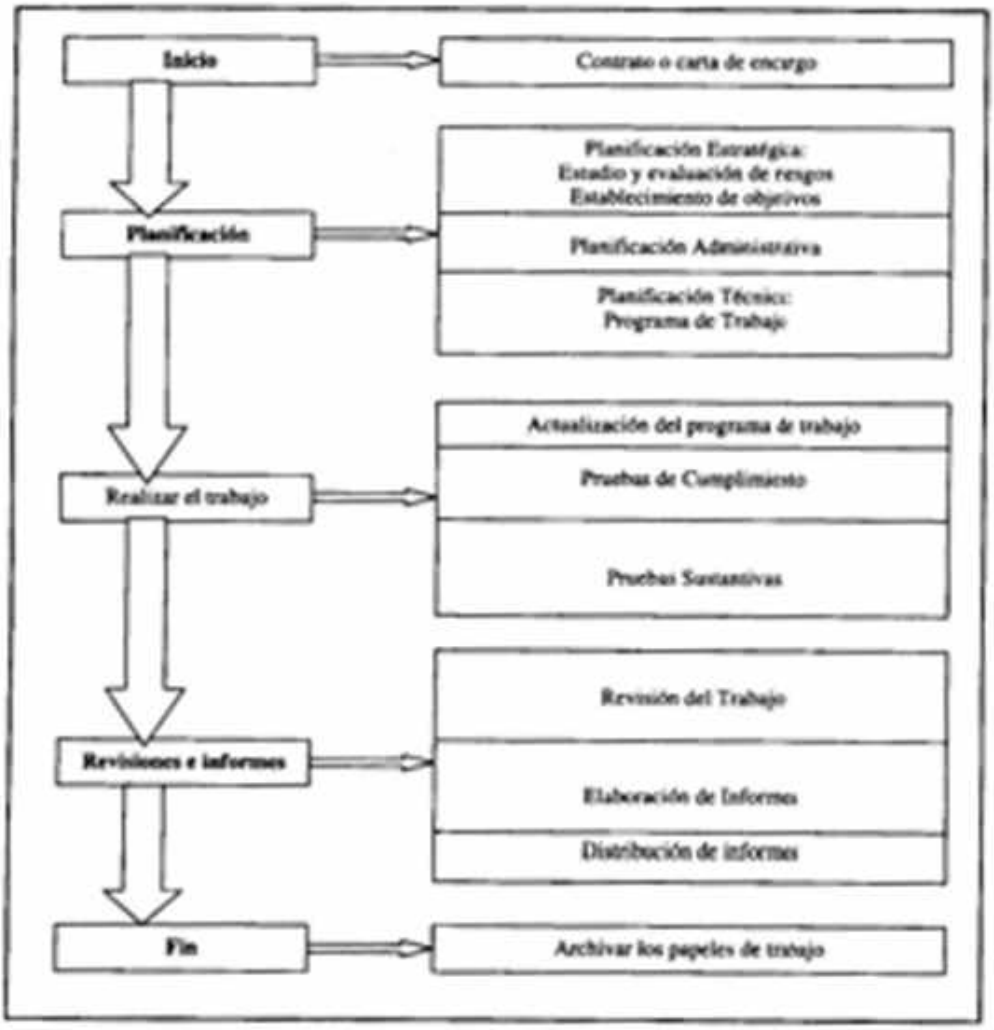


Figura 11.1. Procedimiento de auditoría

11.2. SISTEMAS DE INFORMACIÓN

En un sentido amplio se puede considerar un Sistema de Información (SI) como un conjunto de componentes que interactúan para que la empresa pueda alcanzar sus objetivos satisfactoriamente (véase figura 11.2). Según el Proyecto CobiT los componentes o recursos de un SI son los siguientes:

- *Datos.* En general se considerarán datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- *Aplicaciones.* Se incluyen las aplicaciones manuales y las informativas.
- Tecnología. El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- *Instalaciones.* En ellas se ubican y se mantienen los sistemas de información.

- *Personal.* Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos.

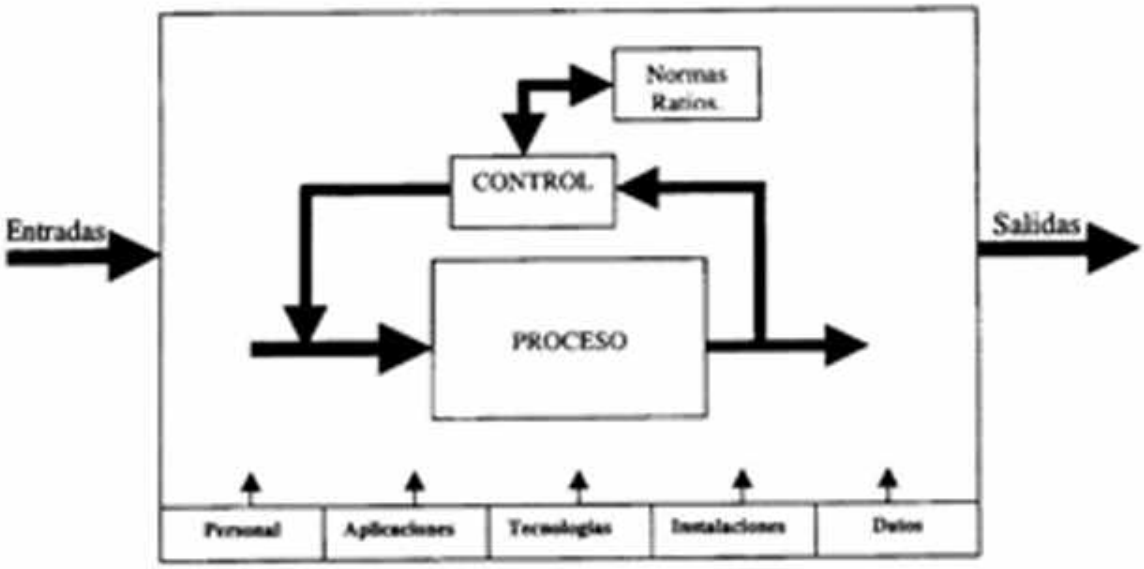


Figura 11.2. Sistema de Información

Estos recursos de los sistemas de información se han de utilizar, –informe COSO (Committee of Sponsoring Organizations of the Treadway Commission. Internal Control -Integrated Framework. 1992)–, de forma que permitan la eficacia y la eficiencia de la empresa; que los datos financieros elaborados por su sistema de información: muestren una imagen fiel de la misma y que la empresa cumpla la legislación vigente. Por otra parte el sistema debe asegurar la confidencialidad de sus datos, aspecto este último contemplado en la legislación vigente.

Para hacer el seguimiento y comprobar que el sistema de información está actuando como es preceptivo, éste habrá de disponer de un control interno que prevenga los eventos no deseados o en su defecto los detecte y los corrija.

Es conveniente recordar que el resultado de la auditoría parcial de un sistema de información no se puede extrapolar al conjunto del sistema. El funcionamiento inadecuado de alguno (o algunos) de los procesos y recursos que intervienen en otras partes del Sistema (subsistemas) puede invalidar el sistema de información.

En el esquema que se irá desarrollando como procedimiento para auditar la explotación del sistema, se adoptarán las normas de ISACA, así como otras Normas

de Auditoría de Sistemas de Información Generalmente Aceptadas y Aplicables (NASIGAA)[2].

11.3. CARTA DE ENCARGO

Las responsabilidades del trabajo de auditoría deben quedar recogidas en un contrato o carta de encargo antes de comenzar su realización (la Norma General número 12 de ISACA "Draft Standard # 12" se refiere a este aspecto sólo en el caso de la auditoría interna; pero también es de aplicación a la auditoría externa, como queda de manifiesto en otros tipos de auditorías). En ese documento debe quedar reflejado de la forma más clara posible, entre otros aspectos, cuál será el alcance del trabajo del auditor.

11.4. PLANIFICACIÓN

Según la Norma General número 6 de ISACA las auditorías de los sistemas de información deben planificarse y supervisarse para tener la seguridad de que los objetivos de las mismas se alcanzan y se cumplen las NASIGAA.

En la planificación de la auditoría vamos a considerar tres fases:

3.1. Planificación estratégica.
3.2. Planificación administrativa.
3.3. Planificación técnica.

11.4.1. Planificación estratégica

Es una revisión global que permite conocer la empresa, el SI y su control interno con la intención de hacer una primera evaluación de riesgos. Según los resultados de esa evaluación se establecerán los objetivos de la auditoría y se podrá determinar su alcance y las pruebas que hayan de aplicarse, así como el momento de realizarlas. Para llevar a cabo esta tarea es necesario conocer entre otros aspectos los siguientes:

- Las características de los equipos informáticos.
- El sistema o los sistemas operativos.
- Características de los archivos o de las bases de datos.
- La organización de la empresa.
- La organización del servicio de explotación.

[2] El término Normas de Auditoría de Sistemas de Información Generalmente Aceptadas y Aplicables tiene el mismo sentido que Principios de Contabilidad Generalmerte Aceptados (PCGA) en la auditoría financiera.

- Las aplicaciones que el SI de la empresa ("auditario")[3] que se esté auditando o que se vaya a auditar estén en explotación.
- El sector donde opera la empresa.
- Información comercial.

La información puede obtenerse:

a) Mediante entrevistas y confirmaciones:

- Con los responsables de explotación.
- Con los responsables del plan de contingencias.
- Con los usuarios.
- Con los proveedores de software y hardware.

b) Inspeccionando la siguiente documentación:

- Informes y papeles de trabajo de auditorías anteriores.
- Las normas y procedimientos de la empresa relacionados con la explotación del sistema de información.
- Los planes de contingencias.
- Agenda de trabajo.
- Instrucciones sobre el encendido y apagado de los equipos.
- Contratos de mantenimiento con otras empresas.
- Procedimientos de emergencia.
- Instrucciones sobre seguridad física y lógica.
- Instrucciones sobre la separación de las bibliotecas de desarrollo y producción.
- Una muestra representativa de las instrucciones operativas de las aplicaciones más importantes donde se incluyan: fecha, entradas, tiempo de proceso, mensajes de errores, instrucciones para finalizar tareas erróneas y diarios de operaciones.

11.4.1.1. Clasificación de los controles

En la auditoría informática se ha distinguido, tradicionalmente, entre controles generales y controles de las aplicaciones.

[3] "Auditario": Al no conocer ningún término con el que referirse al sujeto de la auditoría en cualquier tiempo verbal, es decir, la persona física o jurídica (cliente) cuyo sistema de información ha sido auditado, se está auditando o va a auditarse, el autor propone, salvo mejor parecer, el término *"auditario"* como susceptible de ser utilizado en cualquiera de estas situaciones.

La Norma técnica número 3 de AICPA (American Institute Of Charter Public Accountants), *Efectos del proceso electrónico de datos en el estudio y evaluación del control interno*, publicada en 1974, distingue entre controles generales y controles de las aplicaciones.

La AICPA publicó en 1984 la Norma número 48 (SAS.- Stament on Auditing Standard) *Los efectos del proceso informático en el análisis de los Estados Financieros.* En ella se definen los controles generales como aquellos que están relacionados con todas o con la mayoría de las actividades contables informatizadas, que generalmente incluyen controles del desarrollo de las modificaciones y del mantenimiento de programas informáticos y controles de la utilización y modificación de los datos que se mantienen en archivos informáticos.

En una línea parecida se expresa el documento número 1 sobre *El estudio y evaluación del control interno en entornos informatizados*, publicado por el REA (Registro de Economistas Auditores) en enero de 1996, siendo de interés para el auditor informático tener en cuenta este documento y sobre todo sus anexos.

El documento publicado por el REA dice: "los Controles Generales son una parte del entorno general de control y son aquellos que afectan, en un centro de proceso electrónico de datos, a toda la información por igual y a la continuidad de este servicio en la entidad. La debilidad o ausencia de estos controles pueden tener un impacto significativo en la integridad y exactitud de los datos. También se consideran controles generales aquellos relacionados con la protección de los activos: la información resultante, los elementos físicos del hardware y el software (programas y sistemas operativos).

Los Controles de las Aplicaciones son aquellos relacionados con la captura, entrada y registro de datos en un sistema informática, así como los relacionados con su procesamiento, cálculo y salida de la información y su distribución".

a) Controles generales

Los controles generales se pueden clasificar en las siguientes categorías:

1. Controles Operativos y de Organización:

- Segregación de Funciones entre el Servicio de Información y los usuarios.
- Existencia de Autorización general en lo que respecta a la ejecución y a las transacciones del Departamento (por ejemplo: prohibir al Servicio de Información que inicie o autorice transacciones).
- Segregación de funciones en el seno del Servicio de Información.

2. Controles sobre el desarrollo de programas y su documentación:

   - Realización de revisiones, pruebas y aprobación de los nuevos sistemas.
   - Controles de las modificaciones de los programas.
   - Procedimientos de documentación.

3. Controles sobre los Programas y los Equipos:

   - Características para detectar, de manera automática, errores.
   - Hacer mantenimientos preventivos periódicos.
   - Procedimientos para salir de los errores de los equipos (hardware).
   - Control y autorización adecuada en la implementación de sistemas y en las modificaciones de los mismos.

4. Controles de acceso:

   - Sirven para detectar y/o prevenir errores accidentales o deliberados, causados por el uso o la manipulación inadecuada de los archivos de datos y por el uso incorrecto o no autorizado de los programas.

5. Controles sobre los procedimientos y los datos:

   - Manuales escritos como soporte de los procedimientos y los sistemas de aplicación.
   - Controles de las conciliaciones entre los datos fuente y los datos informáticos.
   - Capacidad para restaurar archivos perdidos, deteriorados o incorrectos.

b) Controles de las aplicaciones

Los controles de las aplicaciones están relacionados con las propias aplicaciones informatizadas. Los controles básicos de las aplicaciones son tres: captura, proceso y salida.

1. Controles sobre la *captura* de datos:

   - Altas de movimientos.
   - Modificaciones de movimientos.
   - Consultas de movimientos.
   - Mantenimiento de los archivos.

2. Controles de *proceso*. Normalmente se incluyen en los programas. Se diseñan para detectar o prevenir los siguientes tipos de errores:

   - Entrada de datos repetidos.
   - Procesamiento y actualización de archivo o archivos equivocados.
   - Entrada de datos ilógicos.
   - Pérdida o distorsión de datos durante el proceso.

3. Controles de *salida* y *distribución*. Los Controles de salida se diseñan para asegurarse de que el resultado del proceso es exacto y que los informes y demás salidas los reciben sólo las personas que estén autorizadas.

En el Proyecto CobiT se establece una nueva clasificación, donde se afirma que existen tres niveles en las Tecnologías de la Información a la hora de considerar la gestión de sus recursos: actividades y/o tareas, procesos y dominios.

Actividades y tareas

Las actividades y las *tareas* son necesarias para alcanzar un resultado cuantificable. Las *actividades* suponen un concepto cíclico, mientras que las *tareas* implican un concepto algo más discreto.

Procesos

Los procesos se definen como una serie de actividades o tareas unidas por interrupciones naturales.

Dominios

Los procesos se agrupan de forma natural dando lugar a los *dominios*, que se confirman, generalmente, como *dominios* de responsabilidad en las estructuras organizativas de las empresas y están en línea con el ciclo de gestión aplicable a los procesos de las Tecnologías de la Información.

La Guía de Auditoría del Proyecto CobiT recoge 32 procesos de los Sistemas de Información donde se sugieren los objetivos de control. Esos procesos están agrupados en cuatro dominios.

Dominios y procesos de las tecnologías de la información

1. ***Planificación y organización***
   - 1.1. *Definir el plan estratégico de las Tecnologías de Información (TTI).*
   - *1.2. Definir la arquitectura de la información.*
   - *1.3. Determinar la dirección tecnológica.*
   - *1.4. Definir la organización y las relaciones.*
   - *1.5. Gestión de las inversiones.*
   - *1.6. Comunicar las tendencias a la dirección.*
   - *1.7. Gestión de recursos humanos.*
   - *1.8. Asegurarse del cumplimiento de los requisitos externos.*
   - *1.9. Evaluación del riesgo.*
   - *1.10. Gestión de proyectos.*
   - *1.11. Gestión de la calidad.*

2. ***Adquisición e implementación***
   - *2.1. Identificar las soluciones automatizados.*
   - *2.2. Adquirir y mantener el software.*
   - *2.3. Adquirir y mantener la arquitectura tecnológica.*
   - *2.4. Desarrollar y mantener procedimientos.*
   - *2.5. Instalar y acreditar los sistemas.*
   - *2.6. Gestión de los cambios.*

3. ***Suministro y mantenimiento***
   - *3.1. Definir el nivel de servicios.*
   - *3.2. Gestionar los servicios de las terceras partes.*
   - *3.3. Gestionar la capacidad y el funcionamiento.*
   - *3.4. Asegurarse del servicio continuo.*
   - *3.5. Asegurarse de la seguridad de los sistemas.*
   - *3.6. Identificar y localizar los costes.*
   - *3.7. Formación teórica y práctica de los usuarios.*
   - *3.8. Asistir y asesorar a los clientes.*
   - *3.9. Manejo de la configuración.*
   - *3.10. Gestión de los problemas y de los incidentes.*
   - *3.11. Gestión de los datos.*
   - *3.12. Gestión de las instalaciones.*
   - *3.13. Gestión de la explotación.*

4. ***Monitorización***
   - *4.1. Monitorizar el proceso.*
   - *4.2. Independencia.*

11.4.1.2. Evaluación de los controles internos

Es función del auditor evaluar el nivel de control interno; también es de su responsabilidad juzgar si los procedimientos establecidos son los adecuados para salvaguardar el sistema de información.

La naturaleza y la extensión de los controles que requieren los sistemas de proceso de datos variarán de acuerdo con la clase de sistemas en uso.

El informe COSO define el CONTROL como "las normas, los procedimientos, las prácticas y las estructuras organizativas diseñadas para proporcionar seguridad razonable de que los objetivos de las empresas se alcanzarán y que los eventos no deseados se preverán, se detectarán y se corregirán".

Para evaluar los controles es necesario buscar evidencia sobre:

- La terminación completa de todos los procesos.
- La separación física y lógica de los programas fuentes y objetos y de las bibliotecas de desarrollo, de pruebas y de producción.
- La existencia de normas y procedimientos para pasar los programas de una biblioteca a otra.
- Las estadísticas de funcionamiento, donde al menos se incluya:
  - Capacidad y utilización del equipo central y de los periféricos.
  - Utilización de la memoria.
  - Utilización de las telecomunicaciones.
- Las normas del nivel de servicios de los proveedores.
- Los estándares de funcionamiento interno.
- El mantenimiento y revisión de los diarios de explotación (*Operations Logs*).
- La realización del mantenimiento periódico de todos los equipos.
- La evidencia de la rotación de los turnos de los operadores y de las vacaciones tomadas.

Una forma de encontrar evidencia, como se comentaba en el punto 11.4.1.1a, es mediante entrevistas; para llevarlas a cabo se pueden elaborar cuestionarios (ver cuadro 11.1) o listas de comprobación (*check lists*) con el objetivo de no olvidar detalles importantes[4]. Es conveniente que los cuestionarios y las listas de comprobación se elaboren de tal manera que de las respuestas negativas se infiera debilidad, posibilidad de riesgo.

[4] En la bibliografía que se recomienda el lector podrá encontrar listas de comprobación y cuestionarios de control interno.

Referencia: 3.13/CCI/1

	Por	Fecha
Preparado		
Revisado		

Cliente : Nombre de la empresa
Fecha de auditoría : 31/12/952
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Cuestionario de Control Interno

Controles sobre la explotación del Servicio de Información	Sí	No	N/A	Observaciones
1. ¿Existen normas y procedimientos escritos sobre el funcionamiento del Servicio de Información?				
2. El Servicio de Información, ¿está separado del resto de los departamentos?				
3. ¿Es adecuada la segregación de funciones entre el Servicio de Información y los departamentos de los usuarios?				
4. ¿El personal de explotación participa en funciones de análisis y desarrollo de aplicaciones?				
5. ¿Existe organigrama del funcionamiento del Servicio de Información?				
6. ¿Se describen con detalle las funciones y responsabilidades del personal?				
7. El personal de explotación ¿conoce perfectamente cuáles son sus funciones y sus responsabilidades?				
8. ¿Es imposible que los operadores accedan a programas y datos no necesarios para su trabajo?				
9. ¿Se rotan las asignaciones de trabajo de los operadores?				
10. ¿Existen normas de cómo deben hacerse los cambios de turno para que exista la seguridad de que las aplicaciones continúan su proceso?				

Cuadro 11.1 (Continúa)

Referencia: 3.13/CCI/2

	Por	Fecha
Preparado		
Revisado		

Cliente : Nombre de la empresa
Fecha de auditoría : 31/12/952
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Cuestionario de Control Interno

Controles sobre la explotación del Servicio de Información	Sí	No	N/A	Observaciones
11. ¿Existe personal con conocimientos y experiencia suficiente que organiza el trabajo para que resulte lo más eficaz posible?				
12. ¿Existen procedimientos de salvaguarda, fuera de la instalación, en relación con ficheros maestros, manuales y programas, que permitan reconstruir las operaciones que sean necesarias?				
13. ¿Se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?				
14. ¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?				
15. ¿Existen procedimientos adecuados para mantener la documentación al día?				
16. ¿Tienen manuales todas las aplicaciones?				
17. ¿Existen controles que garanticen el uso adecuado de discos y cintas?				
18. ¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?				
19. ¿Se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?				
20. ¿Participan los departamentos de usuarios en la evaluación de los datos de prueba?				

Cuadro 11.1 (continuación)

Referencia: 3.13/CCI/3

	Por	Fecha
Preparado		
Revisado		

Cliente : Nombre de la empresa
Fecha de auditoría : 31/12/952
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Cuestionario de Control Interno

Controles sobre la explotación del Servicio de Información	Sí	No	N/A	Observaciones
21. ¿Revisan y evalúan los departamentos de usuarios los resultados de la pruebas finales dando su aprobación antes de poner en funcionamiento las aplicaciones?				
22. Al poner en funcionamiento nuevas aplicaciones o versiones actualizadas, ¿funcionan en paralelo las existentes durante un cierto tiempo?				
23. ¿Se comprueban los resultados con datos reales?				
24. ¿Existe personal con los conocimientos y experiencia adecuados que revisa con periodicidad los componentes físicos de los equipos siguiendo las instrucciones de los fabricantes?				
25. ¿Se cumplen las condiciones ambientales: temperatura, humedad, etc., que recomienda el fabricante para el equipo, cintas, etc.?				
26. ¿Existen controles apropiados para que sólo las personas autorizadas tengan acceso a los equipos, cintas, discos, documentación de programas, etc.?				
27. ¿Existen normas sobre horas extras y se controlan las entradas y salidas del personal fuera de su horario de trabajo?				

Cuadro 11.1 (continuación)

11.4.1.3. Establecimiento de objetivos

En función de la importancia de los riesgos que se hayan detectado, el auditor establecerá los objetivos de la auditoría, cuya determinación concreta permitirá definir con claridad el alcance de la misma.

Se considera que el riesgo es la presentación negativa de un objetivo de auditoría. Si la oración negativa se transforma en oración afirmativa, se tiene como resultado un objetivo de control. Veamos un ejemplo:

Una de las preguntas del cuestionario para la entrevista con el Director de Explotación dice lo siguiente:

¿Tiene su empresa normas escritas de cómo deben hacerse los traspases de programas en desarrollo a programas en explotación?

Si la respuesta fuera negativa, se podría concluir que existe un riesgo por el hecho de que cada empleado podría hacer los trasvases sin tomar las medidas de seguridad necesarias y porque el proceso de trasvase no ha dejado pistas de auditoría para poder rehacer los pasos que se han dado y poder comprobar que el trabajo se ha realizado de manera correcta. Por el solo hecho de no existir normas escritas no quiere decir que los trasvases se realicen mal. No obstante es una posibilidad de riesgo por lo que debemos convertir este riesgo potencial en objetivo de auditoría.

La debilidad sería la siguiente:

La empresa no tiene normas escritas de cómo deben hacerse los traspasos de programas en desarrollo a programas en explotación.

El objetivo de control sería:

Comprobar que la empresa tiene normas escritas de cómo deben hacerse los traspasos de programas en desarrollo a programas en explotación.

Para alcanzar ese objetivo habrá que diseñar una serie de pruebas de cumplimiento y sustantivas. Cada una de esas pruebas es un procedimiento.

Los procedimientos podrían ser:

a) Pruebas de cumplimiento

Si se confirma que realmente no existen manuales, no se pueden hacer pruebas de cumplimiento, pues las pruebas de cumplimiento consisten en comprobar que se están cumpliendo las normas establecidas. El procedimiento podría ser como sigue:

Comprobar que las normas para pasar un programa de desarrollo a explotación son adecuadas y que la empresa las está cumpliendo.

La inexistencia de manuales no implica, forzosamente, que los traspasos se llevan a cabo inadecuadamente. Para confirmarlo, al no existir normas, se tendrían que realizar pruebas sustantivas.

b) Pruebas sustantivas

Revisar las aplicaciones –si son pocas aplicaciones se revisan todas; si son muchas se elige una muestra representativa– que se han pasado de desarrollo a explotación y, revisar que antes de pasarlas han sido sometidas a un lote de pruebas y las han superado satisfactoriamente. Que esas pruebas cumplen los requisitos y estándares del sector. Que el traspaso ha sido autorizado por una persona con la suficiente autoridad.

Así pues, elaborando un cuestionario que contemple todos los aspectos necesarios para la buena explotación del sistema de información y realizando las pruebas oportunas se podrán establecer los objetivos de control de la auditoría (cuadro 11.I).

Para comprender y evaluar los riesgos no siempre es suficiente con entrevistas, inspecciones y confirmaciones; puede ser necesario realizar cálculos y utilizar técnicas de examen analítico.

La confirmación consiste en corroborar la información –que existe en los registros– con terceros, normalmente por escrito.

Los cálculos consisten en la comprobación de la exactitud aritmética de los registros de datos.

Las técnicas de examen analítico consisten en la comparación de los importes registrados con las expectativas desarrolladas por el auditor al evaluar las interrelaciones que razonablemente pueden esperarse entre las distintas partidas de la información auditada.

Siempre que sea posible (y la naturaleza de los datos lo permita) es conveniente utilizar técnicas de examen analítico (Norma Técnica número 5 de ISACA sobre la realización del trabajo: "The Use of Risk Assesment in Auditing Planning").

11.4.2. Planificación Administrativa

La Planificación Administrativa no se debería hacer hasta haber concluido la Planificación Estratégica. En esta fase de la planificación pueden surgir ciertos problemas por coincidir las fechas de trabajo del personal de la empresa auditora con otros clientes. Así en esta etapa deben quedar claros los siguientes aspectos:

Evidencia. En este punto se podrá hacer una relación con la documentación disponible en la etapa anterior, documentación que se utilizará indicando el lugar donde se encuentra para que esté a disposición del equipo de auditoría.

Personal. De qué personal se va a disponer, qué conocimientos y experiencia son los ideales y si va a ser necesario o no contar con expertos, tanto personal de la empresa auditora como expertos externos.

Calendario. Establecer la fecha de comienzo y de finalización de la auditoría y determinar dónde se va a realizar cada tarea: en las dependencias del cliente o en las oficinas del auditor.

Coordinación y cooperación. Es conveniente que el auditor mantenga buenas relaciones con el "auditario", que se establezca, entre ambos, un nivel de cooperación sin que deje de cumplirse el principio de independencia (Normas Generales números 1, 2 y 3 de ISACA) y que se defina con claridad el interlocutor del cliente.

11.4.3. Planificación Técnica

En esta última fase se ha de elaborar el programa de trabajo. En la fase de Planificación Estratégica se han establecido los objetivos de la auditoría. En la fase de Planificación Administrativa se han asignado los recursos de personal, tiempo, etc. En esta fase de Planificación Técnica se indican los métodos, –el método de auditoría que se va a seguir, es decir, si se va a seguir un método que se base en los controles, o por el contrario la auditoría se basará en pruebas sustantivas–, los procedimientos, las herramientas y las técnicas que se utilizarán para alcanzar los objetivos de la auditoría.

El programa de auditoría debe ser flexible y abierto, de tal forma que se puedan ir introduciendo cambios a medida que se vaya conociendo mejor el sistema. El programa y el resto de los papeles de trabajo son propiedad del auditor. Éste no tiene la obligación de mostrárselos a la empresa que se audita ("auditario"), debiendo custodiarlos durante el plazo que marque la ley.

Dedicarle a la planificación el tiempo necesario permite evitar pérdidas innecesarias de tiempo y de recursos. E. Perry [Planing EDP Audits, página 7] dice que la distribución ideal del tiempo empleado en realizar una auditoría sería: un tercio en planificar, un tercio en realizar el trabajo de campo y un tercio en hacer las revisiones y en la elaboración del informe o de los informes.

Para elaborar el programa de trabajo se va a seguir la guía de auditoría del proceso Gestión de la Explotación ["3.13 Gestión de la Explotación"]. Ciertos aspectos de la explotación de un sistema de información pueden quedar al margen del proceso 3.13. Esto es debido a la clasificación que hace CobiT y que se ha comentado anteriormelnte. Seguro que aquellos otros aspectos que el lector eche de menos quedan recogidos en otros procesos. Ésta es, pues, una de las grandes ventajas que presenta la Guía CobiT, facilita la comunicación en el sentido de que podemos determinar con claridad el alcance de la auditoría.

11.5. REALIZACIÓN DEL TRABAJO (PROCEDIMIENTOS)

Consiste en llevar a cabo las pruebas de cumplimiento y sustantivas que se han planificado para poder alcanzar los objetivos de la auditoría (Cuadro 11.2).

11.5.1. Objetivo general

Para el caso de la auditoría de la explotación hemos seguido las recomendaciones que se incluyen en la Guía del Proyecto CobiT. Así el *objetivo general* de la auditoría consistiría en:

Asegurarse de que las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada, y satisfacen los requisitos empresariales.

11.5.2. Objetivos específicos

Para alcanzar el objetivo general, se puede dividir ese objetivo en diversos objetivos específicos sobre los que se realizarán las pruebas oportunas para asegurarse de que el objetivo general se alcanza. El esquema de trabajo, para cada uno de los objetivos, es el siguiente:

Referencia: 3.13/1

	Por	Fecha
Preparado		
Revisado		

Auditario : Nombre de la empresa
Fecha de auditoría : 31/12/XXXX
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Programa de trabajo

1. Objetivo general

Las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada, y satisfacen los requisitos empresariales.

2. Objetivos específicos

2.1. Objetivo de control sobre los manuales de instrucciones y sobre los procedimientos de explotación
El servicio de información ha establecido y ha documentado procedimientos normalizados para la explotación de las Tecnologías de la Información. Todas las soluciones y las plataformas de las Tecnologías de la Información instaladas son operativas utilizando esos procedimientos. Los procedimientos se revisan de manera periódica para asegurarse de que son efectivos y que se ajustan a lo establecido.

2.2. Objetivo de control sobre el inicio de los procesos y otra documentación de funcionamiento
La dirección del servicio de información se ha asegurado de que el personal de explotación:

- Está suficientemente familiarizado con los procesos que están funcionando,
- Que éstos están documentados adecuadamente, y
- Que periódicamente se realizan pruebas y se ajustan si procede.

2.3. Objetivo de control sobre la agenda de trabajo
La dirección del servicio de información se ha asegurado de que la agenda de trabajo, los procesos y las distintas tareas están organizadas con la secuencia más efectiva posible, maximizando su utilización, y se alcanzan los objetivos establecidos. Tanto la agenda inicial como las modificaciones que se han producido han sido autorizadas al nivel de responsabilidad apropiado.

2.4. Objetivo de control sobre salidas fuera del horario normal de trabajo
Los procedimientos implantados identifican, aclaran y aprueban las salidas fuera del horario normal.

2.5. Objetivo de control sobre la continuidad en el proceso
En los cambios de turno de los operadores los procesos mantienen su continuidad siguiendo los protocolos establecidos para el relevo de la actividad.

Cuadro 11.2 (Continúa)

Referencia: 3.13/2

	Por	Fecha
Preparado		
Revisado		

Auditario : Nombre de la empresa
Fecha de auditoría : 31/12/XXXX
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Programa de trabajo

2.6. Objetivo de control sobre los diarios de explotación (Operations Logs)
Los controles de la dirección garantizan que se está guardando, en los diarios de explotación, información cronológica suficiente como para poder reconstruir, revisar en el momento oportuno, y examinar las secuencias del proceso y cualquier otra actividad relacionada y que sirva de soporte al proceso en cuestión.

2.7. Objetivo de control sobre la explotación remota
Para el caso de explotaciones remotas, se han definido e implantado procedimientos concretos que garantizan que las conexiones y desconexiones con los equipos remotos se realizan adecuadamente.

3. Procedimientos (Trabajo a realizar)
a) Pruebas de cumplimiento

Comprobar que el personal de explotación conoce y comprende:

1. Los procedimientos de explotación de los que es responsable.
2. Las expectativas de funcionamiento: las normas de los proveedores, las normas y los procedimientos de la empresa, y el nivel de servicio acordado que se vaya a suministrar a los usuarios.
3. Los planes de emergencia.
4. Requisitos de los diarios de explotación y su revisión por parte de la dirección.
5. Procedimientos para la solución de problemas.
6. Las comunicaciones en los cambios de turno y las responsabilidades de cada uno de los turnos.
7. La interacción de los equipos de proceso remoto con los equipos de proceso central.

Referencia PT*	Realizado Por

* PT = Papel de Trabajo

Cuadro 11.2 (continuación)

Referencia: 3.13/3

	Por	Fecha
Preparado		
Revisado		

Auditario : Nombre de la empresa
Fecha de auditoría : 31/12/XXXX
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Programa de trabajo

b) Pruebas sustantivas

Referencia PT*	Realizado Por

8. Revisar las estadísticas de explotación (equipo y personal) para determinar si su uso es el adecuado; comparar con otras empresas similares, con las normas de los proveedores, con normas internacionales apropiadas y con las prácticas y los ratios de las mejores industrias.
9. Revisar una muestra representativa de los manuales del servicio de información y determinar si cumplen con las normas y los procedimientos.
10. Examinar la documentación sobre el arranque y terminación de los procesos para confirmar que los procedimientos se someten a pruebas y que se actualizan con periodicidad.
11. Examinar el horario de proceso para asegurarse de su adecuación y suficiencia de funcionamiento con el programa.
12. Seleccionar usuarios y determinar si es suficiente el rendimiento operativo de las operaciones de las actividades en curso y en relación con los acuerdos de nivel de servicio.
13. Seleccionar una muestra de terminaciones anormales de los trabajos y determinar la solución de los problemas que ocurrieron.
14. Identificar los cursos de formación práctica de los operadores, los cambios de turnos y lo ocurrido con las vacaciones.
15. Seleccionar una muestra de los diarios de la consola para comprobar la exactitud, tendencias en su funcionamiento, y la revisión por parte de la directiva de la resolución de problemas –evaluar el esquema de solución de problemas donde sea aplicable.

Cuadro 11.2 (continuación)

Referencia: 3.13/4

	Por	Fecha
Preparado		
Revisado		

Auditario : Nombre de la empresa
Fecha de auditoría : 31/12/XXXX
Dominio : Suministro y mantenimiento
Proceso : Gestión de la explotación
Título : Programa de trabajo

16. Identificar a los usuarios para determinar si el nivel de servicio es satisfactorio
17. Identificar los procedimientos de mantenimiento preventivo que se han realizado en todos los equipos por sugerencia de los proveedores.

Referencia PT*	Realizado Por

Cuadro 11.2 (continuación)

- Comprender las tareas, las actividades del proceso que se está auditando.

  Si fuera necesario ampliaríamos las entrevistas que hemos realizado en la fase de planificación estratégica.

- Determinar si son o no apropiados los controles que están instalados.

  Si fuera necesario ampliaríamos las pruebas que hemos realizado en la fase de planificación estratégica.

- Hacer pruebas de cumplimiento para determinar si los controles que están instalados funcionan según lo establecido, de manera consistente y continua.

  El objetivo de las pruebas de cumplimiento consiste en analizar el nivel de cumplimiento de las normas de control que tiene establecidas el "auditario". Se supone que esas normas de control establecidas son eficientes y efectivas.

- Hacer pruebas sustantivas para aquellos objetivos de control cuyo buen funcionamiento con las pruebas de cumplimiento no nos ha satisfecho.

  El objetivo de las pruebas sustantivas consiste en realizar las pruebas necesarias sobre los datos para que proporcionen la suficiente seguridad a la dirección sobre si se ha alcanzado su objetivo empresarial.

Habrá que realizar el máximo número de pruebas sustantivas si:

- No existen instrumentos de medida de los controles.
- Los instrumentos de medida que existen se considera que no son los adecuados.
- Las pruebas de cumplimiento indican que los instrumentos de medida de los controles no se han aplicado de manera consistente y continua.

El auditor debería haber realizado las suficientes pruebas sobre los resultados de las distintas tareas y actividades de la explotación del sistema de información como para, poder concluir si los objetivos de control se han alcanzado o no. Con esa información debe elaborar un informe y si procede hacer las recomendaciones oportunas.

11.6. INFORMES

11.6.1. Tipos de informes

Una vez realizadas todas estas fases, el auditor está en condiciones de emitir un informe en el que exprese su opinión. Los tipos de opiniones básicas, generalmente aceptadas en auditoría, son cuatro: 1. Si se concluye que el sistema es satisfactorio, el auditor daría una opinión *favorable*. 2. Si el auditor considera que el sistema es un desastre, su opinión sería *desfavorable*. 3. El sistema es válido pero tiene algunos fallos que no lo invalidan, opinión con *salvedades*. 4. También podría ocurrir que el auditor no tenga suficientes elementos de juicio para poder opinar; en ese caso no opinaría: *denegación de opinión*. A continuación se muestra cómo podría redactarse el párrafo de opinión en cada uno de los casos que hemos comentado para el objetivo general que se ha propuesto.

1. Favorable

En nuestra opinión el servicio de explotación y las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada y satisfacen los requisitos empresariales.

2. Desfavorable

En nuestra opinión, dada la importancia de los efectos de las salvedades comentadas en los puntos X, X1,... de este informe, el servicio de explotación y las funciones que sirven de apoyo a las Tecnologías de la Información NO se realizan con regularidad, NI de forma ordenada y NO satisfacen los requisitos empresariales.

3. Con salvedades

En nuestra opinión, excepto por los efectos de las salvedades que se comentan en el punto X de este informe... (en una parte del informe se indicarán cuáles son las salvedades y en este mismo documento o en documento aparte se harán las recomendaciones oportunas para mejorar el sistema, para que en una siguiente auditoría no existan las salvedades comentadas) el servicio de explotación y las funciones que sirven de apoyo a las Tecnologías de la Información se realizan con regularidad, de forma ordenada y satisfacen los requisitos empresariales.

4. Denegación de opinión

En el caso de que las salvedades impidan hacernos una opinión del servicio de explotación, ya sea por falta de información o por no haber tenido acceso a ella por los motivos que fueren, pero siempre ajenos a nuestra voluntad, y no obstante, haber intentado hacer pruebas alternativas, el auditor denegará su opinión.

11.6.2. Recomendaciones

En el caso de que el auditor durante la realización de la auditoría detecte debilidades, éste debe comunicarlas al auditado con la mayor prontitud posible. Un esquema, generalmente aceptado, de cómo presentar las debilidades es el siguiente:

- Describir la debilidad.
- Indicar el criterio o instrumento de medida que se ha utilizado.
- Indicar los efectos que puede tener en el sistema de información.
- Describir la recomendación con la que esa debilidad se podría eliminar.

A continuación se completan las características que debe tener un buen informe de auditoría siguiendo las normas que para tal efecto ha emitido ISACA.

11.6.3. Normas para elaborar los informes

La elaboración y el contenido de los informes de auditoría deben ajustarse a las Normas de Auditoría de Sistemas de Información Generalmente Aceptadas y Aplicables (NASIGAA). Entre otros motivos porque facilita la comparación de los informes realizados por distintos auditores. Por tanto, siguiendo las normas números 9 y 10 de "General Standards for Information Systems Auditing" emitidas por ISACA, además del párrafo de opinión antes indicado, el informe de auditoría deberá contener otra información adicional.

El informe es el instrumento que se utiliza para comunicar los objetivos de la auditoría, el alcance que vaya a tener, las debilidades que se detecten y las conclusiones a las que se lleguen. A la hora de preparar el informe, el auditor debe tener en cuenta las necesidades y características de los que se suponen serán sus destinatarios. El informe debe contener un párrafo en el que se indiquen los objetivos que se pretenden cumplir. Si, según la opinión del auditor, alguno de estos objetivos no se pudiera alcanzar, se debe indicar en el informe.

En el informe de auditoría se deben mencionar cuáles son las NASIGAA que se han seguido para realizar el trabajo de auditoría. También se deben indicar: las

excepciones en el seguimiento de estas normas técnicas, el motivo de no seguirlas, y cuando proceda, también se deben indicar los efectos potenciales que pudieran tener en los resultados de la auditoría.

En el informe de auditoría se ha de mencionar el alcance de la auditoría, así como describir la naturaleza y la extensión del trabajo de auditoría. En el párrafo de alcance se deben indicar el área/proceso, el período de auditoría, el sistema, las aplicaciones y los procesos auditados. Asimismo se indicarán las circunstancias que hayan limitado el alcance cuando, en opinión del auditor, no se hayan podido completar todas las pruebas y procedimientos diseñados, o cuando el "auditario" haya impuesto restricciones o limitaciones al trabajo de auditoría.

Si durante el trabajo se detectaran debilidades en el sistema de información de la entidad auditada, éstas deberán indicarse en el informe, así como sus causas, sus efectos y las recomendaciones necesarias para mejorar o eliminar las debilidades.

El auditor debe expresar en el informe su opinión sobre el área o proceso auditado. No obstante, en función de los objetivos de la auditoría, esta opinión puede ser general y referirse a todas las áreas o procesos en su conjunto.

El informe de auditoría debe presentarse de una forma lógica y organizada. Debe contener la información suficiente para que sea comprendido por el destinatario y éste pueda llevar a cabo las acciones pertinentes para introducir las correcciones oportunas que mejoren el sistema.

El informe se debe emitir en el momento más adecuado para que permita que las acciones que tenga que poner en práctica el "auditario", tengan los mayores efectos positivos posibles. Con anterioridad al informe, el auditor puede emitir, si lo considera oportuno, recomendaciones destinadas a personas concretas. Estas recomendaciones no deberían alterar el contenido del informe.

En el informe se debe indicar la entidad que se audita y la fecha de emisión del informe, también se deben indicar las restricciones que fuesen convenientes a la hora de distribuir el informe para que éste no llegue a manos indebidas.

11.7. LA DOCUMENTACIÓN DE LA AUDITORÍA Y SU ORGANIZACIÓN

11.7.1. Papeles de trabajo

La documentación de la auditoría de los sistemas de información es el registro del trabajo de auditoría realizado y la evidencia que sirve de soporte a las debilidades

encontradas y las conclusiones a las que ha llegado el auditor. Esos documentos genéricamente, se denominan papeles de trabajo. Los papeles de trabajo se deben diseñar y organizar según las circunstancias y las necesidades del auditor. Éstos han de ser completos, claros y concisos. Todo el trabajo de auditoría debe quedar reflejado en papeles de trabajo por los siguientes motivos:

- Recogen la evidencia obtenida a lo largo del trabajo.
- Ayudan al auditor en el desarrollo de su trabajo.
- Ofrecen un soporte del trabajo realizado para, así, poder utilizarlo en auditorías sucesivas.
- Permiten que el trabajo pueda ser revisado por terceros.

Para concluir la importancia que tienen los papeles de trabajo, digamos que una vez que el auditor ha finalizado su trabajo, los papeles de trabajo son la única prueba que tiene el auditor de haber llevado a cabo un examen adecuado. Siempre existe la posibilidad de que el auditor tenga que demostrar la calidad de su análisis ante un tribunal.

11.7.2. Archivos

Los papeles de trabajo que el auditor va elaborando se pueden organizar en dos archivos principales: el archivo permanente o continuo de auditoría y el archivo corriente o de la auditoría en curso.

11.7.2.1. Archivo permanente

El archivo permanente contiene todos aquellos papeles que tienen un interés continuo y una validez plurianual tales como:

- Características de los equipos y de las aplicaciones.
- Manuales de los equipos y de las aplicaciones.
- Descripción del control interno.
- Organigramas de la empresa en general.
- Organigramas del Servicio de Información y división de funciones.
- Cuadro de planificación plurianual de auditoría.
- Escrituras y contratos.
- Consideraciones sobre el negocio.
- Consideraciones sobre el sector.
- Y en general toda aquella información que puede tener una importancia para auditorías posteriores.

11.7.2.2. Archivo corriente

Este archivo, a su vez, se suele dividir en archivo general y en archivo de áreas o de procesos.

11.7.2.2.1. Archivo general

Los documentos que se suelen archivar aquí son aquellos que no tienen cabida específica en alguna de las áreas/procesos en que hemos dividido el trabajo de auditoría tales como:

- El Informe del Auditor.
- La Carta de recomendaciones.
- Los Acontecimientos posteriores.
- El Cuadro de planificación de la auditoría corriente.
- La Correspondencia que se ha mantenido con la dirección de la empresa.
- El tiempo que cada persona del equipo ha empleado en cada una de las áreas/procesos.

11.7.2.2.2. Archivo por áreas/procesos

Se debe preparar un archivo para cada una de las áreas o procesos en que hayamos dividido el trabajo e incluir en cada archivo todos los documentos que hayamos necesitado para realizar el trabajo de esa área/proceso concreto. Al menos deberán incluirse los siguientes documentos:

- Programa de auditoría de cada una de las áreas/procesos.
- Conclusiones del área/proceso en cuestión.
- Conclusiones del procedimiento en cuestión.

11.8. CONCLUSIONES

Podemos concluir diciendo que la labor del auditor informático es esencial para garantizar la adecuación de los sistemas informáticos; para ello el auditor debe realizar su trabajo ateniéndose a las Normas de Auditoría de Sistemas de Información Generalmente Aceptadas y Aplicables como requisito necesario que garantice la calidad del trabajo realizado y que la evidencia de este trabajo quede documentada. En función de que la sociedad se va informatizando cada vez más, es necesario ir elaborando normas para que la audiencia de la auditoría –que es toda la sociedad– tenga la seguridad de que, los sistemas funcionan, sus datos se mantienen con la debida confidencialidad y los informes de los distintos auditores se pueden comparar.

11.9. LECTURAS RECOMENDADAS

General Standards for Information Systems Auditing. Information Systems Audit and Control Foundation. Illinois, EE.UU., 1987.

El estudio y evaluación del control interno en entornos informatizados. Documento número 1 del REA (Registro de Economistas Auditores), enero 1996.

Resolución de 19 de enero de 1991, del Instituto de Contabilidad y Auditoría de Cuentas por la que se publican las Normas Técnicas de Auditoría.

EDP Audit Workpapers. EDPAF Audit guide, EDP Auditors Foundation, Inc. Carol Stream, Illinois, EE.UU., 1981.

Planning EDP Audit. William E. Perry. Audit Guide Series, EDP Auditors Foundation, Inc., Altamonte Springs, Florida, EE.UU., 1981.

Computer Audit, Control, and Security. Robert R. Moeller. John Wiley & Sons, Inc. Nueva York, 1989.

Infonnation Systems Audit Process. S. Rao Vallabhaneni. The Auditors Foundatioe, Inc. 2' ed., 1988.

CobiT (Control Objectives for Information and relates Technology). Information Systems Audit and Control Foundation. IL. EE.UU., septiembre 1996.

11.10. CUESTIONES DE REPASO

1. ¿Cuáles son los componentes de un SI según el Proyecto CobiT?
2. ¿Cuál es el fin de la carta de encargo?
3. ¿Cuáles son las fases de la planificación de la auditoría?
4. ¿Qué categorías se pueden distinguir en los controles generales?
5. Defina "control". ¿Cómo se evalúan los controles?
6. ¿Qué diferencias existen entre las pruebas sustantivas y las de cumplimiento?
7. ¿Cuáles son los tipos de informes de auditoría?

8. ¿Cómo estructuraría un informe de auditoría?

9. Defina los tipos de archivos principales y contenido de cada uno.

10. Especifique algunos objetivos de control a revisar en la auditoría de la explotación de los sistemas informáticos.

CAPÍTULO 12

AUDITORÍA DEL DESARROLLO

José Antonio Rodero Rodero

12.1. INTRODUCCIÓN

La necesidad de que una organización cuente con procedimientos de control interno es aceptada ampliamente como garantía de una gestión eficaz orientada a la consecución de los objetivos marcados. La función auditora es precisamente la encargada de comprobar la existencia de estos procedimientos de control y de verificar su correcta definición y aplicación, determinando las deficiencias que existan al respecto y los riesgos asociados a estas carencias de control.

Teniendo en cuenta que cada organización puede descomponerse funcionalmente en distintos departamentos, áreas, unidades, etc., es necesario que los mecanismos de control interno existan y se respeten en cada una de las divisiones funcionales para que éstas cumplan adecuadamente su cometido y hagan posible que la organización en su conjunto funcione de manera correcta.

Aplicando la división funcional al departamento de informática de cualquier entidad, una de las áreas que tradicionalmente aparece es la de desarrollo. Esta función abarca todas las fases que se deben seguir desde que aparece la necesidad de disponer de un determinado sistema de información hasta que éste es construido e implantado. Para delimitar el ámbito de este capítulo sobre auditoría del desarrollo, se entenderá que el desarrollo incluye todo el ciclo de vida del software excepto la explotación, el mantenimiento y la retirada de servicio de las aplicaciones cuando ésta tenga lugar.

Si se entiende por ingeniería del software "el establecimiento y uso de principios de ingeniería robustos, orientados a obtener software económico que sea fiable, cumpla los requisitos previamente establecidos y funcione de manera eficiente sobre

máquinas reales" (Fritz Bauer), la auditoría del desarrollo tratará de verificar la existencia y aplicación de procedimientos de control adecuados que permitan garantizar que el desarrollo de sistemas de información se ha llevado a cabo según estos principios de ingeniería, o por el contrario, determinar las deficiencias existentes en este sentido.

El planteamiento de este capítulo está orientado al desarrollo de sistemas de información en el sentido tradicional, sin que se hayan tenido en cuenta las peculiaridades del desarrollo de otro tipo de software como puedan ser sistemas operativos, software de comunicaciones, software empotrado, etc. Tampoco se ha tenido en cuenta la gestión de la calidad en el desarrollo, pues hay un capítulo dedicado a tal efecto, ni conceptos generales de control interno y auditoría que ya se abordaron en la parte I del libro (por ejemplo, criterios para la realización del informe, recomendaciones en el trato con los auditados, necesidad de independencia del auditor, preparación y realización de las entrevistas, etc.).

12.2. IMPORTANCIA DE LA AUDITORÍA DEL DESARROLLO

Aunque cualquier departamento o área de una organización es susceptible de ser auditado, hay una serie de circunstancias que hacen especialmente importante al área de desarrollo y, por tanto, también su auditoría, frente a otras funciones o áreas dentro del departamento de informática:

- Los avances en tecnologías de los computadores han hecho que actualmente el desafío más importante y el principal factor de éxito de la informática sea la mejora de la calidad del software.

- El gasto destinado a software es cada vez superior al que se dedica a hardware.

- A pesar de la juventud de la ciencia informática, hace años que se produjo la denominada "crisis del software". Incluye problemas asociados con el desarrollo y mantenimiento del software y afecta a un gran número de organizaciones. En el área del hardware no se ha dado una crisis equivalente.

- El software como producto es muy difícil de validar. Un mayor control en el proceso de desarrollo incrementa la calidad del mismo y disminuye los costes de mantenimiento.

- El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual denota la inexistencia o mal funcionamiento de los controles en este proceso. Los datos del Government Accounting Office Report (EE.UU.) sobre diversos proyectos de software (valorados en 6,8 millones de dólares) son ilustrativos:

Un 1.5 % se usó tal y como se entregó.
Un 3.0 % se usó después de algunos cambios.
Un 19.5 % se usó y luego se abandonó o se rehizo.
Un 47 % se entregó pero nunca se usó.
Un 29 % se pagó pero nunca se entregó.

- Las aplicaciones informáticas, que son el producto principal obtenido al final del desarrollo, pasan a ser la herramienta de trabajo principal de las áreas informatizadas, convirtiéndose en un factor esencial para la gestión y la toma de decisiones.

12.3. PLANTEAMIENTO Y METODOLOGÍA

Para tratar la auditoría del área de desarrollo es necesario, en primer lugar, acotar las funciones o tareas que son responsabilidad del área. Teniendo en cuenta que puede haber variaciones de una organización a otra, las funciones que tradicionalmente se asignan al área de desarrollo son:

- Planificación del área y participación, en la medida que corresponda, en la elaboración del plan estratégico de informática.

- Desarrollo de nuevos sistemas. Ésta es la función principal y la que da sentido al área de desarrollo. Incluirá para cada uno de los sistemas, el análisis, diseño, construcción e implantación. El mantenimiento se supondrá función de otra área.

- Estudio de nuevos lenguajes, técnicas, metodologías, estándares, herramientas, etc. relacionados con el desarrollo y adopción de los mismos cuando se considere oportuno para mantener un nivel de vigencia adecuado a la tecnología del momento.

- Establecimiento de un plan de formación para el personal adscrito al área.

- Establecimiento de normas y controles para todas las actividades que se realizan en el área y comprobación de su observancia.

Una vez conocidas las tareas que se realizan en el área de desarrollo, se abordará la auditoría de la misma desglosándola en dos grandes apartados, que más tarde se subdividirán con más detalle:

- Auditoría de la organización y gestión del área de desarrollo.
- Auditoría de proyectos de desarrollo de sistemas de información.

De estos dos apartados se hará más énfasis en el segundo por tratarse de la función principal del área, aunque ha de tenerse en cuenta que una buena organización y gestión es imprescindible para que los proyectos tengan una calidad aceptable.

La metodología que se aplicará es la propuesta por la ISACA (Information Systems Audit and Control Association), que está basada en la evaluación de riesgos: partiendo de los riesgos potenciales a los que está sometida una actividad, en este caso el desarrollo de un sistema de información, se determinan una serie de objetivos de control que minimicen esos riesgos.

Para cada objetivo de control se especifican una o más técnicas de control, también denominadas simplemente controles, que contribuyan a lograr el cumplimiento de dicho objetivo. Además, se aportan una serie de pruebas de cumplimiento que permitan la comprobación de la existencia y correcta aplicación de dichos controles. El esquema para cada objetivo de control es:

...
OBJETIVO DE CONTROL X: ...
C-X-1: Técnica de control *1* del objetivo de control *x* ...
- Pruebas de cumplimiento de C-X-1

C-X-m: Técnica de control *m* del objetivo de control *x* ...
- Pruebas de cumplimiento de C-X-m

...

Una vez fijados los objetivos de control, será función del auditor determinar el grado de cumplimiento de cada uno de ellos. Para cada objetivo se estudiarán todos los controles asociados al mismo, usando para ello las pruebas de cumplimiento propuestas. Con cada prueba de cumplimiento se obtendrá alguna evidencia, bien sea directa o indirecta, sobre la corrección de los controles. Si una simple comprobación no ofrece ninguna evidencia, será necesaria la realización de exámenes más profundos.

En los controles en los que sea impracticable una revisión exhaustiva de los elementos de verificación, bien porque los recursos de auditoría sean limitados o porque el número de elementos a inspeccionar sea muy elevado, se examinará una muestra representativa que permita inferir el estado de todo el conjunto.

El estudio global de todas las conclusiones, pruebas y evidencias obtenidas sobre cada control permitirán al auditor obtener el nivel de satisfacción de cada objetivo de control, así como cuáles son los puntos fuertes y débiles del mismo. Con esta información, y teniendo en cuenta las particularidades de la organización en estudio, se determinará cuáles son los riesgos no cubiertos, en qué medida lo son y qué

consecuencias se pueden derivar de esa situación. Estas conclusiones, junto con las recomendaciones formuladas, serán las que se plasmen en el informe de auditoría.

En los apartados siguientes se agrupan los distintos objetivos de control en varias series, detallándose para cada uno de ellos sus controles asociados y pruebas de cumplimiento. El esquema seguido es el siguiente:

- Organización y gestión del área de desarrollo (serie A, aptdo. 4)
- Proyectos de desarrollo de sistemas de información
  Aprobación, planificación y gestión del proyecto (serie B, aptdo. 5.1)
  Análisis
    Análisis de requisitos (serie C, aptdo. 5.2.1)
    Especificación funcional (serie D, aptdo. 5.2.2)
  Diseño
    Diseño técnico (serie E, aptdo. 5.3.1)
  Construcción
    Desarrollo de componentes (serie F, aptdo. 5.4.1)
    Desarrollo de procedimientos de usuario (serie G, aptdo. 5.4.2)
  Implantación
    Pruebas, implantación y aceptación (serie H, aptdo. 5.5.1)

12.4. AUDITORÍA DE LA ORGANIZACIÓN Y GESTIÓN DEL ÁREA DE DESARROLLO

Aunque cada proyecto de desarrollo tenga entidad propia y se gestione con cierta autonomía, para poderse llevar a efecto necesita apoyarse en el personal del área y en los procedimientos establecidos. La importancia de estos aspectos ha motivado que se dedique un apartado exclusivo a la organización y gestión del área de desarrollo. Se consideran ocho objetivos de control (serie A):

OBJETIVO DE CONTROL A1: El área de desarrollo debe tener unos cometidos asignados dentro del departamento y una organización que le permita el cumplimiento de los mismos.

C-A1-1: Deben establecerse de forma clara las funciones del área de desarrollo dentro del departamento de informática. Se debe comprobar que:

- Existe el documento que contiene las funciones que son competencia del área de desarrollo, que está aprobado por la dirección de informática y que se respeta.

C-AI-2: Debe especificarse el organigrama con la relación de puestos del área, así como el personal adscrito y el puesto que ocupa cada persona. Debe existir un procedimiento para la promoción de personal. Se debe comprobar que:

- Existe un organigrama con la estructura de organización del área. Para cada puesto debe describir las funciones a desempeñar, los requisitos mínimos de formación y experiencia, y la dependencia jerárquica del mismo.
- Existe un manual de organización que regula las relaciones entre puestos.
- Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona. Se deben cumplir los requisitos de los puestos.
- Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo siempre en cuenta la experiencia y formación.

C-AI-3: El área debe tener y difundir su propio plan a corto, medio y largo plazo, que será coherente con el plan de sistemas, si éste existe. Se debe comprobar que:

- El plan existe, es claro y realista.
- Los recursos actuales, más los que esté planificado que se incorporen al área, son suficientes para su cumplimiento.
- Se revisa y actualiza con periodicidad en función de las nuevas situaciones.
- Se difunde a todos los empleados para que se sientan partícipes del mismo, al resto del departamento y a los departamentos a los que les atañe.

C-AI-4: El área de desarrollo llevará su propio control presupuestario. Se debe comprobar que:

- Se hace un presupuesto por ejercicio, y se cumple.
- El presupuesto está en consonancia con los objetivos a cumplir.

OBJETIVO DE CONTROL A2: El personal del área de desarrollo debe contar con la formación adecuada y estar motivado para la realización de su trabajo.

C-A2-1: Deben existir procedimientos de contratación objetivos. Se debe comprobar que:

- Las ofertas de puestos del área se difunden de forma suficiente fuera de la organización y las selecciones se hacen de forma objetiva.

- Las personas seleccionadas cumplen los requisitos del puesto al que acceden.

C-A2-2: Debe existir un plan de formación que esté en consonancia con los objetivos tecnológicos que se tengan en el área. Se debe comprobar que:

- Se tiene aprobado un plan de formación a corto, medio y largo plazo que sea coherente con la política tecnológica.

- Incluye toda la información relevante para cada actividad formativa: fechas, horarios, lugar, ponentes, asistentes, material, medios necesarios, etc.

- Las actividades formativas se evalúan por parte de los asistentes y esta evaluación se tiene en cuenta a la hora de redefinir el plan de formación.

Contempla la formación de todos los empleados y tiene en cuenta el puesto que ocupan.

El plan de trabajo del área tiene en cuenta los tiempos de formación.

C-A2-3: Debe existir un protocolo de recepción/abandono para las personas que se incorporan o dejan el área. Se debe comprobar que:

- El protocolo existe y se respeta para cada incorporación/abandono.

- Para la incorporación, incluye al menos los estándares definidos, manual de organización del área, definición de puestos, etc.

- En los abandonos de personal se garantiza la protección del área.

C-A2-4: Debe existir una biblioteca y una hemeroteca accesibles por el personal del área. Se debe comprobar que:

- Están disponibles un número suficiente de libros, publicaciones periódicas, monogramas, etc. de reconocido prestigio y el personal tiene acceso a ellos.

C-A2-5: El personal debe estar motivado en la realización de su trabajo. Este aspecto es difícil de valorar y no es puramente técnico. Se debe comprobar que:

- Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área.

- No existe una gran rotación de personal y hay un buen ambiente de trabajo.

- El rendimiento del personal no cae por debajo de unos mínimos razonables y el absentismo laboral es similar al del resto de la organización.

OBJETIVO DE CONTROL A3: Si existe un plan de sistemas, los proyectos que se lleven a cabo se basarán en dicho plan y lo mantendrán actualizado.

C-A3-1: La realización de nuevos proyectos debe basarse en el plan de sistemas en cuanto a objetivos, marco general y horizonte temporal. Se debe comprobar que:

- Las fechas de realización coinciden con las del plan de sistemas.

- La documentación relativa a cada proyecto que hay en el plan de sistemas se pone a disposición del director de proyecto una vez comenzado el mismo. Esta información debe contener los objetivos, los requisitos generales y un plan inicial.

C-A3-2: El plan de sistemas debe actualizarse con la información que se genera a lo largo de un proceso de desarrollo. Se debe comprobar que:

- Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas por las implicaciones que pudiera tener.

OBJETIVO DE CONTROL A4: La propuesta y aprobación de nuevos proyectos debe realizarse de forma reglada.

C-A4-1: Debe existir un procedimiento para la propuesta de realización de nuevos proyectos. Se debe comprobar que:

- Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas y en todo caso se aportan los siguientes datos: descripción, necesidad, departamento patrocinador, riesgos, marco temporal, coste de la no realización, ventajas que aporta, adaptación a los planes de negocio, etc.

- Se respeta este mecanismo en todas las propuestas.

C-A4-2: Debe existir un procedimiento de aprobación de nuevos proyectos que dependerá de que exista o no plan de sistemas. Si hay un plan de sistemas se debe comprobar que:

- Se parte de las pautas, prioridades y planificación que éste marque para el desarrollo de cada nuevo sistema.

Si no existe plan de sistemas se debe comprobar que:

- Hay un procedimiento para estudiar la justificación y llevar a cabo el estudio de viabilidad de cada nuevo proyecto, incluyendo un análisis coste/beneficio y teniendo siempre como alternativa la no realización del mismo.

- Están designadas a áreas de la organización que tienen competencia para aprobar formalmente la realización y prioridad de los nuevos proyectos, así como el cauce para reasignar prioridades si fuese necesario. La decisión, afirmativa o negativa, se obtendrá en un tiempo razonable y se comunicará a los promotores.

OBJETIVO DE CONTROL A5: La asignación de recursos a los proyectos debe hacerse de forma reglada.

C-A5-1: Debe existir un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto. Se debe comprobar que:

- El procedimiento existe y se respeta.

- Se tiene en cuenta a todas las personas disponibles cuyo perfil sea adecuado a los riesgos de cada proyecto y que tengan disponibilidad para participar.

- Existe un protocolo para solicitar al resto de las áreas (sistemas, comunicaciones, etc.) la participación de personal en el proyecto, y se aplica dicho protocolo.

C-A5-2: Debe existir un procedimiento para conseguir los recursos materiales necesarios para cada proyecto. Se debe comprobar que:

- El procedimiento existe y se respeta.

OBJETIVO DE CONTROL A6: El desarrollo de sistemas de información debe hacerse aplicando principios de ingeniería del software ampliamente aceptados.

C-A6-1: Debe tenerse implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda (CASE). Se debe comprobar que:

La metodología cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyecto.

- La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y de organización del área de desarrollo.

- Se ha adquirido, homologado e implantado según las normas del área una herramienta CASE que se adapta a la metodología elegida y que cumple con los requisitos mínimos exigibles a una herramienta de este tipo.

- Se ha formado al personal sobre esta metodología y su adaptación, así como sobre las técnicas asociadas y la herramienta CASE.

- Existe un procedimiento que permita determinar en qué proyectos el uso de la herramienta CASE es ventajoso.

- Está claramente especificado de qué forma el uso de la herramienta altera las fases de desarrollo tradicionales.

- La herramienta CASE es capaz de mantener el diccionario de datos.

- La herramienta CASE mantiene los requisitos de confidencialidad necesarios sobre la documentación asociada al proyecto.

C-A6-2: Debe existir un mecanismo de creación y actualización de estándares, así como estándares ya definidos para las actividades principales. Se prestará especial atención a las herramientas y lenguajes de programación no clásicas. Se debe comprobar que:

- El mecanismo para creación de nuevos estándares está documentado y es conocido en el área.

- Hay un estándar para la realización del análisis y diseño, e incluye las técnicas y herramientas a usar, etc.

- Hay un estándar de programación para cada uno de los lenguajes homologados. Se prestará especial atención a las herramientas denominadas RAD (Rapid Application Development), ya que las secuencias posibles de ejecución son muy numerosas (normalmente se activan rutinas por eventos o *triggers* (disparadores) y el orden no se puede prever a priori) y la validación y depuración es prácticamente imposible si no se estandariza la programación.

- Existen convenios sobre los aspectos más importantes de la programación: modularidad, nomenclatura (de funciones, variables, tablas, columnas, etc.), formato de los comentarios, documentación asociada, estilo de programación, etc.

- Hay un estándar general para toda la documentación generada, incluyendo documentación técnica (análisis, diseño, documentación de los programas, cuadernos de carga, etc.), manuales de usuario, procedimientos de operación, etc.

- Hay un estándar para la interfaz de usuario, incluyendo diseño de pantallas, informes, etc.

- Los estándares son conocidos por las personas que deben usarlos y se respetan. Cuando se produce una modificación, ésta se difunde dentro del área.

C-A6-3: Los lenguajes, compiladores, herramientas CASE, software de control de versiones, etc. usados en el área deben ser previamente homologados. Se debe comprobar que:

- Existe un mecanismo para la adquisición y homologación de cualquier nuevo producto software usado en el desarrollo. Se deben evaluar al menos los siguientes parámetros: productividad, portabilidad a otros entornos, transición desde los productos actuales, solvencia del proveedor, riesgo del cambio, cumplimiento de los estándares del área, compatibilidad con el entorno tecnológico (SO, protocolos de comunicaciones, SGBD, etc.), coste, etc.

- Cuando se homologa un nuevo producto de desarrollo se forma al personal del área que lo vaya a manejar.

- Se registra la información más importante acerca de la configuración de los productos recién adquiridos.

- Los productos homologados son suficientes para conseguir los objetivos marcados.

- Periódicamente se comprueba el nivel tecnológico, para ver si es coherente con el plan de sistemas y si está en línea con el de otras organizaciones similares.

C-A6-4: Debe practicarse la reutilización del software. Se debe comprobar que:

- Existe un catálogo con todos los productos software susceptibles de ser reutilizados: librerías de funciones, clases si se utiliza programación orientada a objetos, programas tipo, componentes software, etc.

- El catálogo es conocido y accesible por todos los miembros del área, está actualizado y tiene uno o varios índices que faciliten la búsqueda.

- Existe un catálogo de las aplicaciones disponibles en el área, tanto de las realizadas como de las adquiridas, con toda la información relevante de las mismas.

C-A6-5: Debe existir un método que permita catalogar y estimar los tiempos de cada una de las fases de los proyectos. Se debe comprobar que:

- El método usado es correcto, está bien ajustado y documentado adecuadamente.

- Las desviaciones producidas en cada proyecto se usan para ajustar los parámetros de catalogación y estimación manteniendo un histórico de los mismos.

C-A6-6: Debe existir un registro de problemas que se producen en los proyectos del área, incluyendo los fracasos de proyectos completos. Se debe comprobar que:

- Existe un catálogo de problemas, incluyendo para cada uno de ellos la solución o soluciones encontradas, proyecto en el que sucedió, persona que lo resolvió, etc.

- El catálogo es accesible para todos los miembros del área, está actualizado y tiene uno o varios índices que faciliten la búsqueda.

- Se registran y controlan todos los proyectos fracasados (aquellos que comienzan y no llegan a su fin), así como los recursos invertidos en los mismos.

OBJETIVO DE CONTROL A7: Las relaciones con el exterior del departamento tienen que producirse de acuerdo a un procedimiento.

C-A7-1: Deben mantenerse contactos con proveedores para recibir información suficiente sobre productos que puedan ser de interés. Se debe comprobar que:

- Se está en contacto con un número suficiente de proveedores para recibir una información objetiva y completa, y el tiempo invertido en estas tareas no excede lo razonable.

C-A7-2: Debe existir un protocolo para contratación de servicios externos. Se debe comprobar que:

- Existe el protocolo, está aprobado y se hace uso de él.

- La selección del proveedor se hace de forma objetiva y evita situaciones de monopolio por parte de un único proveedor.

- El protocolo incluye un contrato-tipo que prevea los riesgos más frecuentes cuando se contratan servicios externos, y en todo caso incorpora penalizaciones en caso de incumplimiento de contrato por parte del proveedor.

- El personal externo que intervendrá en los proyectos cumplirá, al menos, los mismos requisitos que se exigen a los empleados del área.

- Una persona del área supervisa el trabajo realizado, certificándolo antes del pago.

- Debe ser compatible con los estándares establecidos en el área.

OBJETIVO DE CONTROL A8: La organización del área debe estar siempre adaptada a las necesidades de cada momento.

C-A8-1: La organización debe revisarse de forma regular. Se debe comprobar que:

- Existe el procedimiento de revisión, se aplica con una periodicidad adecuada y se adapta al dinamismo de la tecnología informática.

- Cuando se reducen modificaciones se documentan, incluyendo la fecha de actualización, y se difunden dentro del área.

12.5. AUDITORÍA DE PROYECTOS DE DESARROLLO DE S.I

Como se planteó en apartados anteriores, cada desarrollo de un nuevo sistema de información será un proyecto con entidad propia. El proyecto tendrá unos objetivos marcados y afectará a determinadas unidades de la organización. Debe tener un responsable y ser gestionado con técnicas que permitan conseguir los objetivos marcados, teniendo en cuenta los recursos disponibles y las restricciones temporales del mismo. En esa gestión deben participar todas las partes de la organización a las que afecte el sistema.

La auditoría de cada proyecto de desarrollo tendrá un plan distinto dependiendo de los riesgos, la complejidad del mismo y los recursos disponibles para realizar la auditoría. Esto obliga a que sean la pericia y experiencia del auditor las que determinen las actividades del proyecto que se controlarán con mayor intensidad en función de los parámetros anteriores.

En este apartado se definirán objetivos y técnicas de control generales aplicables a cualquier proyecto. El auditor decidirá los objetivos más importantes en función de las características del proyecto y de la fase a auditar.

Como se puede observar en el esquema de agrupación de objetivos de control propuesto en el apartado 3, dentro del desarrollo de sistemas de información se han propuesto cinco subdivisiones, entre las cuales se encuentran: análisis, diseño, construcción e implantación. Estas fases, ampliamente aceptadas en ingeniería del software para el desarrollo, son en concreto las que propone la metodología de desarrollo de sistemas de información Métrica versión 2.1.

Además de estas fases, se ha añadido una subdivisión que contiene los objetivos y técnicas de control concernientes a la aprobación, planificación y gestión del proyecto. La aprobación del proyecto es un hecho previo al comienzo del mismo, mientras que la gestión se aplica a lo largo de su desarrollo. La planificación se realiza antes de iniciarse, pero sufrirá cambios a medida que el proyecto avanza en el tiempo.

Aunque los objetivos de control se han catalogado en función de la fase del proyecto a la que se aplican, la auditoría de un proyecto de desarrollo se puede hacer en dos momentos distintos: a medida que avanza el proyecto, o una vez concluido el mismo. Las técnicas a utilizar y los elementos a inspeccionar, normalmente los productos y documentos generados en cada fase del desarrollo, serán los mismos en ambos casos. La única diferencia es que en el primer caso las conclusiones que vaya aportando el auditor pueden afectar al desarrollo del proyecto, aunque nunca participará en la toma de decisiones del mismo.

12.5.1. Aprobación, planificación y gestión del proyecto

Se consideran en este apartado dos objetivos de control (serie B):

OBJETIVO DE CONTROL B1: El proyecto de desarrollo debe estar aprobado, definido y planificado formalmente.

C-B1-1: Debe existir una orden de aprobación del proyecto que defina claramente los objetivos, restricciones y las unidades afectadas. Se debe comprobar que:

- Existe una orden de aprobación del proyecto refrendada por un órgano competente. El estudio de viabilidad debe haber seguido el cauce establecido.
- En el documento de aprobación están definidos de forma clara y precisa los objetivos del mismo y las restricciones de todo tipo que deben tenerse en cuenta (temporales, recursos técnicos, recursos humanos, presupuesto, etc.).

- Se han identificado las unidades de la organización a las que afecta.

C-BI-2: Debe designarse un responsable o director del proyecto. Se debe comprobar que:

- La designación se ha llevado a cabo según el procedimiento establecido.
- Se le ha comunicado al director su nombramiento junto con toda la información relevante del proyecto.

C-BI-3: El proyecto debe ser catalogado y, en función de sus características, se debe determinar el modelo de ciclo de vida que seguirá. Se debe comprobar que:

- Se ha catalogado y dimensionado el proyecto según las normas establecidas.
- Se han evaluado los riesgos asociados al proyecto, especialmente cuando se van a usar tecnologías no usadas hasta el momento.
- Se ha elegido el ciclo de vida más adecuado al tipo de proyecto de que se trata.
- Se ha hecho uso de la información histórica que se dispone tanto para dimensionar el proyecto y sus riesgos como para seleccionar el ciclo de vida.
- Se prestará especial atención si se elige un ciclo de vida basado en prototipado. En este caso deben cumplirse los requisitos necesarios para aplicarlo con éxito (dificultad de los usuarios para expresar los requisitos y disponibilidad de una herramienta de construcción rápida de prototipos) y debe existir un acuerdo con los usuarios sobre el alcance del prototipo y el objetivo que se persigue con el mismo.

P-BI-4: Una vez determinado el ciclo de vida a seguir, se debe elegir el equipo técnico que realizará el proyecto y se determinará el plan del proyecto. Se debe comprobar que:

- La designación del director del proyecto y del equipo de desarrollo se ha llevado a cabo según el procedimiento establecido.
- Los participantes que pertenezcan a otras áreas (sistemas, comunicaciones, ofimática, etc.) se han solicitado según el protocolo existente.
- Si participa personal externo, los perfiles profesionales son adecuados a las funciones que van a realizar. El contrato cumple el protocolo de contratación.

- Se ha comunicado a todos los miembros del equipo de desarrollo los objetivos del proyecto, la responsabilidad que tendrán en el mismo, las fechas en las que participarán y la dedicación (completa/parcial).

- El plan de proyecto realizado es realista y utiliza la información histórica de la que se disponga para realizar estimaciones.

OBJETIVO DE CONTROL B2: El proyecto se debe gestionar de forma que se consigan los mejores resultados posibles teniendo en cuenta las restricciones de tiempo y recursos. Los criterios usados serán coherentes con los objetivos de las unidades afectadas.

C-B2-1: Los responsables de las unidades o áreas afectadas por el proyecto deben participar en la gestión del proyecto. Se debe comprobar que:

- Se ha constituido formalmente el comité de dirección del proyecto y en él están incluidos los responsables de todas las unidades afectadas.

- El comité tiene una periodicidad de reunión mínima, y en cualquier caso siempre que lo exija el desarrollo del proyecto, debe tener competencia para la asignación de recursos, la revisión de la marcha del proyecto y para modificar el plan del proyecto en función de las revisiones.

- Las reuniones se hacen con un orden del día previo y las decisiones tomadas quedan documentadas en las actas de dicho comité.

- El número de reuniones y la duración de las mismas no superan un límite razonable comparado con la envergadura del proyecto.

C-B2-2: Se debe establecer un mecanismo para la resolución de los problemas que puedan plantearse a lo largo del proyecto. Se debe comprobar que:

- Existen hojas de registro de problemas y que hay alguna persona del proyecto encargada de su recepción, así como un procedimiento conocido de tramitación.

- Hay un método para catalogar y dar prioridad a los problemas, así como para trasladarlos a la persona que los debe resolver, informando si es necesario al director del proyecto y al comité de dirección.

- Se controla la solución del problema y se deja constancia de la misma.

C-B2-3: Debe existir un control de cambios a lo largo del proyecto. Se debe comprobar que:

- Existe un mecanismo para registrar los cambios que pudieran producirse, así como para evaluar el impacto de los mismos.
- La documentación afectada se actualiza de forma adecuada y se lleva un control de versiones de cada producto, consignando la última fecha de actualización.
- Se remite la nueva versión de los documentos actualizados a los participantes en el proyecto.

C-B2-4: Cuando sea necesario reajustar el plan del proyecto, normalmente al finalizar un módulo o fase, debe hacerse de forma adecuada. Se debe comprobar que:

- Se respetan los límites temporales y presupuestarios marcados al inicio del proyecto. Si no es así debe ser aprobado por el comité de dirección.
- Se han tenido en cuenta los riesgos del reajuste.
- Se ha hecho uso de la información histórica que se dispone en el área sobre estimaciones.
- Se notifica el cambio a todas las personas que de una u otra forma participen en el proyecto y se vean afectados.
- Si existe un plan de sistemas, se actualizará en consecuencia.

C-B2-5: Debe hacerse un seguimiento de los tiempos empleados tanto por tarea como a lo largo del proyecto. Se debe comprobar que:

- Existe un procedimiento que permita registrar los tiempos que cada participante del proyecto dedica al mismo y qué tarea realiza en ese tiempo.
- Las productividades que se obtienen para distintos empleados en las mismas tareas son similares y están en consonancia con la información histórica.

C-B2-6: Se debe controlar que se siguen las etapas del ciclo de vida adoptado para el proyecto y que se generan todos los documentos asociados a la metodología usada. Se debe comprobar que:

- Antes de comenzar una nueva etapa se ha documentado la etapa previa y se ha revisado y aceptado, especialmente en las fases de análisis y diseño.
- La documentación cumple los estándares establecidos en el área.
- Se respeta el plan establecido y en caso contrario se toman las medidas oportunas o se procede a la aprobación de una modificación del plan.
- Se respeta el uso de recursos previamente establecido.

C-B2-7: Cuando termina el proyecto se debe cerrar toda la documentación del mismo, liberar los recursos empleados y hacer balance. Se debe comprobar que:

- La documentación del proyecto es completa y está catalogada perfectamente para accesos posteriores.
- Los recursos, tanto personales como materiales, se ponen a disposición del área o departamento del que provienen.
- El comité de dirección y el director del proyecto hacen balance del proyecto, estudiando los posibles problemas y sus causas, los cambios de plan, etc. Toda esta información se registra en los archivos históricos sobre estimaciones y problemas.
- La nueva aplicación se incorpora al catálogo de aplicaciones existentes con toda la información relevante de la misma.

12.5.2. Auditoría de la fase de análisis

La fase de análisis pretende obtener un conjunto de especificaciones formales que describan las necesidades de información que deben ser cubiertas por el nuevo sistema de una forma independiente del entorno técnico.

Esta fase se divide en dos módulos:

12.5.2.1. Análisis de Requisitos del Sistema (ARS)

En este módulo se identificarán los requisitos del nuevo sistema. Se incluirán tanto los requisitos funcionales como los no funcionales, distinguiendo para cada uno de ellos su importancia y prioridad.

A partir del conocimiento del sistema actual y sus problemas asociados, junto con los requisitos que se exigirán al nuevo sistema, se determinarán las posibles soluciones, alternativas que satisfagan esos requisitos y de entre ellas se elegirá la más adecuada. Se consideran dos objetivos de control (serie C):

***OBJETIVO DE CONTROL C1*:** Los usuarios y responsables de las unidades a las que afecta el nuevo sistema establecerán de forma clara los requisitos del mismo.

C-C1-1: En el proyecto deben participar usuarios de todas las unidades a las que afecte el nuevo sistema. Esta participación, que se hará normalmente a través de entrevistas, tendrá especial importancia en la definición de requisitos del sistema. Se debe comprobar que:

- Existe un documento aprobado por el comité de dirección en el que se determina formalmente el grupo de usuarios que participará en el proyecto.
- Los usuarios elegidos son suficientemente representativos de las distintas funciones que se llevan a cabo en las unidades afectadas por el nuevo sistema.
- Se les ha comunicado a los usuarios su participación en el proyecto, informándoles del ámbito del mismo y de qué es lo que se espera de ellos, así como la dedicación estimada que les supondrá esta tarea.

C-C1-2: Se debe realizar un plan detallado de entrevistas con el grupo de usuarios del proyecto y con los responsables de las unidades afectadas que permita conocer cómo valoran el sistema actual y lo que esperan del nuevo sistema. Se debe comprobar que:

- Existe un plan consensuado con el comité de dirección que detalla para cada entrevista la fecha, hora y lugar, tipo de entrevista (individual, en grupo, por escrito, etc.) y un guión de los aspectos que en ella se tratarán.
- Se entrevista a todos los integrantes en el grupo de usuarios y a todos los responsables de las unidades afectadas.
- Se remite el guión a los entrevistados con tiempo suficiente para que éstos puedan preparar la entrevista y la documentación que deseen aportar a la misma.
- El guión incluye todas las cuestiones necesarias para obtener información sobre las funciones que el entrevistado realiza en su unidad y los problemas que necesita resolver.

Una vez documentadas las entrevistas, se contrastan las conclusiones de las mismas con los entrevistados.

C-C1-3: A partir de la información obtenida en las entrevistas, se debe documentar el sistema actual así como los problemas asociados al mismo. Se debe obtener también un catálogo con los requisitos del nuevo sistema. Se debe comprobar que:

- Se ha realizado un modelo físico del sistema actual, incluyendo los objetivos y funciones de cada unidad, así como sus flujos de entrada y salida de información.
- Se han catalogado los problemas del sistema actual así como que estos problemas son reales.
- Se han realizado el modelo lógico de datos y el modelo lógico de procesos del sistema actual, así como que éstos son correctos y que se han llevado a cabo con las técnicas usadas en el área.
- Existe el catálogo de requisitos que están justificados.
- Los requisitos son concretos y cuantificables, de forma que pueda determinarse el grado de cumplimiento al final del proyecto.
- Cada requisito tiene una prioridad y está clasificado en funcional o no funcional.
- El catálogo de requisitos ha sido revisado y aprobado por el grupo de usuarios y por el comité de dirección, constituyendo a partir de este momento el "contrato" entre éstos y el equipo que desarrolla el proyecto.

C-C1-4: Debe existir un procedimiento formal para registrar cambios en los requisitos del sistema por parte de los usuarios. Se debe comprobar que:

- El procedimiento existe y está aprobado.
- Es coherente con el procedimiento de control del cambio general para el proyecto.

OBJETIVO DE CONTROL C2: En el proyecto de desarrollo se utilizará la alternativa más favorable para conseguir que el sistema cumpla los requisitos establecidos.

C-C2-1: Dados los requisitos del nuevo sistema se deben definir las diferentes alternativas de construcción con sus ventajas e inconvenientes. Se evaluarán las alternativas y se seleccionará la más adecuada. Se debe comprobar que:

- Existe un documento en el que se describen las distintas alternativas.
- Hay más de una alternativa, y en caso contrario, que no existe realmente otra posible.
- Cada alternativa está descrita desde un punto de vista lógico (al menos modelo lógico de procesos) y es coherente con los requisitos establecidos.
- Si existe en el mercado al un producto que cumpla con unas mínimas garantías los requisitos especificados, una de las alternativas debe ser su compra.
- Si no lo impiden las características del proyecto una de las alternativas debe ser el desarrollo del sistema por parte de una empresa externa.
- Se han evaluado las ventajas e inconvenientes de cada alternativa de forma objetiva (análisis coste/beneficio por ejemplo), así como los riesgos asociados.
- El comité de dirección ha seleccionado una alternativa como la más ventajosa y es realmente la mejor para la organización.

C-C2-2: La actualización del plan de proyecto seguirá los criterios ya comentados.

12.5.2.2. Especificación Funcional del Sistema (EFS)

Una vez conocido el sistema actual, los requisitos del nuevo sistema y la alternativa de desarrollo más favorable, se elaborará una especificación funcional detallada del sistema que sea coherente con lo que se espera de él.

La participación de usuarios en este módulo y la realización de entrevistas siguen las pautas ya especificadas en el análisis de requisitos del sistema, por lo que se pasa por alto la comprobación de estos aspectos. El grupo de usuarios y los responsables de las unidades afectadas deben ser la principal fuente de información. Se considera un único objetivo de control (serie D):

OBJETIVO DE CONTROL D1: El nuevo sistema debe especificarse de forma completa desde el punto de vista funcional, contando esta especificación con la aprobación de los usuarios.

C-D1-1: Se debe realizar un modelo lógico del nuevo sistema, incluyendo Modelo Lógico de Procesos (MLP) y Modelo Lógico de Datos (MLD). Ambos deben ser consolidados para garantizar su coherencia. Se debe comprobar que:

- Se ha partido de los modelos realizados en el análisis de requisitos del sistema.
- Existe el MLP, se ha realizado con la técnica adecuada (normalmente diagramas de flujos de datos) y es correcto técnicamente. Describirá qué debe realizar el sistema sin entrar en la forma en que lo hará. Los procesos manuales deben estar diferenciados. Los usuarios deben entender las convenciones de símbolos usadas.
- En el diagrama de contexto están reflejados todos los agentes externos, incluidos otros sistemas con los que el sistema intercambia información. Para cada flujo de datos de entrada o de salida debe estar documentado el contenido, la frecuencia, suceso que lo origina, etc.
- Existe el MLD, se ha realizado con la técnica adecuada (normalmente modelo entidad-relación o diagramas de estructura de datos) y es correcto técnicamente. Debe estar normalizado al menos hasta la tercera forma normal.
- En el MLD están reflejadas todas las entidades con sus atributos y claves, así como las relaciones entre las mismas.
- El MLP y el MLD son coherentes entre sí. La consolidación se debe hacer usando técnicas adecuadas (Historia de la vida de las entidades, por ejemplo).
- El MLP y el MLD han sido aprobados por los usuarios y por el comité de dirección.

C-D1-2: Debe existir el diccionario de datos o repositorio. Se debe comprobar que:

- Existe el diccionario de datos, es correcto y se gestiona de forma automatizada.
- Se respetan en su gestión todos los procedimientos de control de cambios.

C-D1-3: Debe definirse la forma en que el nuevo sistema interactuará con los distintos usuarios. Ésta es la parte más importante para el usuario porque definirá su forma de trabajo con el sistema. Se debe comprobar que:

- Se han descrito con suficiente detalle las pantallas a través de las cuales el usuario navegará por la aplicación, incluyendo todos los campos significativos, teclas de función disponibles, menús, botones, etc. Si hay normas de diseño o estilo de pantallas en el área, se verificará que se respetan.

- Se han descrito con suficiente detalle los informes que se obtendrán del sistema y los formularios asociados, si éstos existen. Si hay normas de diseño o estilo de informes y formularios en el área, se verificará que se respetan.

- La interfaz de usuario se ha aprobado por el grupo de usuarios y por el comité de dirección.

C-D1-4: La especificación del nuevo sistema incluirá los requisitos de seguridad, rendimiento, copias de seguridad y recuperación, etc. Se debe comprobar que:

- Esta información se ha solicitado a los usuarios en las entrevistas correspondientes a este módulo y se ha documentado y contrastado.

- Se han añadido estos requisitos al catálogo de requisitos ya realizado en el ARS.

C-D1-5: Se deben especificar las pruebas que el nuevo sistema debe superar para ser aceptado. Se debe comprobar que:

- Se ha elaborado el plan de pruebas de aceptación del sistema, que éste es coherente con el catálogo de requisitos y con la especificación funcional del sistema y que es aceptado por el grupo de usuarios y por el comité de dirección.

- El plan de pruebas de aceptación tiene en cuenta todos los recursos necesarios.

C-D1-6: La actualización del plan de proyecto seguirá los criterios ya comentados, detallándose en este punto en mayor medida la entrega y transición al nuevo sistema.

12.5.3. Auditoría de la fase de diseño

En la fase de diseño se elaborará el conjunto de especificaciones físicas del nuevo sistema que servirán de base para la construcción del mismo. Hay un único módulo:

12.5.3.1. Diseño Técnico del Sistema (DTS)

A partir de las especificaciones funcionales, y teniendo en cuenta el entorno tecnológico, se diseñará la arquitectura del sistema y el esquema externo de datos. Se considera un único objetivo de control (serie E):

***OBJETIVO DE CONTROL E1*:** Se debe definir una arquitectura física para el sistema coherente con la especificación funcional que se tenga y con el entorno tecnológico elegido.

C-E1-1: El entorno tecnológico debe estar definido de forma clara y ser conforme a los estándares del departamento de informática. Se debe comprobar que:

- Están perfectamente definidos todos los elementos que configuran el entorno tecnológico para el proyecto (servidores, computadores personales, periféricos, sistemas operativos, conexiones de red, protocolos de comunicación, sistemas gestores de bases de datos, compiladores, herramientas CASE, *middleware* en caso de programación cliente/servidor, librerías, etc.).

- Se dispone de los elementos seleccionados, están dentro de los estándares del departamento de informática y son capaces de responder a los requisitos establecidos de volúmenes, tiempos de respuesta, seguridad, etc.

C-E1-2: Se deben identificar todas las actividades físicas a realizar por el sistema y descomponer las mismas de forma modular. Se debe comprobar que:

- Se han documentado todas las actividades físicas que debe realizar el sistema.

- El catálogo de actividades es coherente con las funciones identificadas en el MLP del módulo EFS.

- Se han identificado las actividades que son comunes, así como las que ya existan en las librerías generales del área.

- Existe el documento con el diseño de la estructura modular del sistema, se ha realizado con una técnica adecuada (Diagramas de estructura de cuadros por ejemplo) y es correcto.

- El tamaño de los módulos es adecuado, el factor de acoplamiento entre ellos es mínimo y la cohesión interna de cada módulo es máxima.

- Los módulos se diseñan para poder ser usados por otras aplicaciones si fuera necesario.

- Los componentes o programas del nuevo sistema se han definido con detalle a partir del diseño modular, la definición es correcta y sigue los estándares del área. La descripción de los componentes es suficiente para permitir su programación por parte de un programador sin conocimiento previo del sistema. Se deben especificar los requisitos de operación de los componentes.

- Se han detallado las interfaces de datos y control con otros módulos y sistemas, así como la interfaz de usuario ya especificada en el módulo EFS.

C-EI-3: Se debe diseñar la estructura física de datos adaptando las especificaciones del sistema al entorno tecnológico. Se debe comprobar que:

El modelo físico de datos está basado en el MLD obtenido en el módulo EFS e incluye todas las entidades, relaciones, claves, vistas, etc.

Tiene en cuenta el entorno tecnológico y los requisitos de rendimiento para los volúmenes y frecuencias de acceso estimados.

Si incluye algún incumplimiento de las normas, está justificada.

C-EI-4: Se debe diseñar un plan de pruebas que permita la verificación de los distintos componentes del sistema por separado, así como el funcionamiento de los distintos subsistemas y del sistema en conjunto. Se debe comprobar que:

- Existe el plan de pruebas y contempla todos los recursos necesarios para llevarlas a efecto.

- Las personas que realizarán las pruebas de verificación son distintas a las que han desarrollado el sistema.

- Es adecuado para validar cada uno de los componentes del sistema, incluyendo pruebas del tipo caja blanca para cada módulo. Tendrán en cuenta todas las posibles condiciones lógicas de ejecución, además de posibles fallos del hardware o software de base.

- Permite validar la integración de los distintos componentes y el sistema en conjunto.

C-EI-5: La actualización del plan de proyecto seguirá los criterios ya comentados.

12.5.4. Auditoría de la fase de construcción

En esta fase se programarán y probarán los distintos componentes y se pondría en marcha todos los procedimientos necesarios para que los usuarios puedan trabajar con el nuevo sistema. Estará basado en las especificaciones físicas obtenidas en la fase de diseño. Hay dos módulos.

12.5.4.1. Desarrollo de los Componentes del Sistema (DCS)

En este módulo se realizarán los distintos componentes, se probarán tanto individualmente como de forma integrada, y se desarrollarán los procedimientos de operación. Se considera un único objetivo de control (serie F):

OBJETIVO DE CONTROL F1: Los componentes o módulos deben desarrollarse usando técnicas de programación correctas.

C-F1-1: Se debe preparar adecuadamente el entorno de desarrollo y de pruebas, así como los procedimientos de operación, antes de iniciar el desarrollo. Se debe comprobar que:

- Se han creado e inicializado las bases de datos o archivos necesarios y que cumplen las especificaciones realizadas en el módulo de diseño.
- En ningún momento se trabaja con información que se encuentra en explotación.
- Se han preparado los procedimientos de copia de seguridad.
- Se han preparado los editores, compiladores, herramientas, etc. necesarios.
- Están disponibles los puestos de trabajo y el acceso a los equipos, redes, etc.
- Están disponibles todos los elementos lógicos y físicos para realizar las pruebas unitarias de los componentes y las pruebas de integración.
- Están documentados todos los procedimientos de operación para cuando el sistema esté en explotación.

C-FI-2: Se debe programar, probar y documentar cada uno de los componentes identificados en el diseño del sistema. Se debe comprobar que:

- Se han desarrollado todos los componentes o módulos.
- Se han seguido los estándares de programación y documentación del área, el código es estructurado, está bien sangrado y contiene comentarios suficientes.
- Se ha probado cada componente y se ha generado el informe de prueba. Si los resultados de las pruebas no son satisfactorios, se modifica el código y se vuelve a realizar la prueba. Si se detecta un fallo de especificación o diseño, el proyecto se actualizará según el procedimiento establecido para ello.

C-FI-3: Deben realizarse las pruebas de integración para asegurar que las interfaces, entre los componentes o módulos funcionan correctamente. Se debe comprobar que:

- Las pruebas de integración se han llevado a cabo según lo especificado en el plan de pruebas realizado en el módulo de diseño.
- Se han evaluado las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.
- No han participado los usuarios. En las pruebas de integración sólo debe participar el equipo de desarrollo.

12.5.4.2. Desarrollo de los Procedimientos de Usuario (DPU)

En este módulo se definen los procedimientos y formación necesarios para que los usuarios puedan utilizar el nuevo sistema adecuadamente. Fundamentalmente se trata de la instalación, la conversión de datos y la operación/explotación. Se considera un único objetivo de control (serie G):

OBJETIVO DE CONTROL GI: Al término del proyecto, los futuros usuarios deben estar capacitados y disponer de todos los medios para hacer uso del sistema.

C-G1-1: El desarrollo de los componentes de usuario debe estar planificado. Se debe comprobar que:

- En el plan del proyecto está incluido el plan para el desarrollo de los procedimientos de usuario e incluye todas las actividades y recursos necesarios.

- Los procedimientos se llevan a cabo después de tener la especificación funcional del sistema y antes de la implantación del mismo.

C-G1-2: Se deben especificar los perfiles de usuario requeridos para el nuevo sistema. Se debe comprobar que:

- Están definidos los distintos perfiles de usuario requeridos para la implantación y explotación del nuevo sistema.
- Para cada perfil se ha definido el rango de fechas y la dedicación necesaria.

C-G1-3: Se deben desarrollar todos los procedimientos de usuario con arreglo a los estándares del área. Se debe comprobar que:

- Están desarrollados todos los procedimientos de usuario, recopilados formando el manual de usuario, y son coherentes con las actividades descritas en EFS.
- Cada procedimiento describe claramente qué realiza, el perfil de usuario asociado, así como los recursos que son necesarios (equipos, consumibles, periféricos especiales, espacio, etc.).
- Los manuales de usuario y el resto de procedimientos cumplen los estándares del área y llevan asociado su control de versiones.

C-G1-4: A partir de los perfiles actuales de los usuarios, se deben definir los procesos de formación o selección de personal necesarios. Se debe comprobar que:

- La comparación de perfiles de usuarios y recursos requeridos con los actuales es realista y los procedimientos que se derivan son adecuados y están aprobados por los responsables de las unidades afectadas.
- Los procedimientos de formación están individualizados y se adaptan a cada persona, y se le ha comunicado a cada usuario el plan de formación que seguirá.
- Se han definido y preparado los recursos necesarios para impartir la formación (aulas, medios audiovisuales, material para los asistentes, tutoriales, etc.).

C-G1-5: Se deben definir los recursos materiales necesarios para el trabajo de los usuarios con el nuevo sistema. Se debe comprobar que:

- Se han determinado los recursos necesarios para cada usuario (consumibles, periféricos especiales, espacio, etc.).

- Se han comparado con los recursos existentes y se ha planificado el alquiler, leasing, adquisición, etc. de los recursos no disponibles dentro de plazo.

12.5.5. Auditoría de la fase de implantación

En esta fase se realizará la aceptación del sistema por parte de los usuarios, además de las actividades necesarias para la puesta en marcha. Hay un único módulo:

12.5.5.1. Pruebas, Implantación y Aceptación del Sistema (PIA)

Se verificará en este módulo que el sistema cumple con los requisitos establecidos en la fase de análisis. Una vez probado y aceptado se pondrá en explotación. Se consideran dos objetivos de control (serie H):

***OBJETIVO DE CONTROL H1*:** El sistema debe ser aceptado formalmente por los usuarios antes de ser puesto en explotación.

C-H1-1: Se deben realizar las pruebas del sistema que se especificaron en el diseño del mismo. Se debe comprobar que:

- Se prepara el entorno y los recursos necesarios para realizar las pruebas.

- Las pruebas se realizan y permiten verificar si el sistema cumple las especificaciones funcionales y si interactúa correctamente con el entorno, incluyendo interfaces con otros programas, recuperación ante fallos, copias de seguridad, tiempos de respuesta, etc.

- Se han evaluado los resultados de las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.

IC-H1-2: El plan de implantación y aceptación se debe revisar para adaptarlo a la situación final del proyecto. Se debe comprobar que:

- Se revisa el plan de implantación original y se documenta adecuadamente.

- Está incluida la instalación de todos los componentes desarrollados, así como los elementos adicionales (librerías, utilidades, etc.).

- Incluye la inicialización de datos y la conversión si es necesaria.
- Especifica los recursos necesarios para cada actividad, así como que el orden marcado para las actividades es compatible.
- Se ha tenido en cuenta la información histórica sobre estimaciones.

C-H1-3: El sistema debe ser aceptado por los usuarios antes de ponerse en explotación. Se debe comprobar que:

- Se sigue el plan de pruebas de aceptación aprobado en la fase de análisis, que debe incluir la conversión de datos y la explotación.
- Las pruebas de aceptación son realizadas por los usuarios.
- Se evalúan los resultados de las pruebas y se han tomado las acciones correctoras necesarias para solventar las incidencias encontradas, actualizándose el proyecto en consecuencia.
- El grupo de usuarios y el comité de dirección firman su conformidad con las pruebas de aceptación.

OBJETIVO DE CONTROL H2: El sistema se pondrá en explotación formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.

C-H2-1: Se deben instalar todos los procedimientos de explotación. Se debe comprobar que:

- Se han instalado además del sistema principal todos los procedimientos auxiliares, por ejemplo copias, recuperación, etc., tanto manuales como automáticos.
- Están documentados de forma correcta.
- Los usuarios han recibido la formación necesaria y tienen en su poder toda la documentación necesaria, fundamentalmente manuales de usuario.
- Se han eliminado procedimientos antiguos que sean incompatibles con el nuevo sistema.

C-H2-2: Si existe un sistema antiguo, el sistema nuevo se pondrá en explotación de forma coordinada con la retirada del antiguo, migrando los datos si es necesario. Se debe comprobar que:

- Hay un período de funcionamiento en paralelo de los dos sistemas, hasta que el nuevo sistema esté funcionando con todas las garantías. Esta situación no debe prolongarse más tiempo del necesario.

- Si el sistema antiguo se va a mantener para obtener información se debe dejar en explotación en modo de sólo consulta.

- Los datos se convierten de acuerdo al procedimiento desarrollado y se verifica la consistencia de la información entre el sistema nuevo y el antiguo.

C-H2-3: Debe firmarse el final de la implantación por parte de los usuarios. Se debe comprobar que:

- Existe el documento y que ha sido firmado por el comité de dirección y por el grupo de usuarios.

- Contiene de forma explícita la aceptación de la implantación correcta del sistema.

C-H2-4: Se debe supervisar el trabajo de los usuarios con el nuevo sistema en las primeras semanas para evitar situaciones de abandono de uso del sistema. Se debe comprobar que:

- El índice de utilización del sistema es adecuado a los volúmenes que se esperaban para cada una de las áreas afectadas por el nuevo sistema.

- Se ha comprobado, al menos informalmente, la impresión de los usuarios respecto al nuevo sistema.

C-H2-5: Para terminar el proyecto se pondrá en marcha el mecanismo de mantenimiento. Se debe comprobar que:

- El mecanismo existe y está aprobado por el director del proyecto, por el comité de dirección y por el área de mantenimiento, si ésta existiese.

- Tiene en cuenta los tiempos de respuesta máximos que se pueden permitir ante situaciones de no funcionamiento.

- El procedimiento a seguir ante cualquier problema o para el mantenimiento del sistema será conocido por todos los usuarios. Incluirá al menos la persona de contacto, teléfono, esquema de la información a aportar, etc.

12.6. CONCLUSIONES

A pesar de ser una de las actividades principales de la informática, el desarrollo de software no ha conseguido alcanzar de forma general unos parámetros de calidad aceptables. Este hecho, unido a la naturaleza especial del software y su difícil validación, convierten al proceso de desarrollo y su estandarización en las claves para cambiar la situación.

Todas las actividades que configuran el proceso de desarrollo tienen la misma importancia a la hora de realizar la auditoría, pues aunque se pueda pensar que la actividad más importante es la programación, se ha demostrado que los errores en las actividades iniciales de los proyectos son más costosos que los que se producen al final de los mismos.

Por otra parte, no parece lógico que los procesos involucrados en el desarrollo de software se estandaricen a lo largo de un proyecto concreto. Es imprescindible que los proyectos de desarrollo se lleven a cabo en el seno de una organización consolidada. Por ello, la organización se convierte en otro elemento crítico a tener en cuenta por el auditor.

Especial mención merecen las nuevas herramientas y técnicas (CASE, programación orientada a objetos, lenguajes de cuarta generación, RAD, prototipado, etc.), que al alterar en cierta medida el proceso tradicional de desarrollo de la ingeniería del software, pasan a ser elementos esenciales a estudiar en un proceso de auditoría.

En este capítulo se han expuesto distintos objetivos de control que de ninguna manera deben interpretarse como un modelo cerrado. El auditor aplicará los objetivos y niveles de cumplimiento mínimos que considere adecuados en función del proyecto y de las peculiaridades de cada organización.

12.7. LECTURAS RECOMENDADAS

Computer Audit, Control and Security. Moeller, R. John Wiley & Sons, 1989.

Técnicas de la auditoría informática. Yann Derrien. Ed. Marcombo, 1994.

Control interno, auditoría y seguridad informática. Coopers & Lybrand, 1996.

Auditoría en centros de cómputo. David H. Li. Ed. Trillas, 1990.

12.8. CUESTIONES DE REPASO

1. ¿Qué factores contribuyen a la importancia de la auditoría de desarrollo?
2. ¿Qué aspectos se deben comprobar respecto a las funciones del área de desarrollo?
3. Comente la importancia, desde el punto de vista de la auditoría, de la formación que deben poseer los profesionales de desarrollo.
4. ¿Qué procedimiento utilizaría para valorar la motivación del personal de desarrollo?
5. ¿Qué repercusiones tiene la existencia de herramientas CASE en el ámbito del desarrollo?
6. Describa diversos procedimientos de Análisis, Evaluación y Selección de herramientas de desarrollo que haya utilizado o conozca.
7. ¿Qué riesgos entraña la subcontratación del desarrollo?
8. ¿Cómo afecta el modelo de ciclo de vida que se adopte en un proyecto a la auditoría a realizar sobre el mismo?
9. ¿Cree que la "trazabilidad" de los requisitos resulta importante en un desarrollo informático?
10. Exponga cómo debería ser la participación del usuario a lo largo de las distintas fases de la metodología Métrica.

CAPÍTULO 13

AUDITORÍA DEL MANTENIMIENTO

Juan Carlos Granja Álvarez

13.1. INTRODUCCIÓN A LA AUDITORÍA INFORMÁTICA DEL MANTENIMIENTO DEL SOFTWARE

Nunca se ha prestado demasiada atención al estudio de la Auditoría Informática en esta etapa, ni se le ha dedicado el esfuerzo necesario que por su alto nivel de coste merece. En ocasiones se ha hablado de una etapa en la que sólo se apercibían parte de los problemas y apenas se empleaba un mínimo esfuerzo en aplicar técnicas de auditoría con lo que surgía el efecto ICEBERG con el que algunos autores han denominado al hecho de que sólo se aprecia una pequeña parte de la problemática que encierra.

Varias investigaciones y experiencias revelan que la etapa de mantenimiento consume la mayor parte de los recursos empleados en un proyecto software. Por tanto, esta etapa debe ser especialmente considerada en los estudios de productividad y de la Auditoría Informática. La mantenibilidad, factor crítico de estudio en Auditoría Informática del Mantenimiento, es el factor de calidad que engloba todas aquellas características del software destinadas a hacer que el producto sea más fácilmente mantenible y, en consecuencia, a conseguir una mayor productividad durante la etapa de mantenimiento. En este capítulo se propone un modelo empírico de estimación de costes de mantenimiento centrado en este factor de calidad, así como el método para su implementación. Finalmente se consideran algunos casos prácticos que refuerzan la validez del modelo.

El control y evaluación de la Mantenibilidad puede ser uno de los factores determinantes en el estudio de la Auditoría Informática en la Etapa de Mantenimiento del Software.

Frecuentemente se olvida que los esfue os de auditoría en la etapa de Mantenimiento se plasman en las primeras etapas de desarrollo del software. En las especificaciones del software y en la llamada Ingeniería de Reqaisitos, se plasman los primeros pasos de los aspectos que van a determinar el esfuerzo o no dificultad de mantenimiento del software.

Podemos decir que la Mantenibilidad va a ser un factor determinante para la Auditoría Informática del Mantenimiento del Software. Vamos a centrar el estudio de este tema en todo lo que rodea la facilidad de mantenimiento del software y los aspectos a auditar.

Es frecuente que las empresas de software busquen la máxima productividad en el desarrollo de sus productos, dejando en un segundo lugar a la etapa de mantenimiento. Esto constituye un lamentable error ya que, como muchos estudios revelan, esta etapa es la que más recursos consume (más del 60% de los recursos empleados en todo el proyecto) [CANN72, WIEN84, HARR90]. Todo ello nos lleva a un profundo estudio de las técnicas de Auditoría en esta etapa.

Si la productividad en la etapa de mantenimiento es baja puede suceder, además de las evidentes implicaciones económicas, que el equipo humano que desarrolló el producto tenga que dedicarse a tiempo completo a su mantenimiento. Consecuentemente, si la empresa quiere abordar nuevos proyectos tendrá que incluir un nuevo equipo en su plantilla. Esto implica el desaprovechamiento, al menos parcial, de la experiencia adquirida por el equipo anterior, que sería de gran valor en los nuevos proyectos. Por otro lado se requiere una labor de formación del nuevo equipo hasta adquirir el conocimiento necesario sobre los métodos y herramientas utilizados por la empresa de software.

La productividad en la etapa de mantenimiento está directamente relacionada con la mantenibilidad del producto. La mantenibilidad es un factor de calidad que engloba todas aquellas características del software destinadas a hacer que el producto sea más fácilmente mantenible. Por tanto, va a ser un parámetro decisivo a la hora de auditar esta etapa.

Se propone un modelo de estimación del costo de mantenimiento que permite aprovechar las experiencias en proyectos previos. Se toma como punto de partida el conocido modelo de estimación de costes elaborado por Boehm (COCOMO), al que se incorporan unos índices que miden la mantenibilidad del producto y que afectan de manera importante al coste de mantenimiento.

13.2. LISTAS DE COMPROBACIÓN EN AUDITORÍA INFORMÁTICA DEL MANTENIMIENTO

Siguiendo un enfoque clásico de la Auditoría Informática del Mantenimiento, nos encontramos con las técnicas de utilización de diferentes tipos de listas de comprobación.

Cara a la revisión del software en la etapa de mantenimiento, podríamos resaltar cinco grandes bloques o enfoques hacia los cuales poder orientar las preguntas:

1. ¿Se han tenido en cuenta las implicaciones laterales asociadas con el cambio?

2. ¿Se han tenido en cuenta los aspectos documentales en cuarto a evaluar y aprobar la petición de cambios?

3. ¿Se ha documentado el cambio, una vez realizado y procediéndose a dar información a todos los que se ven implicados en el proceso?

4. En cuanto a las revisiones técnicas formales, ¿se han realizado las adecuadas?

5. ¿Se ha hecho una revisión de aceptación final para asegurar que toda la arquitectura software, fue actualizada y probada y se procedió a los cambios adecuadamente?

La utilización de grandes bloques como los mencionados nos va a permitir centrar nuestro esfuerzo de auditoría informática, si bien vemos que la problemática persiste en buscar aquellos aspectos que con el menor esfuerzo de auditoría nos permitan llegar a auditar y conseguir la mayor cantidad de información que sea posible.

Surge así la necesidad de centrar el esfuerzo de auditoría en un factor que pueda ser determinante, tal como es la Mantenibilidad en la etapa de Mantenimiento del Software.

13.3. MODELIZACIÓN EN LA ETAPA DE MANTENIMIENTO

Podemos tomar como referente el COCOMO (COnstructive COst MOdel), que es un modelo de estimación de costes de proyectos software creado por Boehm en 1981 a partir de datos recogidos de 63 proyectos [BOEH81]. El importante número de proyectos tratados y la esmerada elaboración del modelo hacen que su validez perdure

hasta la actualidad. Este modelo ofrece fórmulas empíricas de estimación de costes o esfuerzos software.

Tras aplicar la versión inicial del modelo a una amplia variedad de entornos se comprobó que no bastaba con un único modo de desarrollo, por lo que se plantearon tres modos (orgánico, *semidetached* y *embedded)* en función de varias características: tamaño, necesidades de comunicación, experiencia en proyectos similares, etc.

Por otro lado, se ofrecen tres versiones del modelo: básico, intermedio y detallado. El básico es adecuado para estimaciones rápidas, aunque sin una gran precisión. El intermedio considera 15 atributos del proyecto (fiabilidad requerida, tamaño de la base de datos, restricciones de memoria, tiempo de respuesta requerido, etc.) cuya valoración actúa como factor multiplicador en el modelo. La versión detallada considera las estimaciones en cada una de las etapas del ciclo de vida del proyecto.

La versión básica del modelo ofrece las siguientes fórmulas de cálculo del **esfuerzo de desarrollo** (medido en MM=month-man u hombre-mes):

Modo orgánico	$MM_{DES} = 2.4\ KS^{1.05}$
Modo semidetached	$MM_{DES} = 3.0\ KS^{1.12}$
Modo embedded	$MM_{DES} = 3.6\ KS^{1.20}$

Siendo KS = Estimación del tamaño del programa (en miles de líneas).

Para la estimación del **esfuerzo de mantenimiento** se necesita un nuevo parámetro: el Tráfico de Cambio Anual (TCA), que consiste en la proporción de instrucciones fuente que sufren algún cambio durante un año, bien sea por adición o por modificación.

$$TCA = \frac{NLN + NLM}{NLI}$$

NLN = Número de líneas nuevas
NLM = Número de líneas modificadas
NLI = Número de líneas inicial

Así, el esfuerzo en la etapa de mantenimiento, según el modelo COCOMO, viene dado como producto del esfuerzo de desarrollo y el tráfico de cambio anual.

$$MM_{MANT} = TCA\ MM_{DES}$$

13.4. MODELO DE ESTIMACIÓN EN EL MANTENIMIENTO

La mantenibilidad es, sin duda, el factor de calidad del software con mayor influencia en la etapa de mantenimiento y, por tanto, elemento decisivo de referencia en los estudios de Auditoría Informática del Mantenimiento. Un estudio realizado por W. Itzfeld en Alemania, recogido por Wallmüller en [WALL94] presenta un *ranking*

de utilización de métricas de calidad en el cual las métricas de mantenibilidad se encuentran en primer lugar, empleadas por un 67% de los encuestados.

Boehm [BOEH79] reconocía la importancia de la mantenibilidad. Uno de sus estudios indicaba que el esfuerzo de mantenimiento de un software de baja mantenibilidad puede estar en relación de 40 a 1 con respecto al esfuerzo de nuevos desarrollos. Es decir, existe una relación de dependencia entre las características de mantenibilidad del software desarrollado y el esfuerzo de mantenimiento, lo cual es bastante evidente.

Por tanto, para el cálculo del coste estimado de mantenimiento hemos de considerar un factor que indique el grado de mantenibilidad o facilidad de mantenimiento del producto. Tomando como punto de partida la fórmula de estimación del esfuerzo de mantenimiento del modelo COCOMO de Boehm, se va a incluir en ella dicho factor que denominamos **índice de mantenibilidad,** y que va a ser función de algunas medidas del software desarrollado:

$$MM_{MANT} = TCA\ MM_{DES}\ I_{MANT}$$

$$I_{MANT} = f(X_1, X_2, \ldots, X_n)$$

Este índice va a mostrar el grado de mantenibilidad o facilidad de mantenimiento del producto de forma que valores grandes expresan baja mantenibilidad mientras que los valores bajos indican alta mantenibilidad. Al mismo tiempo va a ser un buen indicador de la productividad en la etapa de mantenimiento.

Así pues, nuestro principal objetivo consiste en determinar qué forma ha de tener este índice. Dicho de otro modo, se trata de obtener la relación que existe entre el esfuerzo estimado de mantenimiento y aquellas características que hacen que el producto sea más o menos mantenible.

Dos son, pues, los pasos a seguir para la normalización del modelo:

a) Establecimiento de las métricas de mantenibilidad.

b) Obtención de las funciones de mantenibilidad que relacionan las métricas establecidas con el índice de mantenibilidad.

Previamente a abordar estos dos puntos y teniendo en cuenta las tres actividades que conforman una acción de mantenimiento, el índice de mantenibilidad se va a descomponer a su vez en tres índices: índice de comprensibilidad, índice de modificabilidad e índice de testeabilidad.

13.4.1. Elementos de la mantenibilidad

Una acción de mantenimiento se puede descomponer en tres actividades:

- **Comprensión** del cambio a realizar.
- **Modificación** o realización del cambio.
- **Prueba** de colección del cambio realizado.

Son tres tareas claramente diferenciadas que se realizan una tras otra, por lo que el esfuerzo de mantenimiento se puede considerar como suma de los tres esfuerzos: comprensión, modificación y prueba.

$$MM_{MANT} = MM_C + MM_M + MM_T$$

Así pues, vamos a tener tres índices de mantenibilidad, I_C, I_M e I_T que relacionan los parámetros del proyecto, TCA y MMDES con los tres componentes del esfuerzo de mantenimiento: MM_C, MM_M y MM_T

$$MM_C = TCA\ MM_{DES}\ I_C$$
$$MM_M = TCA\ MM_{DES}\ I_M$$
$$MM_T = TCA\ MM_{DES}\ I_T$$

En consecuencia, el índice de mantenibilidad, IMANT vendrá dado por la suma de los tres índices anteriores:

$$I_{MANT} = I_C + I_M + I_T$$

I_{MANT} =Índice de mantenibilidad
I_C = Índice de comprensibilidad
I_M - Índice de modificabilidad
I_T =Índice de testeabilidad

El esfuerzo total de mantenimiento:

$$MM_{MANT} = MM_C + MM_M + MM_T = TCA\ MM_{DES}\ (I_C + I_M + I_T)$$

13.4.2. Métricas de mantenibilidad

El modelo aquí propuesto, y que ha sido empleado en los casos de estudio, considera tres características, cada una de las cuales afecta de manera directa a un componente de la mantenibilidad:

X_C: *Métrica de comprensibilidad*: Número de líneas de comentario por cada 100 líneas de código. La estrecha relación entre la documentación interna del código (o autodocumentación) y el esfuerzo de comprensión es evidente.

X_M: *Métrica de modificabilidad*: Número de líneas sin datos constantes por cada 100 líneas de código. La existencia de un gran número de datos constantes en el código implica un mayor esfuerzo para la modificación.

X_T: *Métrica de testeabilidad*: Número de líneas de tratamiento de errores por cada 100 líneas de código. La depuración o *testing* del código va a ser más fácil si existen procedimientos de detección y manejo de errores.

Las tres características se han elegido de manera que resulten fácilmente medibles y que tengan una gran influencia sobre la mantenibilidad. No obstante, el modelo puede aplicarse cualquiera que sea el conjunto de métricas escogido, siempre que quede demostrada la dependencia entre dichas métricas y el componente de mantenibilidad correspondiente.

13.4.3. Funciones de mantenibilidad

Las funciones así denominadas relacionan los índices de mantenibilidad (I_C, I_M e I_T) con las métricas recién comentadas (X_C, X_M y X_T).

$$I_C = F_C(X_C)$$
$$I_M = F_M(X_M)$$
$$I_T = F_T(X_T)$$

Para la obtención de estas funciones se hace necesario el empleo de un elemento que resulta fundamental en toda estimación: la información histórica. La experiencia adquirida en proyectos anteriores adquiere un gran valor al emprender nuevos proyectos. Por tanto, se ha de disponer de mecanismos que permitan tomar varias medidas:

a) Del producto desarrollado

X_C: Métrica de comprensibilidad
X_M: Métrica de modificabilidad
X_T : Métrica de testeabilidad

b) Del proceso de mantenimiento

MM_C: Esfuerzo de comprensión
MM_M: Esfuerzo de modificación
MM_T: Esfuerzo de prueba

Los índices de mantenibilidad se obtienen a partir de los valores de esfuerzo mediante la siguiente fórmula:

$$I_C = \frac{MM_C}{TCA * MM_{DES}}$$

I_C = Índice de comprensibilidad
MM_C = Esfuerzo de comprensión en mantenimiento
TCA = Tráfico de cambio anual
MM_{DES} = Esfuerzo de desarrollo

Del mismo modo se obtienen I_M e I_T, considerando el esfuerzo de modificación MM_M y el esfuerzo de prueba MM_T respectivamente.

Toda la información necesaria para la aplicación del modelo, ya comentada, puede incluirse en una tabla que denominamos Tabla Histórica (TH) con la siguiente estructura:

Proyecto	TCA	MM_{DES}	X_C	MM_C	I_C	X_M	MM_M	I_M	X_T	MM_T	I_T
P_1	TCA_1	MM_{DES1}	X_{C1}	MM_{C1}	I_{C1}	X_{M1}	MM_{M1}	I_{M1}	X_{T1}	MM_{T1}	I_{T1}
...	...	...	...	...	...	...	...	...	...	...	...
P_n	TCA_n	MM_{DESn}	X_{Cn}	MM_{Cn}	I_{Cn}	X_{Mn}	MM_{Mn}	I_{Mn}	X_{Tn}	MM_{Tn}	I_{Tn}

Tomando la subtabla formada por las columnas X_C e I_C tenemos una nube de puntos representable en un plano de dos dimensiones $\{(X_{Ci},I_{Ci}) / i=1..n\}$. Haciendo un sencillo análisis de regresión sobre este conjunto de puntos se puede obtener la curva que mejor se ajusta, así como el coeficiente de determinación o grado en que dicha función es representativa de dicho conjunto de puntos. Así obtendríamos la función F_C.

Del mismo modo llegaríamos a las funciones F_M y F_T a partir de los conjuntos de puntos $\{(X_{Mi},I_{Mi}) / i=1..n\}$ y $\{(X_{Ti}/I_{Ti}) / i=1..n\}$.

13.4.4. Método de implementación

En este apartado se describe el método a seguir para implementar el modelo en un proyecto software. La figura 13.1 muestra los elementos y procesos que intervienen en el modelo.

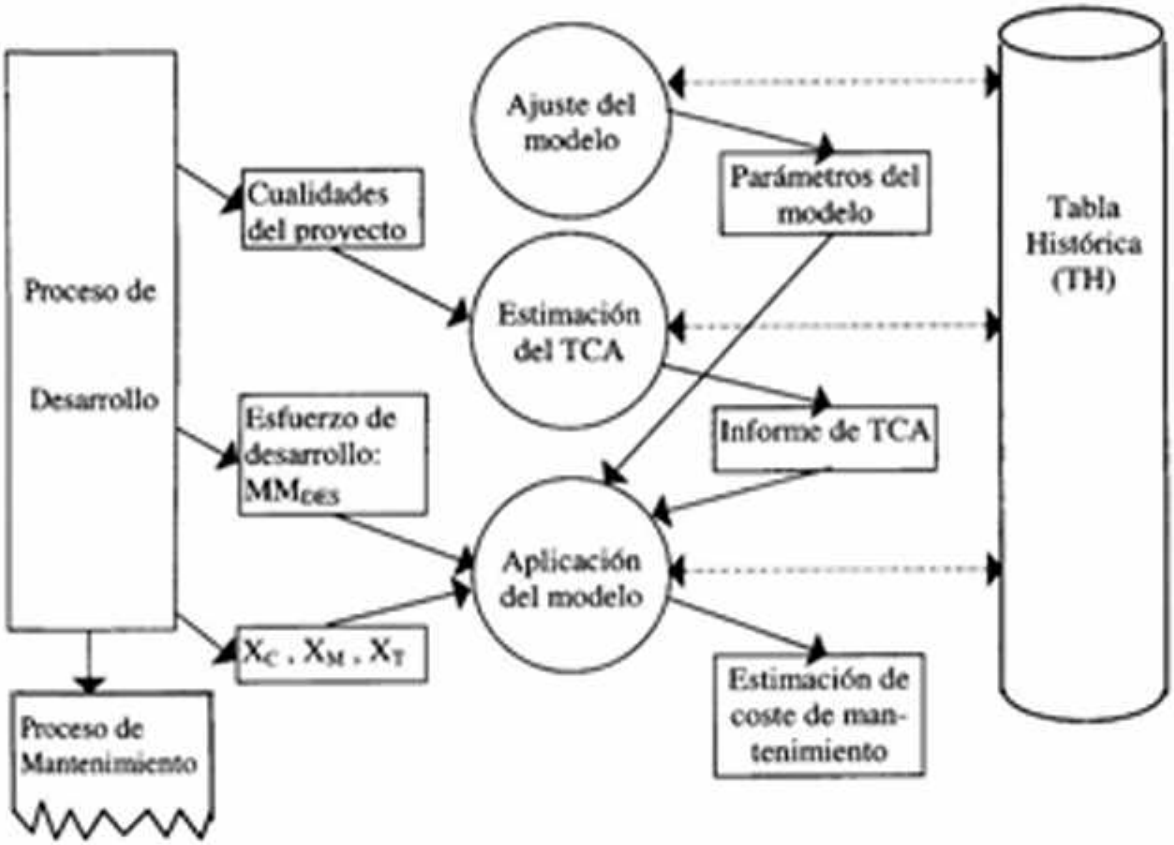


Figura 13.1. Elementos y procesos que intervienen en el modelo de mantenimiento

Como se observa en el esquema, hay tres procesos que utilizan tanto la información histórica de la TH como cierta información que se solicita del proceso de desarrollo.

13.4.4.1. Enfoque de ajuste del modelo

Se trata de determinar la forma de las funciones de mantenibilidad. Realizando un análisis de regresión sobre cada conjunto de puntos $\{(X_{Ci},I_{Ci}) / i=1..n\}$, $\{(X_{Mi},I_{Mi}) / i=1..n\}$ y $\{(X_{Ti},I_{Ti}) / i=1..n\}$ recogidos de la TH, se podrán obtener respectivamente las funciones o líneas de regresión F_C, F_M, y F_T que mejor representen a cada conjunto.

El método de ajuste aquí empleado es el conocido **método de ajuste por mínimos cuadrados.** Para el caso de la función de comprensibilidad, F_C es tal que la suma de los cuadrados de los errores es mínima, es decir,

$$\sum_{i=1}^{n} e_{ci}^2 \text{ es mínimo, siendo } e_{ci} = |I_{Ci} - F_C(X_{Ci})|$$

13.4.4.2. Estimación del TCA

Éste es un proceso que ha de basarse en la experiencia. Dos son los elementos básicos en todo proceso experimental: la información histórica y el juicio de expertos.

El método aquí propuesto se sirve de estos dos elementos para obtener la estimación. Partimos de la existencia de un conjunto de **cualidades** atribuibles a un proyecto software. Este conjunto va a ser elaborado inicialmente y revisado de forma periódica por los expertos de forma que manifieste las características distintivas de los proyectos que componen la tabla de datos históricos. Cada cualidad j va a tener un **peso** p_j que permite valorar unas cualidades más que otras. Cada proyecto tendrá sólo dos posibilidades con respecto a cada cualidad: poseerla o no poseerla. Así, si la tabla histórica está compuesta por *n* proyectos, tendremos la siguiente información que representamos en forma matricial:

Información histórica

A Matriz de nxm elementos que indica las cualidades de cada proyecto que compone la tabla histórica (TH)

$$A = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1m} \\ C_{21} & C_{22} & \cdots & C_{2m} \\ \cdots & \cdots & & \cdots \\ C_{n1} & C_{n2} & \cdots & C_{nm} \end{pmatrix}$$

C_{ij} = Cualidad *j* para el proyecto *i*
Dos valores posibles:
1: El proyecto posee la cualidad
0: En otro caso

T Matriz de nx1 elementos que indica el tráfico de cambio anual de cada proyecto de la TH

$T = (TCA_1, TCA_2 \ldots TCA_n)^T$ TCA_i = Tráfico de cambio anual de proyecto i

NOTA: El superíndice T indica "matriz transpuesta".

Información del proyecto en estudio

C Matriz de 1xm elementos que indica las cualidades del proyecto en curso. La extracción de esta información requiere la intervención de personal experto. Es en este momento cuando se va a revisar el conjunto de cualidades. La modificación de este conjunto requiere la actualización de la tabla histórica revisando las cualidades de todos los proyectos que la componen.

$C = (c_1, c_2, ..., c_m)$ c_j = Cualidad *j* para el proyecto en curso
Dos valores posibles:
p_j : El proyecto posee la cualidad
0 : En otro caso.

B Matriz de nx1 elementos que indica el número de coincidencias que tiene el proyecto en curso con respecto a cada proyecto de la TH, es decir, el número de cualidades que tienen en común.

$$B = A * C^T$$

NOTA: El símbolo * representa el producto de matrices.

El TCA estimado viene dado por la siguiente expresión:

$$TCA = \frac{B * T^T}{B^T * B}$$

De esta forma, cada proyecto interviene en el cálculo de la estimación en la medida en que sus cualidades coinciden con las del proyecto en estudio

13.4.4.3. Aplicabilidad del modelo

Una vez que se dispone de las funciones de mantenibilidad (FC, FM y FT) así como del TCA estimado, el coste estimado de mantenimiento se obtiene sólo con aplicar la fórmula ya conocida:

$$MM_{MANT} = MM_C + MM_M + MM_T = TCA\ MM_{DES}\ (I_C + I_M + I_T)$$

siendo

$I_C = F_C(X_C)$
$I_M = F_M(X_M)$
$I_T = F_T(X_T)$

Por tanto, el proceso de desarrollo ha de suministrar la siguiente información:

MM_{DES} : Esfuerzo de desarrollo
X_C : Métrica de comprensibilidad
X_M : Métrica de modificabilidad
X_T : Métrica de testeabilidad

Con toda esta información recogida se podrá aplicar la fórmula y obtener la estimación del esfuerzo o coste de mantenimiento.

13.5. CASO DE ESTUDIO

Se han estudiado tres proyectos con el fin de aplicar el modelo recién expuesto. Se trata de un proyecto para el desarrollo de un paquete de gestión contable (P_1) y dos de gestión comercial (P_2 y P_3). El estudio se ha simplificado considerando solamente uno de los componentes de la mantenibilidad, a saber, la comprensibilidad. El estudio de la modificabilidad y de la testeabilidad se haría de manera idéntica.

Seguidamente se muestra la tabla histórica en la que intervienen los tres proyectos citados. En ella, todos los datos han sido medidos excepto el índice de comprensibilidad, IC, que se obtiene mediante la fórmula:

$$I_C = \frac{MM_C}{TCA \cdot MM_{DES}}$$

Hemos de mencionar también que C_1 y C_2 son las cualidades escogidas para diferenciar los proyectos en base a su incidencia en el tráfico de cambio anual:

C_1 .- Proyecto de gestión contable
C_2 .- Proyecto de gestión comercial

Asignamos igual peso a ambas cualidades e igual a la unidad ($p_1 = 1$, $p_2 = 1$)

Proyecto	C_1	C_2	TCA	MM_{DES}	X_C	MM_C	I_C
P_1	1	0	0,23	48	14	6,6	0,60
P_2	0	1	0,29	72	11	15,7	0,75
P_3	0	1	0,30	24	115	3,8	0,53

El proyecto en estudio, P_4, tiene como finalidad el desarrollo de un paquete de gestión comercial. Su etapa de desarrollo ha concluido. El coste del desarrollo ha sido de 57 Hombres *x* Mes y la métrica de comprensibilidad, X_C, tiene un valor de 17.

a) Obtención de la función de comprensibilidad (F_C)

Como cabe esperar, según aumenta el valor de la métrica de comprensibilidad (número de líneas de comentario), el índice de comprensibilidad (directamente proporcional al esfuerzo de comprensión) va a disminuir. Por tanto, para el análisis de regresión del conjunto de puntos $\{(X_C, I_C)\}$ hay dos modelos bastante evidentes con

los cuales ensayar: el modelo lineal de pendiente negativa y el modelo exponencial negativo.

De los dos modelos, el exponencial negativo es el más adecuado ya que, normalmente, la mejora de comprensión que supone una nueva línea de comentario va a ser mayor cuanto menor sea la concentración de líneas de comentario en el programa. Esto se comprende perfectamente yéndonos a los límites, es decir, viendo lo que sucede si se añade una línea de comentario en:

a) Un programa sin ninguna documentación interna
b) Un programa con una documentación interna perfecta.

Es evidente que la comprensión en el caso (a) va a verse mejorada en una cuantía mucho mayor que en el caso (b).

Empleando el método de ajuste por mínimos cuadrados, tenemos que se trata de:

$$\text{minimizar} \sum_{i=1}^{n} \left(I_{ci} - \left(X_{ci}\right)\right)$$

Por su sencillez, vamos a considerar en primer lugar el caso de ajuste a una función lineal:

$$\text{minimizar} \sum_{i=1}^{n} \left(I_{ci} - \left(a + bX_{ci}\right)\right)$$

Derivando parcialmente esta expresión respecto de *a* e igualando a 0, y por otro lado, derivando parcialmente respecto de *b* e igualando a 0, se obtiene el siguiente sistema de ecuaciones (en el que simplificamos la notación no incluyendo los límites de los sumatorios que siempre son i=1 hasta n):

$$\left.\begin{aligned} \sum I_{ci} &= aN + b\sum X_{ci} \\ \sum X_{ci} I_{ci} &= a\sum X_{ci} + b\sum X_{ci}^2 \end{aligned}\right\}$$

Consideremos ahora la función exponencial:

$$I_{ci} = ae^{bX_{ci}}$$

Aplicando logaritmos obtenemos:

$$\text{Ln}I_{C_i} = \text{Ln}\,a + b\,X_{C_i}$$

Por tanto, volvemos a tener una función lineal donde la variable independiente es X_{C_i}, y la variable dependiente es Ln I_{C_i}. Haciendo el cambio de variable $I'_{C_i} = Ln\, I_{C_i}$ así como $a' = Ln\, a$ obtenemos el siguiente sistema a resolver:

$$\left.\begin{aligned}\sum I'_{c_i} &= a'N + b\sum X_{c_i}\\ \sum X_{c_i} I'_{c_i} &= a'\sum X_{c_i} + b\sum X_{c_i}^2\end{aligned}\right\}$$

Los datos requeridos se muestran en la siguiente tabla:

Proyecto	X_C	I_C	$I'_C = \text{Ln}\, I_C$	X^2_C	$X_C\, I'_C$
P_1	14	0,60	-0,51	196	-7,14
P_2	11	0,75	-0,29	121	-3,19
P_3	15	0,53	-0,63	225	-9,45
Sumas	40	1,88	1,43	542	-19,78

Sustituyendo y resolviendo el sistema de ecuaciones resultante, obtenemos los valores:

a = 1,86
b = -0,08

Por tanto, la función de comprensibilidad (F_C) obtenida tiene la forma:

$$I_C = F_C(X_C) = 1{,}86\, e^{-0{,}08\, X_C}$$

b) Obtención del tráfico de cambio anual estimado (TCA)

Vamos a construir las matrices A, T, C y B de acuerdo al procedimiento ya expuesto:

$$A = \begin{pmatrix}1 & 0\\ 0 & 1\\ 0 & 1\end{pmatrix}\quad T = \begin{pmatrix}0{,}23\\ 0{,}29\\ 0{,}30\end{pmatrix}\quad C = (0 \quad 1)\quad B = \begin{pmatrix}0\\ 1\\ 1\end{pmatrix}$$

Aplicando la fórmula de cálculo de TCA tenemos:

$$TCA = \frac{B * T^T}{B^T * B} = \frac{0,29 + 0,30}{2} = 0,30$$

c) Aplicación del modelo al proyecto P_4 para el cálculo del coste de comprensión estimado en la etapa de mantenimiento (MM_C)

$$MM_C = TCA \cdot MM_{DES} \cdot I_C$$

$$MM_C = 0,30 \cdot 57 \cdot 1,86 \cdot e^{0,08 \cdot 17} = 8,16 \text{ Hombres x Mes}$$

Como ya se ha comentado, en el caso de estudio se ha considerado sólo un componente de la mantenibilidad. Para los otros dos componentes, el procedimiento sería idéntico. El coste o esfuerzo estimado de mantenimiento se obtendría como suma de los tres costes, comprensión (MM_C), modificación (MM_M) y prueba (MM_T).

13.6. CONCLUSIONES

Como hemos podido comprobar, mediante el estudio de la mantenibilidad y auditando la utilización en el proyecto software de las técnicas que permitan asegurar unos niveles de mantenibilidad, podremos fijar el campo de actuación de la Auditoría Informática en el Mantenimiento.

13.7. LECTURAS RECOMENDADAS

La publicación periódica *The Journal of Information Systems Audit and Control Association* de la ISACA.

La obra de Weber R. EDP Auditing. *Conceptual Foundations and Practice*, 2ª ed., editada por McGraw-Hill, Sydney, 1988.

Por último podríamos mencionar por el campo de su utilización la obra de Buttery R. Hurford C. y Simpson R.K. de la *Internal Audit in the Public Sector*, publicada por ICSA cop en 1993.

13.8. CUESTIONES DE REPASO

1. Exponga las razones que hacen de la auditoría del mantenimiento un área especialmente crítica.

2. Desarrolle una lista de comprobación que recoja los aspectos más importantes a la hora de evaluar la gestión de cambios.

3. ¿Qué ventajas aporta una herramienta de gestión de configuración a la hora de auditar el mantenimiento de sistemas informáticos?

4. Aplique las métricas propuestas en este capítulo a algún sistema real, calibrándolas si fuera necesario a su entorno específico.

5. ¿Qué factores pueden influir en la modificabilidad de los programas?

6. Analice en la literatura existente diversas métricas de complejidad y describa su influencia en la mantenibilidad.

7. Existen herramientas específicas para la gestión de pruebas de software, analice su impacto en la testeabilidad.

8. ¿Cómo debería organizarse la gestión de incidencias de mantenimiento en un departamento de informática desde el punto de vista de la auditoría?

9. La influencia de la documentación en el mantenimiento de los sistemas parece obvia, pero ¿cómo mediría la documentación existente sobre un sistema?

10. Compare otros modelos de estimación que conozca con el propuesto en este capítulo.

CAPÍTULO 14

AUDITORÍA DE BASES DE DATOS

Mario G. Piattini Velthuis

14.1. INTRODUCCIÓN

La gran difusión de los Sistemas de Gestión de Bases de Datos (SGBD), junto con la consagración de los datos como uno de los recursos fundamentales de las empresas, ha hecho que los temas relativos a su control interno y auditoría cobren, cada día, mayor interés.

Como ya se ha comentado, normalmente la auditoría informática se aplica de dos formas distintas; por un lado, se auditan las principales áreas del departamento de informática: explotación, dirección, metodología de desarrollo, sistema operativo, telecomunicaciones, bases de datos, etc.; y, por otro, se auditan las aplicaciones (desarrolladas internamente, subcontratadas o adquiridas) que funcionan en la empresa. La importancia de la auditoría del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoría de las aplicaciones que utilizan esta tecnología.

14.2. METODOLOGÍAS PARA LA AUDITORÍA DE BASES DE DATOS

Aunque existen distintas metodologías que se aplican en auditoría informática (prácticamente cada firma de auditores y cada empresa desarrolla la suya propia), como se vio en el Capítulo 3, se pueden agrupar en dos clases.

14.2.1. Metodología tradicional

En este tipo de metodología el auditor revisa el entorno con la ayuda de una lista de control *(checklist)*, que consta de una serie de cuestiones a verificar. Por ejemplo:

S N NA

¿Existe una metodología de diseño de BD?

El auditor deberá, registrar el resultado de su investigación: *S*, si la respuesta es afirmativa, *N*, en caso contrario, o *NA* (no aplicable).

Este tipo de técnica suele ser aplicada a la auditoría de productos de bases de datos, especificándose en la lista de control todos los aspectos a tener en cuenta. Así, por ejemplo, si el auditor se enfrenta a un entorno Oracle 8, en la lista de control se recogerán los parámetros de instalación que más riesgos comportan, señalando cuál es su rango adecuado. De esta manera, si el auditor no cuenta con la asistencia de un experto en el producto, puede comprobar por lo menos los aspectos más importantes de su instalación.

14.2.2. Metodología de evaluación de riesgos

Este tipo de metodología, conocida también por *risk oriented approach*, es la que propone la ISACA, y empieza fijando los objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno. En Touriño y Fernández (1991) se señalan los riesgos más importantes que lleva consigo la utilización de una base de datos y que se recogen en la figura 14.1.

Considerando estos riesgos, se podría definir por ejemplo el siguiente:

Objetivo de Control:

El SGBD deberá preservar la confidencialidad de la base de datos.

Una vez establecidos los objetivos de control, se especifican las técnicas específicas correspondientes a dichos objetivos:

Técnica de Control:

Se deberán establecer los tipos de usuarios, perfiles y privilegios necesarios para controlar el acceso a la base de datos.

Figura 14.1. Riesgos debidos a la utilización de una base de datos, TOURIÑO y FERNÁNDEZ (1991)

Un objetivo de control puede llevar asociadas varias técnicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser preventivas (como la arriba mencionada)" detectivas (como monitorizar los accesos a la BD) o correctivas (por ejemplo, una copia de respaldo –*backup*–).

En caso de que los controles existan, se diseñan unas pruebas (denominadas *pruebas de cumplimiento)* que permiten verificar la consistencia de los mismos, por ejemplo:

Prueba de cumplimiento:

Listar los privilegios y perfiles existentes en el SGBD.

Si estas pruebas detectan inconsistencias en los controles, o bien, si los controles no existen, se pasa a diseñar otro tipo de pruebas –denominadas *pruebas sustantivas*– que permitan dimensionar el impacto de estas deficiencias:

Prueba sustantiva:

Comprobar si la información ha sido corrompida comparándola con otra fuente, o revisando, los documentos de entrada de datos y las transacciones que se han ejecutado.

Una vez valorados los resultados de las pruebas se obtienen unas conclusiones que serán comentadas y discutidas con los responsables directos de las áreas afectadas con el fin de corroborar los resultados. Por último, el auditor deberá emitir una serie de *comentarios* donde se describa la situación, el riesgo existente y la deficiencia a solucionar, y, en su caso, sugerirá la posible solución.

Como resultado de la auditoría, se presentará un informe final en el que se expongan las conclusiones más importantes a las que se ha llegado, así como el alcance que ha tenido la auditoría.

Ésta será la técnica a utilizar para auditar el entorno general de un sistema de bases de datos, tanto en su desarrollo como durante la explotación.

14.3. OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS

A continuación expondremos algunos objetivos y técnicas de control a tener en cuenta a lo largo del ciclo de vida de una base de datos (véase la figura 14.2) que abarca desde el estudio previo hasta su explotación; para ello nos basaremos en los propuestos por la ISACA a principios de esta década, MENKUS (1990), y en los recientemente publicados COBIT, ISACF (1996).

14.3.1. Estudio previo y plan de trabajo

En esta primera fase, es muy importante elaborar un estudio tecnológico de viabilidad en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis coste-beneficio para cada una de las opciones. Se debe considerar entre estas alternativas la posibilidad de no llevar a cabo el proyecto (no siempre está justificada la implantación de un sistema de bases de datos) así como la disyuntiva entre desarrollar y comprar (en la práctica, a veces nos encontramos con que se ha desarrollado una aplicación que ya existía en el mercado, cuya compra hubiese supuesto un riesgo menor, asegurándonos incluso una mayor calidad a un precio inferior).

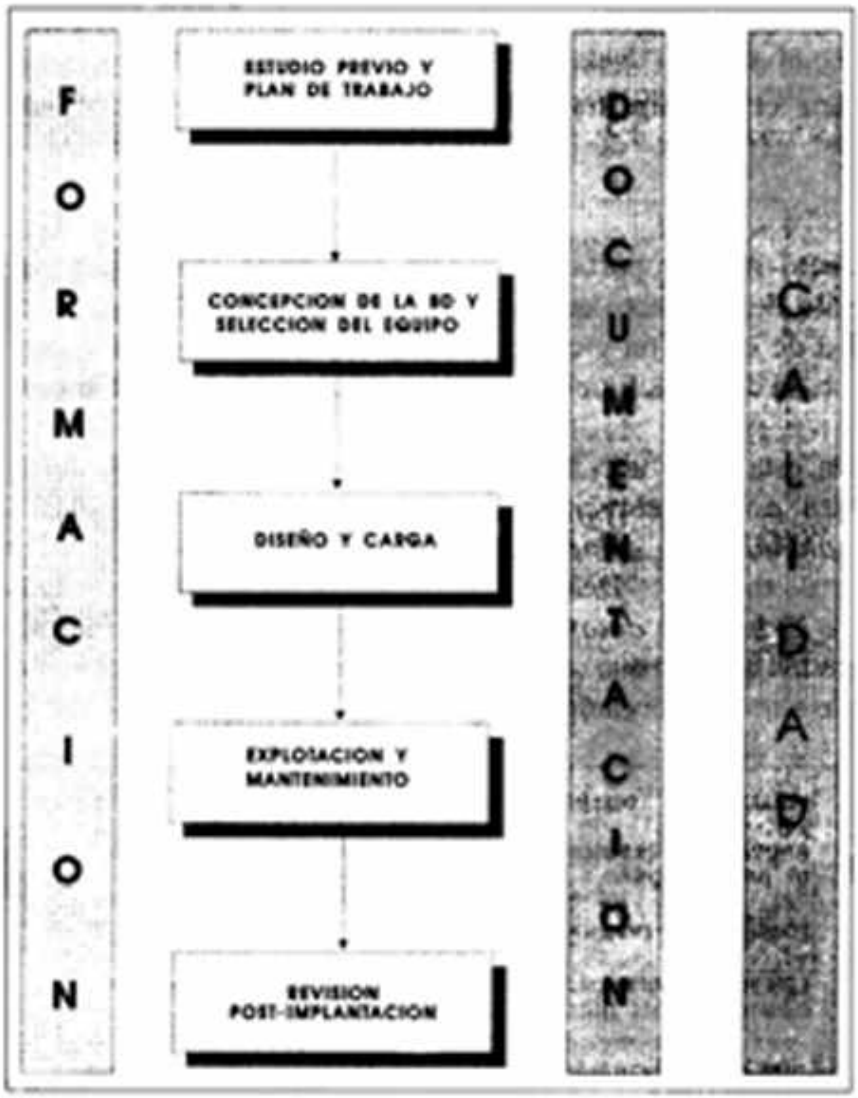


Figura 14.2. Ciclo de vida de una base de datos

Desafortunadamente, en bastantes empresas este estudio de viabilidad no se lleva a cabo con el rigor necesario, con lo que a medida que se van desarrollando, los sistemas demuestran, a veces, ser poco rentables.

El auditor debe comprobar también que la alta dirección revisa los informes de los estudios de viabilidad y que es la que decide seguir adelante o no con el proyecto. Esto es fundamental porque los técnicos han de tener en cuenta que si no existe una decidida voluntad de la organización en su conjunto, impulsada por los directivos, aumenta considerablemente el riesgo de fracasar en la implantación del sistema.

En los nuevos COBIT se enfatiza la importancia de llevar a cabo una gestión de riesgos (valoración, identificación, medida, plan de acción y aceptación), que es objeto de atención, afortunadamente, de un número cada día mayor de empresas.

En caso de que se decida llevar a cabo el proyecto es fundamental que se establezca un plan director, debiendo el auditor verificar que efectivamente dicho plan se emplea para el seguimiento y gestión del proyecto y que cumple con los procedimientos generales de gestión de proyectos que tenga aprobados la organización.

Otro aspecto muy importante en esta fase es la aprobación de la estructura orgánica no sólo del proyecto en particular, sino también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos; recordemos que, para que un entorno de base de datos funcione debidamente, esta unidad es imprescindible.

Se pueden establecer acerca de este tema dos objetivos de control, MENKUS *(1990): "Deben asignarse responsabilidades para la planificación, organización, dotación de plantillas y control de los activos de datos de la organización"* (administrador de datos) y *"Debe asignarse la responsabilidad de la administración del entorno de la base de datos"* (administrador de la base de datos); señalando la mayor parte de los autores que ambas funciones tienen que posicionarse a un nivel lo suficientemente alto en el organigrama para asegurar su independencia.

REALIZAR EL DISEÑO CONCEPTUAL Y LOGICO DE LA BASE

APOYAR AL PERSONAL DE SISTEMAS DURANTE EL DESARROLLO DE APLICACIONES

FORMAR AL PERSONAL

ESTABLECER ESTANDARES DE DISEÑO DE BD, DESARROLLO Y CONTENIDO DEL DICCIONARIO DE DATOS

DISEÑAR LA DOCUMENTACION INCLUIDA EN EL DICCIONARIO

DESABROLLAR POLITICAS DE GESTION DE DATOS

DESARROLLAR PLANES ESTRATEGICOS Y TACTICOS PARA LA MANIPULACION DE LOS DATOS

DESARROLLAR LOS REQUISITOS DE LOS ELEMENTOS DEL DICCIONARIO DE DATOS

DESARROLLAR NORMAS PARA LA DENOMINACION

CONTROLAR LA INTEGRIDAD Y SEGURIDAD DE LOS DATOS

PLANIFICAR LA EVOLUCION DE LA BD DE LA EMPRESA

IDENTIFICAR OPORTUNIDADES DE COMPARTICION DE DATOS

TRABAJAR CON LOS AUDITORES EN LA AUDITORIA DE LA BASE

PROPORCIONAR CONTROLES DE SEGURIDAD

Figura 14.3. Tareas del administrador de datos, BRATHWAITE (1985)

En las figuras 14.3 y 14.4 se muestran algunas de las funciones y responsabilidades tanto del administrador de datos como del administrador de la base de datos. Remitimos al lector interesado en tratar con más profundidad este tema, a BRATHWAITE (1985), donde se analiza desde la perspectiva del control de datos.

Figura 14.4. Tareas del administrador de la base de datos, BRATHWAITE (1985)

A la hora de detallar las responsabilidades de estas funciones hay que tener en cuenta uno de los principios fundamentales del control interno: la separación de funciones. Se recomienda una separación de funciones entre:

- El personal de desarrollo de sistemas y el de explotación.
- Explotación y control de datos.
- Administración de bases de datos y desarrollo.

Debería existir también una separación de funciones entre el administrador de la seguridad y el administrador de la base de datos. Esto no quiere decir que estas tareas tengan forzosamente que desempeñarlas personas distintas (lo que no sería viable en muchas pequeñas y medianas empresas) pero sí que es un aspecto importante de control a considerar, por lo que en caso de que no pueda lograrse la separación de funciones, deberán establecerse controles compensatorios o alternativos; como, por

ejemplo, una mayor atención de la dirección y la comprobación por parte de algún usuario del contenido y de las salidas más importantes producidas a partir de la BD.

La situación que el auditor encuentra normalmente en las empresas es que al no existir una descripción detallada de los puestos de trabajo (que incluyan responsabilidades, conocimientos, etc.), la separación de funciones es muy difícil de verificar.

14.3.2. Concepción de la base de datos y selección del equipo

En esta fase se empieza a diseñar la base de datos, por lo que deben utilizarse los modelos y las técnicas definidos en la metodología de desarrollo de sistemas de la empresa, véase Capítulo 12.

La metodología de diseño debería también emplearse para especificar los documentos fuentes, los mecanismos de control, las características de seguridad y las pistas de auditoría a incluir en el sistema, estos últimos aspectos generalmente se descuidan, lo que produce mayores costes y problemas cuando se quieren incorporar una vez concluida la implementación de la base de datos y la programación de las aplicaciones.

El auditor debe, por tanto, en primer lugar, analizar la metodología de diseño con el fin de determinar si es o no aceptable, y luego comprobar su correcta utilización. Como mínimo una metodología de diseño de BD debería contemplar dos fases de diseño: lógico y físico, aunque la mayoría de las empleadas en la actualidad contempla tres fases; además de las dos anteriores, una fase previa de diseño conceptual que sería abordada en este momento del ciclo de vida de la base de datos; véase, por ejemplo, De Miguel, Piattini y Marcos (1999).

Un importante aspecto a considerar, al que los COBIT dedican un apartado específico, es la definición, de la arquitectura de la información, que contempla cuatro objetivos de control relativos a:

- Modelo de arquitectura de información, y su actualización, que es necesaria para mantener el modelo consistente con las necesidades de los usuarios y con el plan estratégico de tecnologías de la información.
- Datos y diccionario de datos corporativo.
- Esquema de clasificación de datos en cuanto a su seguridad.
- Niveles de seguridad para cada anterior clasificación de datos.

En cuanto a la selección del equipo, en caso de que la empresa no disponga ya de uno, deberá realizarse utilizando un procedimiento riguroso; en el que se consideren,

por un lado, las necesidades de la empresa (debidamente ponderadas) y, por otro, las prestaciones que ofrecen los distintos SGBD candidatos (puntuados de manera oportuna). En ISACF (1996) se destaca también que en este procedimiento se debe tener en cuenta el impacto que el nuevo software tiene en el sistema y en su seguridad.

14.3.3. Diseño y carga

En esta fase se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente; determinando si la definición de los datos contempla además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad. El auditor tendrá que tomar una muestra de ciertos elementos (tablas, vistas, índices) y comprobar que su definición es completa, que ha sido aprobada por el usuario y que el administrador de la base de datos participó en su establecimiento.

Es importante que la dirección del departamento de informática, los usuarios e incluso, en algunas ocasiones, la alta dirección, aprueben el diseño de los datos, al igual que el de las aplicaciones.

Una vez diseñada la BD, se procederá a su carga, ya sea migrando datos de un soporte magnético o introduciéndolos manualmente.

Las migraciones o conversiones de sistemas, como el paso de un sistema de archivos a uno de bases de datos, o de un tipo de SGBD (de jerárquico a relacional), entrañan un riesgo muy importante, por lo que deberán estar claramente planificadas para evitar pérdida de información y la transmisión al nuevo sistema de datos erróneos. También se deberán realizar pruebas en paralelo, verificando que la decisión real de dar por terminada la prueba en paralelo se atenía a los criterios establecidos por la dirección y que se haya aplicado un control estricto de la corrección de errores detectados en esta fase.

Por lo que respecta a la entrada manual de datos, hay que establecer un conjunto de controles que aseguren la integridad de los mismos. A este respecto, cabe destacar que las declaraciones escritas de procedimientos de la organización referentes a la entrega de datos a ser procesados deben asegurar que los datos se autorizan, recopilan, preparan, transmiten, y se comprueba su integridad de forma apropiada.

También es aconsejable que los procedimientos y el diseño de los documentos fuentes minimicen los errores y las omisiones, así como el establecimiento de unos procedimientos de autorización de datos.

Un aspecto muy importante es el tratamiento de datos de entrada erróneos, para los que deben cuidarse, con atención los procedimientos de reintroducción de forma que no disminuyan los controles; a este respecto lo ideal es que los datos se validen y corrijan tan cerca del punto de origen como sea posible.

Como sabemos, no toda la semántica de los datos puede siempre almacenarse en el esquema de la base de datos, por lo que parte de esta semántica se ve obligada a residir en los programas. Será necesario, por tanto, comprobar que los programas implementan de forma adecuada esta integridad.

14.3.4. Explotación y mantenimiento

Una vez realizadas las pruebas de aceptación, con la participación de los usuarios, el sistema se pondrá (mediante las correspondientes autorizaciones y siguiendo los procedimientos establecidos para ello) en explotación.

En esta fase, se debe comprobar que se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas sólo se modifica mediante la autorización adecuada.

En los nuevos COBIT se dedica un apartado completo a detallar los objetivos de control para la gestión de datos, clasificándolos en un conjunto de apartados que se muestran en la figura 14.5.

Sería conveniente también que el auditor pudiera llevar a cabo una auditoría sobre el rendimiento del sistema de BD, comprobando si se lleva a cabo un proceso de ajuste *(tuning)* y optimización adecuados que no sólo consiste en el rediseño físico o lógico de la BD, sino que también abarca ciertos parámetros del SO e incluso la forma en que acceden las transacciones a la BD. Recordemos que *"la función de administración de la base de datos debe ser la responsable de monitorizar el rendimiento y la integridad de los sistemas de BD"*, Moeller (1989).

Procedimientos de preparación de datos
Procedimientos de autorización de documentos fuente
Recogida de datos de documentos fuente
Manejo de errores de documentos fuente
Retención de documentos fuente
Procedimientos de autorización de datos
Verificación de exactitud, compleción y autorización
Manejo de errores de entrada de datos
Integridad del procesamiento de datos
Edición y validación del procesamiento de datos
Manejo de errores de procesamiento de datos
Retención y manejo de salidas
Distribución de salidas
Reconciliación y balanceo de salidas
Manejo de errores y revisión de salidas
Medidas de seguridad para informes de salidas
Protección de información sensible
Protección de información sensible dispuesta
Gestión de almacenamiento
Períodos de retención y términos de almacenamiento
Sistema de gestión de biblioteca de medios
Responsabilidades de gestión de la biblioteca de medios
Copias de respaldo y recuperación
Trabajos de copias de respaldo
Almacenamiento de respaldo

Figura 14.5. Clasificación de los objetivos de control para la gestión de datos, ISACA (1996)

14.3.5. Revisión post-implantación

Aunque en bastantes organizaciones no se lleva a cabo, por falta de tiempo y recursos, se debería establecer el desarrollo de un plan para efectuar una revisión post-implantación de todo sistema nuevo o modificado con el fin de evaluar si:

- Se han conseguido los resultados esperados.
- Se satisfacen las necesidades de los usuarios.
- Los costes y beneficios coinciden con los previstos.

14.3.6. Otros procesos auxiliares

A lo largo de todo el ciclo de vida de la base de datos se deberá controlar la formación que precisan tanto usuarios informativos (administrador, analistas, programadores, etc.) como no informáticos, ya que la formación es una de las claves para minimizar el riesgo en la implantación de una base de datos, Piattini (1990).

Esta formación no se puede basar simplemente en cursos sobre el producto que se está instalando, sino que suele ser precisa una formación de base que resulta imprescindible cuando: se pasa de trabajar en un entorno de archivos orientado al proceso a un entorno de bases de datos, por lo que supone de "cambio filosófico"; lo mismo puede decirse si se cambia de tipo de SGBD (por ejemplo, de relacional a orientado a objetos).

Hay que tener en cuenta que usuarios poco formados constituyen uno de los peligros más importantes de un sistema. Esta formación no debería limitarse al área de las bases de datos, sino que tendría que ser complementada con formación relativa a los conceptos de control y seguridad.

Además el auditor tendrá que revisar la documentación que se produce a lo largo de todo el proceso, paya verificar si es suficiente y si se ajusta a los estándares establecidos por la metodología adoptada en la empresa.

A este respecto resulta muy importante que se haya llevado a cabo un aseguramiento de calidad; véase Capítulo 16, lo ideal sería que en la propia empresa existiera un grupo de calidad que se encargara, entre otras cosas, de asegurar la calidad de los diseños de bases de datos. Es cierto que existen pocas "medidas" de calidad para una base de datos; de todas maneras, hay ciertas técnicas bastante difundidas que se pueden aplicar a una base de datos como es la teoría de la normalización.

14.4. AUDITORÍA Y CONTROL INTERNO EN UN ENTORNO DE BASES DE DATOS

Cuando el auditor, se encuentra el sistema en explotación, deberá estudiar el SGBD y su entorno. Como se señala en Menkus (1991), *"en el desarrollo y mantenimiento de sistemas informativos en entornos de BD, deberían considerarse el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios. Esto debe abarcar a todos los componentes del entorno de BD"*. El gran problema de las bases de datos es que su entorno cada vez es más complejo y no puede limitarse sólo al propio SGBD. En la figura 14.6 se muestra un posible entorno de bases de datos en el que aparecen los elementos más usuales.

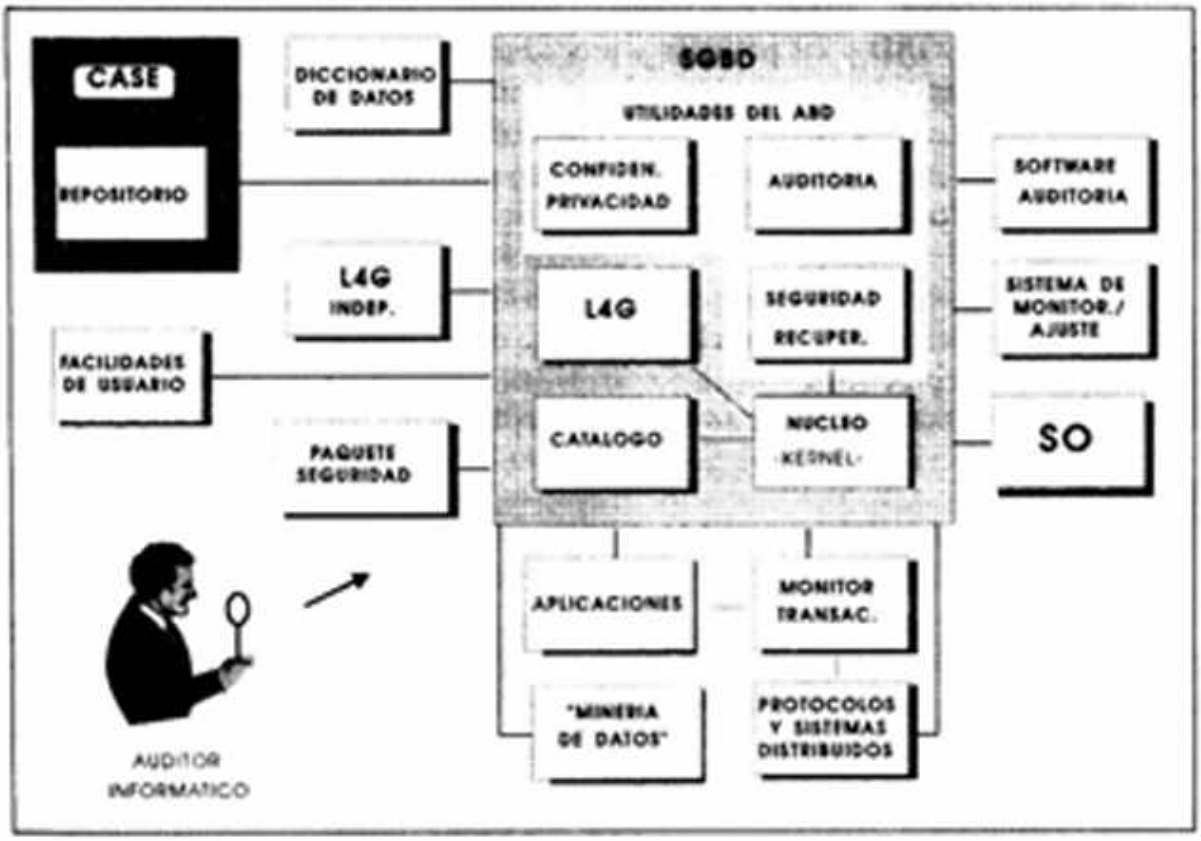


Figura 14.6. Entorno de base de datos

14.4.1. Sistema de Gestión de Bases de Datos (SGBD)

Entre los componentes del SGBD podemos destacar el núcleo *(kernel)*, el catálogo (componente fundamental para asegurar la seguridad de la base de datos), las utilidades para el administrador de la base de datos (entre las que se suelen encontrar algunas para crear usuarios, conceder privilegios y resolver otras cuestiones relativas a la confidencialidad); las que se encargan de la recuperación de la BD: rearranque, copias de respaldo, archivos diarios *(log)*, etc. y algunas funciones de auditoría, así como los lenguajes de cuarta generación (L4G) que incorpora el propio SGBD.

En cuanto a las funciones de auditoría que ofrece el propio sistema, prácticamente todos los productos del mercado permiten registrar ciertas operaciones realizadas sobre la base de datos en un archivo (o en un conjunto de tablas) de pistas de auditoría *(audit trail)*. El propio Modelo de Referencia de Gestión de Datos –ISO (1993)– considera las pistas de auditoría como un elemento esencial de un SGBD, señalando que *"el requisito para la auditoría es que la causa y el efecto de todos los cambios de la base de datos sean verificables"*.

El auditor deberá revisar, por tanto, la utilización de todas las herramientas que ofrece el propio SGBD y las políticas y procedimientos que sobre su utilización haya definido el administrador, para valorar si son suficientes o si deben ser mejorados.

14.4.2. Software de auditoría

Son paquetes que pueden emplearse para facilitar la labor del auditor, en cuanto a la extracción de datos de la base, el seguimiento de las transacciones, datos de prueba, etc. Hay también productos muy interesantes que permiten cuadrar datos de diferentes entornos permitiendo realizar una verdadera "auditoría del dato".

14.4.3. Sistema de monitorización y ajuste *(tuning)*

Este tipo de sistemas complementan las facilidades ofrecidas por el propio SGBD, ofreciendo mayor información para optimizar el sistema, llegando a ser en determinadas ocasiones verdaderos sistemas expertos que proporcionan la estructura óptima de la base de datos y de ciertos parámetros del SGBD y del SO.

La optimización de la base de datos, como ya hemos señalado, es fundamental, puesto que si actúa en un entorno concurrente puede degradarse fácilmente el nivel de servicio que haya podido establecerse con los usuarios.

14.4.4. Sistema Operativo (SO)

El SO es una pieza clave del entorno, puesto que el SGBD se apoyará, en mayor o menor medida (según se trate de un SGBD independiente o dependiente) en los servicios que le ofrezca; el SO en cuanto a control de memoria, gestión de áreas de almacenamiento intermedio *(buffers)*, manejo de errores, control de confidencialidad, mecanismos de interbloqueo, etc. Desafortunadamente, el auditor informática tiene serias dificultades para controlar de manera rigurosa la interfaz entre el SGBD y el SO, debido a que, en parte, constituye información reservada de los fabricantes de los productos, además de requerir unos conocimientos excepcionales que entran en el campo de la técnica de sistemas, véase Capítulo 15.

14.4.5. Monitor de Transacciones

Algunos autores lo incluyen dentro del propio SGBD, pero actualmente, puede considerarse un elemento más del entorno con responsabilidades de confidencialidad y rendimiento.

14.4.6. Protocolos y Sistemas Distribuidos

Cada vez más se está accediendo a las bases de datos a través de redes, con lo que el riesgo de violación de la confidencialidad e integridad se acentúa. También las bases de datos distribuidas pueden presentar graves riesgos de seguridad.

Moeller (1989) establece cinco objetivos de control a la hora de revisar la distribución de datos:

1. El sistema de proceso distribuido debe tener una función de administración de datos centralizada que establezca estándares generales para la distribución de datos a través de las aplicaciones.

2. Deben establecerse unas funciones de administración de datos y de base de datos fuertes, para que puedan controlar la distribución de los datos.

3. Deben existir pistas de auditoría para todas las actividades realizadas por las aplicaciones contra sus propias bases de datos y otras compartidas.

4. Deben existir controles software para prevenir interferencias de actualización sobre las bases de datos en sistemas distribuidos.

5. Deben realizarse las consideraciones adecuadas de costes y beneficios en el diseño de entornos distribuidos.

Respecto a este último punto, es importante destacar cómo, por ejemplo, muy pocas empresas han considerado rentable implementar bases de datos "realmente" distribuidas; siendo bastante más económico y usual actualizar bases de datos distribuidas mediante transferencia de archivos y procesos por lotes *(batch)*, que hacerlo en línea.

14.4.7. Paquete de seguridad

Existen en el mercado varios productos que permiten la implantación efectiva de una política de seguridad, puesto que centralizan el control de accesos, la definición de privilegios, perfiles de usuario, etc. Un grave inconveniente de este tipo de software es que a veces no se encuentra bien integrado con el SGBD, pudiendo resultar poco útil su implantación si los usuarios pueden "saltarse" los controles a través del propio SGBD.

14.4.8. Diccionarios de datos

Este tipo de sistemas, que empezaron a implantarse en los años setenta, también juegan un papel primordial en el entorno de los SGBD en cuanto a la integración de componentes y al cumplimiento de la seguridad de los datos, véase Piattini y Daryanani (1995).

Los propios diccionarios se pueden auditar de manera análoga a las bases de datos (puesto que son bases de "metadatos"), las diferencias entre unos y otros, residen principalmente en que un fallo en una base de datos puede atentar contra la integridad de los datos y producir un mayor riesgo financiero, mientras que un fallo en un diccionario (o repositorios, suele llevar consigo una pérdida de integridad de los procesos; siendo más peligrosos los fallos en los diccionarios puesto que pueden introducir errores de forma repetitivo a lo largo del tiempo, que son más difíciles de detectar, Perry (1991).

Para aspectos relacionados con las facilidades de control y auditoría de diccionarios de datos, remitimos, al lector a Narayan (1988).

14.4.9. Herramientas CASE *(Computer Aided System/Software Engineering). IPSE (Integrated Project Support Environments)*

Desde la década pasada venimos asistiendo a una gran difusión de este tipo de herramientas como soporte al diseño y concepción de sistemas de información, véase Piattini y Daryanani (1995). Suelen llevar incorporado un diccionario de datos (enciclopedia o repositorios más amplio que los mencionados anteriormente en los que se almacenan además de información sobre datos, programas, usuarios, etc., los diagramas, matrices y grafos de ayuda al diseño. Constituyen una herramienta clave para que el auditor pueda revisar el diseño de la base de datos, comprobar si se ha empleado correctamente la metodología y asegurar un nivel mínimo de calidad.

En Piattini y Ramos (1995) se expone cómo llevar a cabo la auditoría de los entornos CASE/IPSE.

14.4.10. Lenguajes de Cuarta Generación (L4G) independientes

Además de las herramientas que ofrezca el propio SGBD, el auditor se puede encontrar con una amplia gama de generadores de aplicaciones, de formas, de

informes, etc. que actúan sobre la base de datos y que, por tanto, también son un elemento importante a considerar en el entorno del SGBD.

En Moeller (1991) se ofrecen varios objetivos de control para los L4G, entre los que destacan los siguientes:

- El L4G debe ser capaz de operar en el entorno de proceso de datos con controles adecuados.
- Las aplicaciones desarrolladas con L4G deben seguir los mismos procedimientos de autorización y petición que los proyectos de desarrollo convencionales.
- Las aplicaciones desarrolladas con L4G deben sacar ventaja de las características incluidas en los mismos.

En efecto, uno de los peligros más graves de los L4G es que no se apliquen controles con el mismo rigor que a los programas desarrollados con lenguajes de tercera generación. Esto puede deberse, en parte, a una inadecuada interfaz entre el L4G y el paquete de seguridad y a la falta de código fuente en el sentido tradicional, que hacen más difícil de esta manera el control de cambios en las aplicaciones.

Otros problemas asociados a los L4G y con los que nos encontramos frecuentemente, pueden ser su ineficiencia y elevado consumo de recursos, las limitaciones que, en ocasiones, imponen al programador, los cambios que pueden suponer en la metodología de desarrollo, etc. Respecto a este último punto, muchos L4G se utilizan en la actualidad para desarrollar prototipos que facilitan a los usuarios la exposición de sus necesidades. Moeller (1989), señala que *"el prototipo de una aplicación desarrollado con L4G debe proporcionar suficiente detalle para reemplazar los documentos escritos asociados a los procedimientos convencionales de la metodología de desarrollo de sistemas"*.

El auditor deberá estudiar los controles disponibles en los L4G utilizados en la empresa, analizando con atención si permiten construir procedimientos de control y auditoría dentro de las aplicaciones y, en caso negativo, recomendar su construcción utilizando lenguajes de tercera generación.

14.4.11. Facilidades de usuario

Con la aparición de interfaces gráficas fáciles de usar (con menús, ratón, ventanas, etc.) se ha desarrollado toda una serie de herramientas que permiten al usuario final acceder a los datos sin tener que conocer la sintaxis de los lenguajes del SGBD. El auditor deberá investigar las medidas de seguridad que ofrecen estas

herramientas y bajo qué condiciones han sido instaladas; las herramientas de este tipo deberían "proteger al usuario de sus propios errores".

Las aplicaciones desarrolladas empleando facilidades de usuario deben seguir los mismos sólidos principios de control y tratamiento de errores que el resto; Moeller (1989) destaca también otros dos importantes objetivos de control:

- La documentación de las aplicaciones desarrolladas por usuarios finales debe ser suficiente para que tanto sus usuarios principales como cualquier otro puedan operar y mantenerlas.

- Los cambios de estas aplicaciones requieren la aprobación de la dirección y deben documentarse de forma completa.

En este apartado podemos incluir también las diferentes facilidades que ofrecen algunos SGBD que pemiten su conexión con paquetes ofimáticos (por ejemplo, hojas de cálculo), que pueden acceder a la base de datos e incluso actualizarla. En este caso el auditor debe prestar especial atención a los procedimientos de carga y descarga *(uploading/downloading)* de datos de la base a/desde los paquetes ofimáticos; comprobando, por ejemplo, si se puede actualizar la base de datos desde cualquiera de éstos o si la descarga se realiza con datos correctamente actualizados ("descarga de los datos correctos en el momento correcto").

14.4.12. Herramientas de "minería de datos"

En los últimos años ha explosionado el fenómeno de los almacenes de datos *datawarehouses* y las herramientas para la explotación o "minería" de datos *(datamining)*. Estas herramientas ofrecen soporte a la toma de decisiones sobre datos de calidad integrados en el almacén de datos. En el Capítulo 20 se revisa la auditoría de los EIS/DSS, cuyos principios se pueden aplicar a las herramientas de "minería"; debiéndose controlar la política de refresco y carga de los datos en el almacén a partir de las bases de datos operacionales existentes, así como la existencia de mecanismos de retroalimentación *(feedback)* que modifican las bases de datos operacionales a partir de los datos del almacén:

14.4.13. Aplicaciones

El auditor deberá controlar que las aplicaciones no atentan contra la integridad de los datos de la base, véase Capítulo 19.

14.5. TÉCNICAS PARA EL CONTROL DE BASES DE DATOS EN UN ENTORNO COMPLEJO

Como hemos visto en el epígrafe anterior, existen muchos elementos del entorno del SGBD que influyen en la seguridad e integridad de los datos, en los que cada uno se apoya en la operación correcta y predecible de otros. Como se destaca en CLARK *et al.* (1991), el efecto de todo esto es *"debilitar la seguridad global del sistema, reduciendo la fiabilidad e introduciendo un conjunto de controles descoordinados y solapados, difíciles de gestionar"*, esta situación se acentúa aún más si los diferentes componentes provienen de distintos fabricantes que se adaptan a estándares muchas veces contrapuestos.

La dirección de la empresa tiene, por tanto, una responsabilidad fundamental por lo que se refiere a la coordinación de los distintos elementos y a la aplicación consistente de los controles de seguridad. Para llevar a cabo esta labor se deben fijar claramente las responsabilidades sobre los diferentes componentes, utilizar informes de excepción efectivos que permitan monitorizar los controles, establecer procedimientos adecuados, implantar una gestión rigurosa de la configuración del sistema, etc.

Cuando el auditor se enfrenta a un entorno de este tipo, puede emplear, entre otras, dos técnicas de control:

14.5.1. Matrices de control

Estas matrices, como la que aparece en la figura 14.7, sirven para identificar los conjuntos de datos del SI junto con los controles de seguridad o integridad implementados sobre los mismos.

Figura 14.7. Matriz de control

Los controles se clasifican, como puede observarse, en detectivos, preventivos y correctivos.

14.5.2. Análisis de los caminos de acceso

Con esta técnica se documentan el flujo, almacenamiento y procesamiento de los datos en todas las fases por las que pasan desde el mismo momento en que se introducen, identificando los componentes del sistema que atraviesan (tanto hardware como software) y los controles asociados (véase figura 14.8).

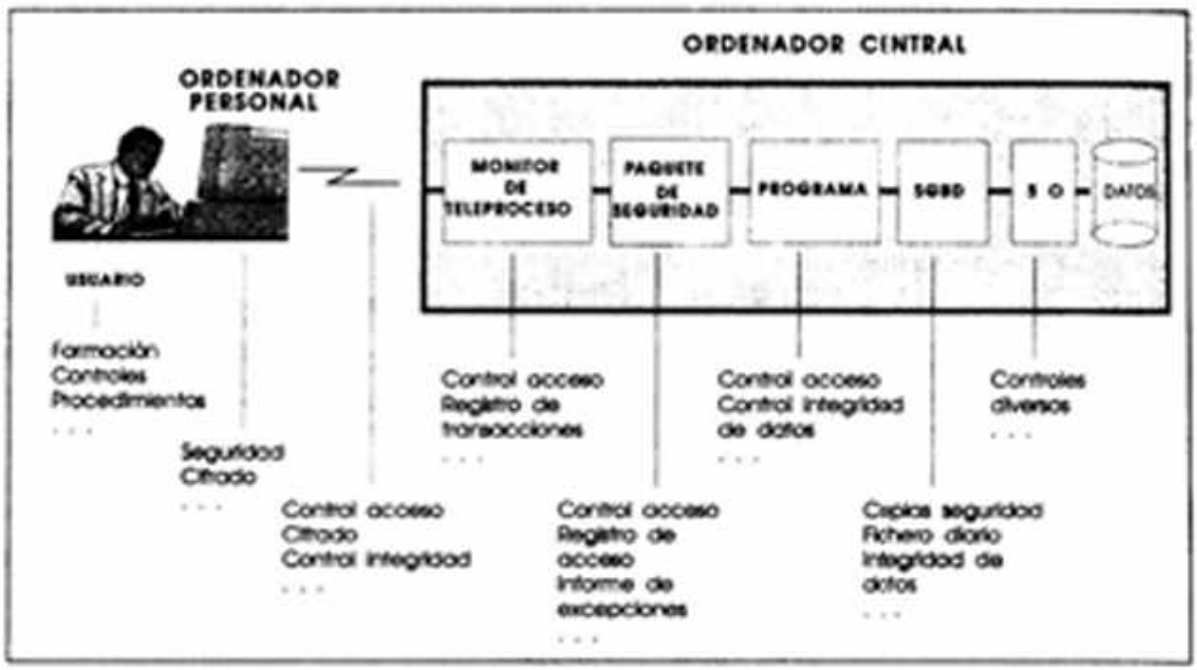


Figura 14.8. Análisis de los caminos de acceso, CLARK et al. *(1991)*

Con este marco, el auditor puede identificar las debilidades que expongan los datos a riesgos de integridad, confidencialidad y seguridad, las distintas interfaces entre componentes y la compleción de los controles.

En la práctica se suelen utilizar conjuntamente ambas técnicas, si bien la del análisis de caminos de acceso requiere unos mayores conocimientos técnicos y se emplea en sistemas más complejos.

14.6. CONCLUSIONES

Como señala BRATHWAITE (1985), *"la tecnología de bases de datos ha afectado al papel del auditor interno más que a cualquier otro individuo. Se ha convertido en extremadamente difícil auditar alrededor del computador"*. Esto se debe, como hemos visto, no sólo a la complejidad de la propia tecnología de bases de datos, sino también a que el entorno del SGBD ha ido creciendo de manera

extraordinaria en los últimos años, por lo que requiere personal especializado (auditores informáticos).

El gran número de componentes que forman dicho entorno y sus interfaces hacen necesario que, antes de empezar una revisión de control interno, el auditor deba examinar el entorno en el que opera el SGBD; que está compuesto, como hemos visto, por el personal de la empresa (dirección, informáticos y usuarios finales), hardware, software, etc.

El auditor debe verificar que todos estos componentes trabajan conjunta y coordinadamente para asegurar que los sistemas de bases de datos continúan cumpliendo los objetivos de la empresa y que se encuentran controlados de manera efectiva.

Por otro lado, hemos visto cómo las consideraciones de auditoría deberían incluirse en las distintas fases del ciclo de vida de una base de datos, siendo muy importante que los auditores participen cada vez más en el proceso de desarrollo, disminuyendo así ciertos costes y haciendo "más productiva" su labor (la dirección de las empresas no siempre "ve" la labor de auditoría y control como realmente productiva, asumiéndola, la mayoría de las veces, como un gasto necesario).

Por lo que respecta al futuro de esta área, con la aparición de nuevos tipos de bases de datos, como las activas, orientadas a objetos, temporales, multimedia, multidimensionales, etc., véase Piattini y Díaz (2000), y la creciente distribución de los datos (bases de datos federadas, multibases de datos, Web, bases de datos móviles, etc.), aparecen nuevos riesgos de interés para el auditor como, por ejemplo, en el área de seguridad, véase Castano *et al.* (1995), o en las metodologías de desarrollo. No olvidemos precisamente que uno de los objetivos de control que señala la ISACF (1996) es que la metodología de desarrollo debe actualizarse, y en estos momentos existen pocas propuestas que abarquen las nuevas tecnologías de bases de datos.

En el futuro es previsible que los SGBD aumenten el número de mecanismos de control y seguridad, operando de forma más integrada con el resto de componentes. Para ello, es fundamental el desarrollo y la implantación de estándares y marcos de referencia como los propuestos por ISO y por el OMG (CORBA), que faciliten unas interfaces claramente definidas entre componentes del sistema de información. Para conseguir este objetivo es importante que las instituciones y personas encargadas de definir estos estándares tomen conciencia de la importancia del control y la auditoría e implementen los mecanismos adecuados.

Desafortunadamente, como nos enseña la experiencia, los sistemas aumentan su complejidad y alcance con mayor rapidez que los procedimientos y técnicas para controlarlos.

Por último, queremos destacar la importancia cada día mayor de una disciplina más amplia que la de bases de datos: la de Gestión de Recursos de Información (o en sus siglas inglesas, IRM, *Information Resource Management),* que nace precisamente con la vocación integradora necesaria para lograr convertir los datos en el activo más importante de las empresas; lo que lleva consigo que las medidas de control y auditoría pasen a un primer plano dentro de las actividades de las empresas.

14.7. LECTURAS RECOMENDADAS

Brathwaite, K. S. (1995). *Data Administration: Selected Topics of Data Control.* Nueva York, EhU U, John Wiley & Sons.

Castano, S., Fugini, M., Martella, G. y Samarati, P. (1995). *Database Security.* Addison-Wesley, Wokingham, Inglaterra.

Clark, R. *et al.* (ed.) (1991). *The Security, Audit and Control of Databases.* Avebury Technical, Aldershot, Gran Bretaña.

De Miguel, A. y Piattini, M. (1999). *Fundamentos y modelos de bases de datos.* 2.ª Ed. Ra-Ma, Madrid.

14.8. CUESTIONES DE REPASO

1. Establezca objetivos de control relativos al diseño de una base de datos.
2. Defina un procedimiento para la adquisición de SGBD.
3. ¿Cuáles son las diferencias más importantes entre las funciones de un administrador de datos y las de un administrador de bases de datos?
4. ¿Por qué resulta tan crítico un diccionario de datos?
5. ¿Qué controles establecería sobre la distribución de listados extraídos a partir de la base de datos?
6. Objetivos de control sobre la formación del personal relacionado con el SGBD (usuarios finales, administradores, diseñadores, etc.).
7. Analice el grado de ajuste existente entre los paquetes de seguridad del mercado (TOP SECRET, RACF, etc.) y los SGBD.

8. ¿Qué riesgos adicionales implica el hecho de distribuir las bases de datos?

9. ¿Qué controles establecería para desarrollos que empleen lenguajes visuales que acceden a bases de datos?

10. Analice el soporte que ofrecen las herramientas de minería de datos al auditor informático.

CAPÍTULO 15

AUDITORÍA DE TÉCNICA DE SISTEMAS

Julio A. Novoa Bermejo

15.1. ÁMBITO DE TÉCNICA DE SISTEMAS

Cuando se habla de sistemas, por definición, se trata de un conjunto de elementos que cooperan en un todo armónico. En ocasiones esos elementos se imbrican unos en otros para integrarse mejor en el conjunto, de manera que a veces resulta difícil identificar los componentes parciales.

Éste es el caso de la Técnica de Sistemas puesto que, según se analice, podría abarcar prácticamente la totalidad del proceso informático como quedar reducido a una parcela muy precisa y con un desempeño muy restringido.

Para ilustrar el primer supuesto valga como ejemplo la titulación que la primera escuela especializada (INSTITUTO DE INFORMÁTICA, 1970) empezó a otorgar a quienes acababan los estudios tras superar el quinto año: TÉCNICO DE SISTEMAS. Según aquel plan de estudios, el TS abarcaba todo el ámbito de la informática, existiendo además tres especialidades que, si no me fallan los datos de que dispongo, eran:

SISTEMAS FÍSICOS
INFORMÁTICA FUNDAMENTAL
INFORMÁTICA DE GESTIÓN

Según esto, tan TS (Técnico de Sistemas) era la persona especialista en Hardware (Sistemas Físicos) como el que se dedicaba al desarrollo de Lenguajes Formales o

Autómatas (Informática Fundamental) como el que trabajaba Aplicaciones (Informática de Gestión).

No obstante, la evolución de la Informática ha obligado a un grado tal de especialización que Comunicaciones, Sistemas Operativos, Seguridad y Bases de Datos han necesitado expertos en áreas muy concretas, dejando la figura de TS relacionada exclusivamente con el Sistema Operativo, no sin habilitar –naturalmente– especialistas en Comunicaciones, Seguridad y Bases de Datos (administradores de esas actividades y/o entornos). Este grado de especialización ha sido necesario, sobre todo, en centros grandes en que las tareas se han hecho más complejas y laboriosas, y en consecuencia, no desempeñables por una única persona. En ocasiones la necesidad de administrar con rigor determinadas instalaciones ha llegado incluso a crear departamentos con las personas que colaboran, en la realización del trabajo correspondiente a la función concreta.

El despegue de la Microinformática y las Redes generan unos nuevos entornos de trabajo, en algunos casos únicos (empresas más pequeñas) y en otros mezclados con los convencionales, pero que requieren una preparación y dedicación específicas. En este sentido oímos hablar cada día (incluso en anuncios de prensa) de TS de Microinformática o TS de Redes.

Parece pues que no es fácil determinar el ámbito de la tarea de TS, pero nuestro compromiso con lo que queremos escribir nos obliga a acotar con claridad la materia en cuestión para poder establecer después las correspondientes actividades de control.

Tratando de utilizar el sentido común y la praxis habitual determinaríamos como ámbito de la tarea de TS la infraestructura informática, es decir el conjunto de instalaciones, equipos de proceso y el llamado software de base. Vamos a puntualizar lo que, según mi criterio, debe incorporar cada uno de estos apartados.

Instalaciones

Este apartado incluiría salas de proceso, con sus sistemas de seguridad y control, así como elementos de conexión y cableado, es decir los elementos base para acondicionar los componentes del apartado siguiente.

Equipos de proceso

Aquí estarían los computadores (main, mini y micro), así como sus periféricos (pantallas, impresoras, unidades de cinta...) y los dispositivos de conmutación y comunicaciones (routers, módems, frads...)

Software de Base

Se compone de los Sistemas Operativos, Compiladores, Traductores e Intérpretes de comandos y programas, junto con los Gestores de Datos (o sistemas de administración de Bases de Datos) y toda una serie de herramientas y componentes auxiliares e intermedios (herramientas de desarrollo, facilidades de explotación como planificadores, paquetes de seguridad, middleware...

Si consideramos infraestructura todo cuanto hemos detallado, es decir, todo lo necesario para que las Aplicaciones funcionen –pues no olvidemos que son el objetivo de nuestros sistemas–, estableceríamos, según mi criterio, el ámbito de TS.

No obstante, dado que existen en esta publicación capítulos específicos dedicados a Auditoría Física, de la Explotación, de Bases de Datos, de la Seguridad y de las Redes, intentaremos centrarnos en el apartado del Sistema Operativo y las Comunicaciones como aspectos no cubiertos en los apartados mencionados.

15.2. DEFINICIÓN DE LA FUNCIÓN

Parece que antes de entrar en la Auditoría de Técnica de Sistemas, deberíamos definir primero la tarea a auditar como una actividad informática que requiere un determinado desempeño profesional para cumplir unos objetivos precisos.

Siguiendo este esquema y buscando un enunciado simple podemos decir que Técnica de Sistemas consiste en la actividad a desempeñar para instalar y mantener en adecuado orden de utilización la infraestructura informática.

De acuerdo con lo ya comentado en el apartado anterior de ámbito, buscando un compromiso formal para separar las Aplicaciones de todo lo necesario para que éstas funcionen correctamente y profundizando en esto diríamos que el funcionamiento correcto se caracterizaría por:

- Disponer de todos los elementos necesarios.
- Por parte de los usuarios autorizados.
- En el momento requerido.
- Con el rendimiento adecuado.

15.3. EL NIVEL DE SERVICIO

No debemos perder de vista que el cumplimiento de tales características constituye el objetivo de los SI (Sistemas de Información) y que su consecución se

expresa en términos de nivel de servicio. Toda nuestra actividad debería estar fundamentada en el logro de ese objetivo y, tanto los procedimientos de actuación como los correspondientes controles, deberían tener como fin último dicha meta.

Entendemos por nivel de servicio una serie de parámetros cuya medición es capaz de determinar objetivamente el mayor o menor grado de eficacia del servicio prestado. No cabe duda de que la obtención de dicho nivel se ve afectada por cuantas incidencias, de cualquier tipo, impacten en el normal desenvolvimiento de la actividad del SI. Así, paradas por instalación de nuevos dispositivos, cambios de versiones del sistema operativo, puesta en servicio de nuevas herramientas, averías de máquina, fallos de corriente o elementos de acondicionamiento, arranque o modificación de enlaces de comunicaciones, inclusión de nuevos usuarios o cualquier tipo de problema con el hardware o el software puede degradar el servicio, con el consiguiente perjuicio para la organización, que no podrá desarrollar sus funciones adecuadamente o en el tiempo preciso, con el correspondiente impacto económico que esto supone y que, generalmente, resultará difícil de calcular, pero, en cualquier caso, importante.

Este apartado de nivel de servicio, requiere un tratamiento específico, toda vez que en la búsqueda de la calidad se convierte en el aspecto clave de la gestión de la configuración. Bastaría decir que sin los clientes del SI no tiene sentido el SI. Y lo que tales clientes necesitan es la garantía de que el SI cumple su función adecuadamente, puesto que, cada vez más, es el fundamento de toda la actividad de la organización.

Digamos para terminar esta breve incursión en el concepto expuesto que la garantía del funcionamiento global se obtiene primero consiguiendo la de cada uno de sus elementos, lo que nos obliga a determinar los puntos críticos que afecten a la actividad del SI y a prever su fallo y planificar los controles y acciones correspondientes para soslayarlo. Comprenderemos que es tan importante detectar la anomalía en un elemento de hardware como la capacidad de subsanarla en tiempo útil, para lo que deberemos disponer del correspondiente contrato de asistencia con un proveedor que nos permita reducir, a lo previsto, el impacto por tiempo de inactividad. Debe añadirse que, con esta filosofía, se negocian con los usuarios y proveedores que reciben el servicio o aportan actividades para su consecución, acuerdos de nivel de servicio (SLA: *Service Level Agreement*) que, por un lado aseguran a nuestros clientes el grado de eficacia negociado y exigen a nuestros proveedores la asistencia requerida para conseguir lo anterior. Hay que entender que en estos términos, se habla comúnmente de disponibilidades por encima del 99,9% (según sectores y grado de criticidad de los SI con relación al impacto en la organización) lo que nos llevaría a no tener interrupciones durante más de 2 horas en total en un año para un servicio estimado en 2.000 horas anuales. Véase que un total de 10 horas de parada en un año para ese mismo servicio supondría una disponibilidad del 99,5%.

La disponibilidad, siendo fundamental, no es el único parámetro a medir, toda vez que no se trata de tener un sistema que responda durante un determinado número de horas al año, sino que además, debe hacerlo bien. Este último aspecto sólo puede comprobarse mediante tiempos de respuesta que den una medida de la utilidad del servicio.

La satisfacción de los usuarios es fruto del resultado general del servicio y depende tanto de la eficacia de las aplicaciones como de la eficiencia del sistema. Este último aspecto está bien representado por los parámetros de disponibilidad y tiempo de respuesta, pero se completa con el análisis de las incidencias originadas por la infraestructura y las opiniones de los usuarios sobre el servicio en la parte correspondiente a ese mismo componente.

15.4. LOS PROCEDIMIENTOS

Toda tarea organizada debe estar descompuesta en una serie de actividades o acciones a realizar con unos procedimientos específicos que garanticen su calidad (o correcto funcionamiento).

De la orientación que hemos dado hacia el servicio, se deduce la tarea de administración de los recursos del SI (infraestructura) que debe optimizar los parámetros antes mencionados, cuestión que ha de convertirse en el objetivo de nuestros procedimientos.

Podemos efectuar una clasificación en:

1. Instalación y puesta en servicio.
2. Mantenimiento y soporte.
3. Requisitos para otros componentes.
4. Resolución de Incidencias.
5. Seguridad y Control.
6. Información sobre la actividad.

La clasificación anterior sirve para cualquier elemento de infraestructura, pero como ejemplo, podemos pensar en el Sistema Operativo de una máquina.

15.4.1. Instalación y puesta en servicio

Comprendería todas las actividades para conseguir el funcionamiento adecuado del elemento en cuestión:

Planificación.	Procedimiento general del suministrador adaptado a la instalación concreta.
Documentación.	Inventario de componentes del elemento y normas de actualización.
Parametrización.	Valores de parámetros del sistema en función del resto de elementos planificados (número y tipos de usuarios, aplicaciones...)
Pruebas.	Verificaciones a realizar y sus resultados.

Debe partirse de los documentos existentes en la organización sobre normativa general: estructura organizativa (especialmente informática), normativas de instalación (como, por ejemplo, direcciones IP a utilizar), metodología general de proyectos y demás informaciones que puedan y deban condicionar la instalación.

15.4.2. Mantenimiento y soporte

Comprendería el conjunto de acciones necesarias para la puesta al día del elemento, así como la asistencia de terceros para la consecución de dicha puesta al día y la asistencia a prestar a otros colectivos (desarrolladores, por ejemplo) para facilitar información necesaria sobre el sistema y sus herramientas para su mejor utilización.

Planificación.	Control del período de garantía y comienzo del mantenimiento del elemento.
Documentación.	Procedimiento para contactar con el soporte.
Parametrización.	Adaptación de los parámetros del sistema en función de nuevos requerimientos o como resultado de nuevas versiones o resolución de incidencias.
Pruebas.	Verificaciones de los cambios o adaptaciones realizadas.

15.4.3. Requisitos para otros componentes

Procedimiento de requerimientos o recomendaciones para el mejor comportamiento de otros componentes del SI.

Planificación.	Considerar los requisitos cruzados de unos elementos con otros, por ejemplo: considerar el espacio en disco necesario para una nueva instancia de una base de datos y, por ende, el impacto en el subsistema de discos y las consecuencias en los back-ups en cuanto a espacio requerido y tiempo necesario, teniendo en cuenta las limitaciones que en cualquiera de estos aspectos pudieran existir.

Documentación.	Procedimiento que determina los efectos a considerar en otros componentes.
Parametrización.	Adaptación de los parámetros del sistema en función de nuevos requerimientos o como resultado de nuevas versiones o resolución de incidencias.
Pruebas.	Verificaciones de los cambios o adaptaciones realizadas.

15.4.4. Resolución de incidencias

Procedimiento para registrar, analizar, diagnosticar, calificar y seguir las incidencias que se produzcan en relación con el elemento en cuestión con el objetivo de su resolución.

Registrar	Supone abrir un formulario en el medio habilitado (papel, electrónico...) que permita recoger los datos que identifican la anomalía: momento en que se produjo, elementos y servicios/usuarios afectados, daños producidos y/o que pueden producirse, entorno del problema y una descripción de lo acaecido (las opiniones de los observadores pueden resultar de interés en algunos casos).
Analizar	Supone buscar una relación entre el efecto y sus posibles causas, para lo que se cuenta, además de los comentarios de los observadores ya mencionados, con la experiencia del técnico que trata la incidencia y la información ya registrada sobre otras incidencias producidas que pudieran estar relacionadas o responder a la misma causa u otra parecida.
Diagnosticar	Determinar de entre las causas posibles aquella que tuviera más probabilidad de resultar el origen del problema una vez analizada la información disponible. En el caso hipotético de no poder establecer una causa del fenómeno reportar al soporte disponible para su diagnóstico.
Calificar	Es un dato importante en el enfoque de la resolución, pues no tiene el mismo tratamiento una anomalía bloqueante que afecta a todo un sistema que un error que se produce de forma muy esporádica y cuyos efectos no son muy problemáticos.
Resolución	Para resolver definitivamente un problema hace falta conocer su causa y la forma de evitar que se reproduzcan las condiciones origen. En caso de disponer de la solución, su

aplicación deberá atenerse a los criterios de nivel de servicio, evaluando la problemática creada por la falta de solución y la que pueda crear la resolución, para coordinar las acciones que menos perjudiquen el servicio global en curso. Supóngase el caso de un problema que sólo puede solucionarse mediante un "parche" de software que sólo puede instalarse parando una máquina que controla un proceso crítico (imagínese cualquier ejemplo en: hospital, banco, producción de fábrica...).

Seguimiento — Es la acción continua y normalizada para conseguir el diagnóstico de una incidencia y la persecución de su resolución.

15.4.5. Seguridad y control

Estos procedimientos adquieren una especial relevancia en el proceso de evitación de incidencias y, caso de producirse, en su temprana detección.

La protección debe considerar tanto la posibilidad de hechos fortuitos como malintencionados. Los primeros se evitarán partiendo de un formación adecuada y competencia profesional más la organización que establezca unos procedimientos robustos que incluyan elementos de control. Los hechos malintencionados se prevendrán mediante una política de personal adecuada y unos procedimientos que eviten concentración de tareas y consideren la segregación de funciones y los correspondientes controles.

Es necesario proteger los accesos a la información y funciones con criterio de mínimos reservando funciones y accesos especiales a niveles de responsabilidad superiores con los controles adecuados.

Por poner ejemplos, diremos que el personal de desarrollo no debe tener acceso a modificar parámetros del sistema operativo y, de igual forma, los TS no deben poder modificar programas.

Uno de los controles típicos en cuanto a los programas objeto o compilados en explotación es el que comprueba que dichos objetos se corresponden con las versiones fuente en vigor. Un control de este tipo también detecta aquellos objetos que no disponen de su correspondiente programa fuente.

Los entornos de desarrollo y mantenimiento de programas deben dejar información sobre las sentencias borradas, modificadas y añadidas, así como los autores de las modificaciones. Estas pistas de auditoría permiten realizar investigaciones para determinar el origen de un determinado cambio.

Es importante que existan una serie de normativas para realizar las funciones informáticas, aunque es igual de importante que tales normas se cumplan.

15.4.6. Información sobre la actividad

Forma parte de la esencia de cualquier actividad rendir cuentas al responsable superior del trabajo realizado. Disponer de una información estructurado, de acuerdo con los parámetros de seguimiento más acordes con los objetivos de desempeño, es cuestión primordial para:

- Conocer la evolución de la actividad.
- Comparar la realidad con objetivos y estándares.
- Mejorar la calidad de la tarea.
- Anticiparse a situaciones críticas analizando las tendencias.

Es uno de los elementos básicos del nivel de servicio siempre que se objetiven parámetros para su seguimiento, es decir, que seamos capaces de medir comportamientos del sistema que estén directamente ligados con la calidad del servicio.

La información debe servir para gestionar y, por tanto, debe ser resumida y expresiva en cuanto a la representación de la realidad, permitiendo profundizar si se requiere un análisis más fino de algún parámetro en aras de localizar la causa de un determinado comportamiento o magnitud.

15.5. LOS CONTROLES

Deberían determinar el comportamiento del sistema y prevenir situaciones no deseadas desde cualquier punto de vista:

Hardware	Existen los componentes adquiridos (inventario) Están correctamente instalados Se mantienen adecuadamente Dan el rendimiento requerido
Software	Se dispone de las correspondientes licencias Está correctamente instalado Se mantiene adecuadamente (versiones oficialmente soportadas) Dan el rendimiento adecuado

Comunicaciones	Existen componentes Están correctamente instalados
Conmutación	Se mantienen adecuadamente Dan el rendimiento adecuado
Comunicaciones	Existen los contratos o servicios Están correctamente parametrizados
Enlaces	Se mantienen adecuadamente Dan el ancho de banda y respuesta necesarios
Seguridad	Existen los procedimientos Se llevan a cabo Se controlan las excepciones Se toman medidas
Información	Se dispone de procedimientos de back-up Se realizan los back-ups correspondientes Se guardan adecuadamente Se comprueban por muestreo
Plan de contingencia	Se dispone de un procedimiento Están contratados los servicios necesarios Está debidamente actualizado Se realizan los ensayos periódicos

La Fundación de Auditoría y Control de Sistemas de Información (ISACF) que otorga la certificación CISA (Certified Information System Auditor) dispone de una publicación interesante sobre los Objetivos de Control para la Información y la Tecnología relacionada (COBIT). Allí se relacionan los procesos de los Sistemas de Información clasificados en dominios: Organización y Planificación, Compras e Implantación, Puesta en Servicio y Soporte y, por último, Monitorización. Estos procesos engloban todas las actividades relacionadas con los Sistemas de Información y, a su vez, con factores como: Personas, Aplicaciones, Tecnología, Explotación y Datos. Por otra parte tienen una conexión mayor o menor con siete Criterios de Información:

1. Eficacia
2. Eficiencia
3. Confidencialidad
4. Integridad
5. Disponibilidad
6. Legalidad
7. Fiabilidad.

La definición del factor Tecnología puede identificarse con el ámbito que estamos aplicando a Técnica de Sistemas, puesto que comprende:

Hardware,
Sistemas Operativos,
Gestores de Bases de Datos,
Redes,
Multimedia,
...

Extrayendo los procesos relacionados con esta definición de Tecnología obtendríamos, según ISACA, los objetivos de control correspondientes al área que nos ocupa: Técnica de Sistemas.

Veamos los objetivos de control en los que se involucra Técnica de Sistemas, según, el concepto anterior:

Definición del plan estratégico tecnológico

Pretende la satisfacción de los requerimientos del negocio buscando un balance óptimo entre las oportunidades de la tecnología de la información, dichos requerimientos y su posterior cumplimiento. Permite un proceso de planificación estratégica que, a intervalos regulares, va cumpliendo los planes a largo plazo. Estos planes a largo plazo deben traducirse periódicamente en planes operativos con objetivos claros y concretos a corto plazo.

Toma en consideración objetivos de negocio y necesidades de tecnología de la información, inventario de soluciones tecnológicas e infraestructura actual y estudios de factibilidad.

Primando fundamentalmente el criterio de eficacia, concede también importancia a la eficiencia.

Determinación de la dirección tecnológica

Se trata de obtener ventajas de las tecnologías emergentes. Pretende crear y mantener un plan de infraestructura tecnológica, adecuando y haciendo evolucionar la capacidad de la infraestructura actual siguiendo los desarrollos tecnológicos, las restricciones del negocio y los planes de adquisición.

Como en el caso anterior, prima la eficacia sobre la eficiencia.

Gestión de inversiones

Asegura la disposición y el control de desembolsos de recursos financieros por medio de los correspondientes presupuestos operativos periódicos establecidos y convenientemente aprobados.

Tiene en cuenta alternativas de financiación, control sobre lo gastado y justificación de costes.

En este proceso tienen la misma importancia, eficacia y eficiencia, considerándose, además, la fiabilidad de lo adquirido.

Apreciación de riesgos

Pretende el aseguramiento de la obtención de los objetivos de TI (tecnología de la información), previniendo las amenazas en la obtención de los servicios de TI. Permite a la organización identificar los riesgos, analizar su impacto y tomar las medidas de coste efectivo para mitigarlos.

Considera distintos tipos de riesgos (tecnología, seguridad, continuidad...), los momentos de análisis (periódicos o durante la implantación de nuevos sistemas), ámbitos globales o específicos, informes de incidencias y el mantenimiento de un modelo de riesgo.

Están involucrados los siete criterios, pero especialmente: confidencialidad, integridad y disponibilidad.

Gestión de proyectos

Supone marcar prioridades para conseguir objetivos en tiempo dentro de los presupuestos. Permite a la organización identificar y priorizar proyectos en línea con el plan operativo. Más aún, la organización debe adoptar y aplicar técnicas seguras de gestión de proyectos para cada proyecto emprendido.

Es preciso tener en cuenta el promotor del proyecto, los usuarios involucrados, las incidencias y los hitos, la determinación de responsabilidades, el comité de seguimiento, los presupuestos de costes y mano de obra, la calidad del plan y la seguridad del plan para con los sistemas sensibles.

En este caso intervienen por igual los criterios de eficacia y eficiencia.

Identificación de soluciones automatizados

Se trata de asegurar la mejor aproximación para satisfacer los requerimientos de los usuarios, facilitando un análisis claro de las oportunas alternativas ajustadas a los requisitos.

Se han de tomar en consideración las restricciones internas y externas (como sistemas heredados), la dirección de la tecnología, los estudios de factibilidad (costes, beneficios, alternativas...), los requerimientos y la arquitectura de información.

Prevalece la eficacia, aunque la eficiencia debe considerarse también.

Adquisición y mantenimiento de infraestructura tecnológica

Este proceso provee las plataformas adecuadas para soportar las aplicaciones del negocio. Permite definir consideraciones específicas de requerimientos funcionales y operativos y una implantación por fases con hitos claros.

Se deben considerar: la disponibilidad de la tecnología, la dirección de su evolución, las políticas de seguridad, el ajuste de los procedimientos a la instalación y la flexibilidad.

Es importante la integridad, pero han de prevalecer eficacia y eficiencia.

Desarrollo y mantenimiento de procedimientos relacionados con los SI (Sistemas de Información)

Pretende asegurar el uso adecuado de las aplicaciones y de las soluciones tecnológicas instaladas. Supone una aproximación estructurada, al desarrollo del usuario y a los manuales de procedimientos operativos, así como a requerimientos de servicio y material de entrenamiento.

Tiene en consideración tanto procedimientos como controles de usuario y procedimientos y controles operativos.

Prevaleciendo eficacia y eficiencia, también –en segundo término– intervienen criterios de integridad, legalidad y fiabilidad.

Instalación y certificación de sistemas

Verifica y confirma que la solución encaja con el propósito perseguido, lo que permite la realización de una correctamente formalizada instalación, migración y conversión así como un plan de aceptación.

Considera la aprobación de la estructura, la documentación, pruebas específicas, entrenamiento, conversión y/o carga de datos y revisiones post-implantación.

Busca la integridad y la disponibilidad, prevaleciendo la eficacia.

Gestión de cambios

Pretende minimizar disfunciones, alteraciones no autorizadas y errores, habilitando la gestión del sistema para el análisis, la implantación y el seguimiento de los cambios solicitados y realizados en la infraestructura de TI existente.

Tiene en cuenta la identificación de los cambios, la categorización, priorización y procedimientos de emergencia, el impacto, la autorización de los cambios, gestión delegada y distribución de software.

Son criterios prioritarios, además de eficacia y eficiencia, integridad y disponibilidad, mientras que la fiabilidad se considera en un segundo plano.

Definición de niveles de servicio

Persigue un entendimiento generalizado sobre el nivel de servicio requerido. Permite el establecimiento de acuerdos de nivel de servicio que formalizan los criterios de rendimiento con los que deben medirse cantidad y calidad del servicio.

Involucra definición de responsabilidades, volúmenes y tiempos de respuesta, dependencias, cargas, garantías de integridad y acuerdos de discreción.

Intervienen los siete criterios, siendo primarios: eficacia y eficiencia.

Gestión de relaciones de servicios de terceros

Aseguran que los roles y responsabilidades de terceras partes están definidos con claridad, son conformes con los requerimientos y continúan satisfaciéndolos. Facilitan

medidas de control para revisar y monitorizar los contratos existentes y los procedimientos para su eficacia y cumplimiento de las políticas de la organización.

Tiene que ver con los acuerdos de nivel de servicio, con los acuerdos de discreción, las políticas de la compañía, las leyes y regulaciones y los contratos de *outsourcing*.

Igual que el proceso anterior, requiere de todos los criterios y, en especial, de eficacia y eficiencia.

Gestión de rendimiento y capacidad

Asegura la existencia de la capacidad adecuada, su disponibilidad y uso óptimos de acuerdo con los requerimientos establecidos. Permite controles para gestionar la capacidad y el rendimiento, que recopilan datos e informan para gestionar la carga, el tamaño de las aplicaciones y la gestión de recursos y peticiones.

Tiene en cuenta volúmenes, tiempos de respuesta y rendimientos.

Busca el factor de disponibilidad, prevaleciendo siempre eficacia y eficiencia.

Aseguramiento de la continuidad del servicio

Dispone el servicio tal y como se requiere y continúa facilitándolo cuando se produce una incidencia. Permite el ejercicio regular de un plan de contingencia estructurado (simulacros) facilitando distintas fases e hitos claros, alineando las TI con los aspectos del negocio.

Considera la clasificación crítica, el plan documentado, los procedimientos alternativos y las pruebas y ensayos sistemáticos y regulares.

Se fundamenta en disponibilidad y eficacia y, de manera secundaria, en eficiencia.

Aseguramiento de la seguridad de los sistemas

Para salvaguardar la información contra usos no autorizados, revelación de información, modificación, corrupción o pérdida, controla el acceso lógico al sistema, a los datos y a los programas, restringiendo éstos a los usuarios autorizados.

Involucra autorización, autenticación, perfiles e identificación de usuarios, gestión de claves e informe de incidencias y seguimiento.

Aplica criterios de confidencialidad e integridad y, en segundo orden, disponibilidad, legalidad y fiabilidad.

Identificación y reparto de costes

Asegurar la correcta atribución de los costes de los servicios de TI. Debe disponerse de un sistema de contabilidad de costes que garantice el registro de los mismos, con el consiguiente cálculo y distribución de detalle.

Considera los recursos a incluir, las políticas de reparto y los ratios de distribución.

Utiliza criterios de eficiencia y fiabilidad.

Gestión de la configuración

Inventariar todos los componentes de los SI, previendo alteraciones no autorizadas, verificando su existencia física y facilitando una base precisa para gestionar el cambio, los controles que identifican y registran todos los bienes y su localización física, así como un programa regular de verificación que asegure su existencia.

Tiene en cuenta el registro de activos y su etiquetado.

Usa criterios de disponibilidad y fiabilidad, dando prioridad a la eficacia.

Gestión de problemas e incidencias

Asegura que se conocen los problemas y las incidencias, que se investigan las causas y que se previene su repetición, permitiendo un sistema que registre y persiga su resolución.

Determina la existencia de pistas de auditoría suficientes sobre problemas y soluciones, el tiempo de resolución de los problemas reportados, procedimientos de escalado (paso de problema a otras instancias) e informes de incidencias.

Criterios primarios: eficacia y eficiencia; secundarios: disponibilidad.

Monitorización de los procesos

Persigue la consecución de los objetivos buscados por los procesos de los SI, definiendo la gestión de informes relevantes para la dirección y de indicadores de rendimiento de la implantación del soporte de los sistemas, así como clarificando los informes sobre una base regular y normalizada.

Son importantes los auto-controles, *benchmarks*, indicadores clave de medición de rendimientos e informes de gestión.

Intervienen los siete criterios, siendo primaria la eficacia.

Seguridad independiente

Para incrementar los niveles de confidencialidad y el beneficio de referencias de las mejores prácticas es importante realizar auditorías independientes a intervalos regulares.

La mencionada auditoría independiente con conceptos de auditoría proactiva, la ejecución de los controles por personal cualificado y la clarificación de las observaciones y las recomendaciones constituyen aspectos clave de esta actividad.

Como en el caso anterior, intervienen los siete criterios, pero aquí, con prioridad los de eficacia y eficiencia.

15.6. AUDITORÍA DE LA FUNCIÓN

No vamos a repetir conceptos clásicos de auditoría, como la necesidad de confeccionar un plan de la misma que incluya el análisis de ejercicios anteriores determinando objetivos precisos y estableciendo un conjunto de pruebas: sustantivas y de cumplimiento que permitan obtener unas conclusiones reflejadas en el informe correspondiente.

Se trata pues de aplicar las ideas anteriores, al segmento de actividad al que nos estamos refiriendo: Técnica de Sistemas.

El último informe de auditoría realizado debe servir para fijar un objetivo concreto: la comprobación de que se han llevado a cabo las recomendaciones expuestas y se han corregido debilidades o puntos negros detectados con anterioridad. El informe final deberá reflejar, en este caso, la realidad contrastada, haciendo hincapié en aquellos objetivos no conseguidos las razones expuestas por los

responsables y unas nuevas recomendaciones al respecto que pueden ratificar los planteamientos originales o plantear alternativas o nuevos objetivos para resolver las debilidades encontradas (controles compensatorios).

En cuanto a los procedimientos, y de acuerdo con lo expuesto en el punto anterior, debe comprobarse:

1. Que existen.
2. Que son consistentes con los objetivos de control.
3. Que se ejecutan.

Comoquiera que el ejercicio de auditoría supone coleccionar unos hechos observados para emitir un juicio ecuánime, profesional e independiente, dichos hechos deben estar contrastados, por lo que se realizan las pruebas sustantivas y de cumplimiento cuyo resultado debe soportar las conclusiones del informe de auditoría.

No podemos olvidar que es el informe de auditoría –como resultado final del trabajo realizado– la base de las acciones correctoras posteriores que debe promover la dirección para soslayar cuantas debilidades y problemas pueda plantear el sistema en su funcionamiento, y consecuentemente, mejorarlo para que responda a los requerimientos que constituyen su razón de ser.

Una adecuada metodología en el desarrollo de la auditoría es fundamental y requiere de aspectos generales, tanto del campo de la auditoría como de la organización de los Sistemas de Información, tanto como de aspectos específicos que, en el caso de TS son especialmente importantes, a tenor de la tecnificación profunda de la función y de la especificidad de los diferentes entornos tecnológicos existentes.

Existe, además, un problema añadido que se origina en la variedad y multiplicidad de los entornos. Hoy en día es difícil encontrar entornos puros y, en la realidad actual, existen distintas partes de los SI que se ubican en máquinas de tipo mainframe, de tipo mini y micros que cada vez son menos micro, puesto que la tecnología evoluciona y desarrollos de unos entornos se aplican a otros; baste poner como ejemplo que la tecnología de discos del entorno microinformático ha sido la base de los actuales desarrollos de sistemas *array* que construyen grandes sistemas de almacenamiento por agregación de elementos más pequeños con el origen mencionado, que, además, se beneficia de los desarrollos de entornos *mainframe* en cuanto a rendimientos: varias vías de acceso, dispositivos caché, etc.

Resulta normal en una empresa de cierto tamaño encontrar un entorno *mainframe* que soporte una serie de funcionalidades, junto con entornos medios para otras y un soporte microinformático, articulado generalmente alrededor de una red que completa la infraestructura de sus sistemas centrales. Pero esto no es todo, sino que se completa

–también usualmente– con equipos en sus centros periféricos que integran las instalaciones con los correspondientes enlaces de comunicaciones y la electrónica inherente.

En entornos heterogéneos se requieren conocimientos específicos de cada sistema operativo, gestor de base de datos, herramientas de desarrollo, administración, seguridad y monitorización.

La función, en estos casos, debe ser auditada desde dos perspectivas diferentes y con equipos de personas distintas:

- Equipo de organización con conocimientos generales que chequee aspectos operativos, como establecimiento y separación de entornos y los procedimientos inherentes a dicha separación y a las funciones generales como resolución de incidencias, planes de contingencia, niveles de servicio o informes periódicos de Técnica de Sistemas sobre el desarrollo de la tarea.

- Equipos expertos en entornos específicos que sean capaces de analizar los parámetros claves del software de base en sus distintas concepciones: sistemas operativos, gestores de bases de datos y herramientas varias.

La existencia de una red de comunicaciones incorpora un nuevo nivel de complejidad, puesto que, para diferentes servicios, pueden existir distintas infraestructuras que se solapan, por ejemplo: líneas de datos para conectar terminales/redes a instalaciones centrales (computadores y/o redes) y otro conjunto de enlaces para interconectar las diferentes ubicaciones de la organización y soportar el servicio de correo electrónico.

Los servicios a través de redes públicas más abiertas y económicas pero mucho menos seguras generan una complejidad añadida que, desde el punto de vista del control, hacen cada vez más difícil su vigilancia, dado el elevado nivel tecnológico de las soluciones en curso y su vocación de apertura y flexibilidad que chocan frontalmente, como se puede comprender fácilmente y ya hemos dicho, con aspectos de seguridad y control necesarios.

En grandes organizaciones es relativamente sencillo urdir estrategias organizativas que cumplan con los criterios básicos de control en cuanto a establecimiento de procedimientos y segregación de funciones para que, por ejemplo, los programadores no puedan modificar los parámetros del sistema (operativo, gestor de datos...) y quienes puedan ejecutar programas en real no puedan modificarlos.

Pero a veces, bien porque se trata de organizaciones más pequeñas con menos recursos tanto operativos como de control, como de grupos de servicio a determinados objetivos parciales con elementos de proceso departamentales, se producen situaciones donde la segregación funcional no existe y surgen –en consecuencia– amenazas y

debilidades que el auditor debe determinar para que mediante otros medios puedan compensarse dichas debilidades, bien a través de otros controles y/o medidas (seguros, por ejemplo).

Puesto que en la presente obra se tratan específicamente aspectos que tienen que ver con TS, vamos a profundizar un poco en el área específica del sistema operativo y herramientas complementarias.

La separación de entornos de traba o constituye un planteamiento fundamental para aislar la producción de los riesgos del desarrollo. Hay que tener en cuenta que, llevadas las cosas al límite en el área de producción, se persigue la estabilidad de los procesos, mientras que en desarrollo, se trata de comprobarla, lo que obligaría a intentar –en pruebas– buscar sus fallos y conseguir incidencias para prevenirlas. En ocasiones, cabría incluso la existencia de otros entornos (en función de las organizaciones) como el de implantación que –siendo una réplica del de producción– permitiría comprobar (en laboratorio) incidencias producidas en explotación, probar circunstancias específicas, sin necesidad de involucrar a las ejecuciones reales e impartir entrenamiento (training) a nuevos usuarios o ante nuevas versiones de aplicación. Por otra parte, las mencionadas separaciones deben conllevar un control sobre las conexiones entre los mismos y las restricciones de acceso de los distintos perfiles (operadores que no pueden compilar programas, programadores que no pueden acceder al entorno de producción, etc.).

Los datos reales no deben ser accesibles ni utilizados para pruebas: sólo en casos especiales para pruebas de volumen podrían tomarse como punto de partida, desvirtuándose en su contenido para el traspaso al entorno correspondiente.

El software de base debe aportar herramientas para modificar programas y controlar los cambios dejando pistas de auditoría, debiendo existir el correspondiente procedimiento que contemple la segregación funcional (aprobación del cambio, realización, validación y puesta en explotación).

La consistencia de los programas ejecutables con las fuentes origen es verificable y garantiza que las aplicaciones en ejecución coinciden con las desarrolladas, validadas, y que sirven de base para cualquier modificación posterior.

Debe comprobarse la existencia de todas las fuentes. La pérdida de alguno deja a la organización en precario frente a cualquier modificación necesaria que afecte a la funcionalidad que soporta el programa en cuestión.

Un control especial debe aplicarse con las utilidades de uso restringido que permiten accesos directos al núcleo del sistema operativo o a los datos. Se trata de elementos sensibles cuyo uso debe estar especificado, toda vez que –en determinados

casos– no dejan pista de las modificaciones realizadas. Existen opiniones a favor de disponer de estas funciones fuera del sistema, cargándolas únicamente cuando sean necesarias y borrándolas después, para evitar que –por una debilidad de seguridad– alguien pudiera acceder a ellas. Con esto se trata de eliminar la omnipotencia de los Técnicos de Sistemas, que deben estar, también, sujetos a una normativa rigurosa.

Ha de tenerse en cuenta el nivel de actualización de los módulos del SO (sistema operativo) y si existen parches pendientes de aplicar, dado que la no actualización mencionada supondría el riesgo ante los errores que las actualizaciones corrigen.

La planificación de acciones debe ser cuidadosa, documentada y con posibilidad de alternativas y de marcha atrás ante cualquier eventualidad imprevista que no permita el correcto funcionamiento del sistema. Ha de tener en consideración los niveles de servicio pactados y procurar el mínimo impacto en la explotación del sistema.

Deben existir planes de respaldo y continuidad en cuanto al software de sistemas, así como el adecuado soporte interno/externo.

El seguimiento de la adecuada sintonía del sistema y su rendimiento debe ser una práctica habitual y continua, para lo cual, además de los datos objetivos sobre parámetros y mediciones, existen herramientas de contraste que permiten evaluar su funcionamiento.

Constituyen riesgos una dependencia inadecuada (del responsable del desarrollo, por ejemplo, lo que supondría falta de segregación funcional), los cambios sin una planificación adecuada y la existencia de superusuarios con una concentración de poder que atente igualmente contra la segregación funcional. Los controles deben buscar supervisión, comprobar la restricción de los accesos y efectuar las revisiones correspondientes.

El riesgo valorado debe estar en consonancia con la organización: no es el mismo en un hospital o en un banco que en un fabricante de sillas. Aunque la repercusión para el negocio pueda ser la misma, no son iguales, ni la probabilidad de su producción ni la repercusión en otros factores (las personas, por ejemplo). En ciertos casos, como complemento o como sustitución por no justificarse determinadas medidas en función de la complejidad y el riesgo en cuestión, puede estudiarse una política de seguros:

SPS	Seguro de soportes de datos
SPW	Seguro de software
SICO	Seguro para cobertura de contingencias
ISPB	Seguro de pérdida de beneficios

También conviene destacar la existencia de herramientas que ayudan en la metodología, recogiendo resultados de observaciones, tabulándolos de acuerdo con factores y parámetros de riesgo para obtener un valor objetivo de los resultados, construyendo, de forma semiautomática el informe de auditoría. De igual forma cabe utilizar útiles específicos para sistemas concretos y revisar sus parámetros e históricos –en cuanto a pistas de auditoría– que, en casos de sistemas complejos, son especialmente recomendables.

15.7. CONSIDERACIONES SOBRE LA TECNOLOGÍA Y SU EVOLUCIÓN

Debemos prepararnos para el cambio de paradigma que se nos avecina, puesto que la complejidad alcanzada por los sistemas distribuidos no compensa su sólo aparente eficiencia. Para justificar esta apreciación baste con referir el alcance técnico de los sistemas distribuidos que –para conseguir la consistencia en la información de los diferentes nodos– se ha normalizado el *comit* de doble fase para garantizar la actualización, en tiempo real, de todos los computadores de la red. En términos vulgares baste con decir que es necesario un enlace de comunicaciones fiable y permanente para garantizar que *en todos los nodos queda actualizada la información en el momento* y yo me pregunto ¿qué diferencia existe entre este sistema y uno centralizado clásico? Según mi opinión, la diferencia es inexistente toda vez que –en ambos casos– el funcionamiento correcto se basa en unas comunicaciones fiables *sin las cuales no funciona, adecuadamente ninguno de los dos, y con las que ambos permiten una operativa correcta.*

En el límite un sistema distribuido podría tener ciertas ventajas en los costes de las comunicaciones siempre que parte de los accesos puedan ser locales y la diferencia compense las actualizaciones distribuidas. Lo que sucede es que es más barato crear, mantener y actualizar un sistema centralizado y, además, *si hay caída en comunicaciones en algún enlace, el resto están totalmente operativos,* mientras que en el caso distribuido, si cae un enlace, sólo están operativos los accesos locales y *hasta que no se restaura el enlace caído, no funciona el sistema para actualizaciones que deban replicarse.*

Para soslayar estas dificultades, los sistemas distribuidos han urdido otras estrategias, basadas en replicadores de transacciones y permitiendo registros pendientes de actualizar que se ponen al día al levantarse la línea de comunicaciones caída. Lo que sucede es que, para que este esquema de replicación (sin *comit* de doble fase) funcione, *obliga a mantener la actualización en un único nodo,* lo que supone la única opción para mantener la consistencia de los datos.

Para colmo de males, la liberalización del sector de las telecomunicaciones y el incremento de las redes y la mejora de calidad de los enlaces, junto al incremento de los costes de desarrollo y mantenimiento de los sistemas, especialmente de los distribuidos, inclina definitivamente la balanza en favor de los sistemas centralizados.

Resulta curioso que en el momento en que la microinformática ha adquirido el espectacular desarrollo de hoy nos planteemos el retorno a los sistemas centralizados, pero todo indica ese camino, ya que, además de los razonamientos expuestos, la realidad de los que se nos ofrece es incuestionable:

- Network Computer (NC). Computadores más simples gobernados por elementos remotos que les suministran los programas a ejecutar.
- Desarrollo de navegadores (Netscape y Explorer) como entornos de trabajo universales.
- Internet como paradigma de conexión y protocolo de comunicación (TCP/IP).

Este nuevo modelo se convertirá en la base de la evolución de las aplicaciones, los centros de proceso y los usuarios.

Las aplicaciones se desarrollarán para instalarse en entornos Web y la parte cliente (a ejecutar en los terminales más o menos inteligentes) en estándar Java, derivados o similares.

Los centros de proceso se centralizarán y los servicios se conectarán con intranets, extranets y/o Internet, tomando una relevancia capital la protección de la información y los accesos, sobre todo en el entorno de negocios; considérense los esfuerzos para poner en marcha el estándar SET para securizar las transacciones vía Internet, cuestión que supone integrar en el proceso a las entidades financieras y de crédito (es un paso más adelante del tradicional EDI).

Los usuarios sufrirán también cambios radicales, puesto que los dos aspectos anteriores son la base para poder trabajar desde cualquier punto (a través de las redes globales mencionadas), tanto en oficinas como en centros de servicio o domicilios particulares servirán de base para todo trabajo que se pueda realizar a través de un computador, es decir, aquel en el que únicamente se maneje información, y no podemos olvidar que el sector de servicios (creciente en economías desarrolladas) tiene un componente importantísimo de trabajo cuyo fundamento es la información.

Para justificar cuanto antecede y sin necesidad de ejercitar la imaginación baste, además de considerar el desarrollo del teletrabajo en otros países, la experiencia, por ejemplo, de entidades financieras en tal asunto: bancos, aseguradoras...

15.8. ALGUNAS REFERENCIAS

Desde el punto de vista metodológico y para ayudar en el proceso de recopilación y tabulación de la información, así como en la redacción de resultados, LOGIC CONTROL dispone de un programa: AUDINFORM que funciona en entorno PC.

Aunque cada fabricante de equipo dispone de ofertas complementarias en cuanto a herramientas para administrar, controlar y monitorizar los sistemas, existen especialistas que se han centrado en desarrollar paquetes que ayudan a normalizar toda una serie de aspectos relacionados con la seguridad, el control y la monitorización de los sistemas que se convierten en piezas básicas para la articulación de los procedimientos de que hemos hablado.

Tal es el caso de Computer Associates, que con su sistema UNICENTER pretende integrar un conjunto de herramientas como el descrito, buscando, además, una homogeneidad funcional de dichas herramientas en los distintos sistemas operativos (como MVS de IBM, Unix, o NT de Microsoft). Es ejemplo obligado citar CAExamine que, en un entorno MVS, permite obtener en tiempo real una revisión sobre seguridad, integridad y mecanismos de control, cuestión que –por otros medios- resulta muy costosa.

También existen compañías cuya especialización consiste en la monitorización de los sistemas, tratando alertas de sistemas operativos, bases de datos y aplicaciones. Tal es el caso de la línea PATROL de BMC Software y otras líneas como TÍVOLI o productos de fabricante de software de base como Oracle Alert (Oracle) o equipos como AV/Alert (Data General).

En el apartado de las comunicaciones el sistema SNMP, para control de elementos remotos (a través de agentes que reportan información a un sistema central), se ha convertido en un estándar, y productos como Openview (HP) o Netview (IBM), gestionan la información de este tipo de agentes para permitir una administración centralizada de elementos remotos de red (redes WAN, estaciones de trabajo o elementos distribuidos).

En el campo del contraste, COMPASS (sede en Barcelona) realiza en España estudios de instalaciones considerando distintos parámetros y comparándolos con otras organizaciones *(bestpractices)* y estándares, produciendo un análisis y el correspondiente diagnóstico de la instalación.

En materia de seguros TELA IBÉRICA (compañía re-aseguradora) especializada en sistemas electrónicos, constituye una referencia (al igual que las principales compañías de seguros: AGF-Fénix, La Estrella...) como especialista en seguros de

soportes de datos, software, mantenimiento de actividad ante contingencias y pérdida de beneficios.

Existen organizaciones independientes, como el *Transaction Processing Council*, que realizan pruebas de rendimientos estándar y facilitan datos certificados e independientes del funcionamiento de los equipos. Tales datos se expresan en Tpm-C o TpmD (transacciones por minuto de tipo C o D) que sirven para evaluar la potencia de las máquinas y contrastar –con la requerida para cada usuario software- la validez de la instalación. Los resultados del T. P. Council están disponibles en Internet.

15.9. LECTURAS RECOMENDADAS

COBIT (Control Objetives for Information and related Technology) de ISACA (Information Systems Audit and Control Association).

Handbook of EDP Auditing.

En general la mencionada ISACA constituye una fuente muy amplia de información, al ser su principal objetivo el control y la auditoría de los SI. Su publicación *IS AUDIT & CONTROL JOURNAL* publica en su número de 1997 (volumen III) interesantes artículos como:

- "Steps to auditing Windows NT".
- "SAP R/3 and auditing logical access".

15.10. CUESTIONES DE REPASO

1. ¿Qué ámbito abarca actualmente la técnica de sistemas?
2. Defina nivel de servicio.
3. ¿Qué procedimientos deberían existir para la instalación y puesta en servicio de un equipo?
4. Enumere los principales aspectos a contemplar en la resolución de incidencias.
5. ¿Con qué criterios auditaría un plan de infraestructura tecnológica?
6. ¿Cómo afecta la heterogeneidad de los entornos a la auditoría de técnica de sistemas?

7. ¿Por qué son peligrosas algunas utilidades que permiten acceso directo a los datos o al núcleo del sistema operativo?

8. ¿Cómo afecta el avance de las comunicaciones a la técnica de sistemas? ¿Y a su auditoría?

9. Analice el impacto de la replicación de datos en un entorno distribuido.

10. Establezca los principales criterios para evaluar herramientas de monitorización de sistemas.

CAPÍTULO 16

AUDITORÍA DE LA CALIDAD

José Luis Lucero Manresa

16.1. PREÁMBULO

La calidad ha dejado de ser un tópico, y forma parte, es necesario que forme parte, de los productos o servicios que comercializamos para nuestros clientes. Está incorporada en nuestra forma de ver la vida. Cada vez exigimos más que los productos o servicios que nos suministran nuestros proveedores tengan el mayor grado de calidad dentro de un precio razonable. El aforismo de "El precio se olvida y la calidad perdura" se hace cada vez más patente.

El cliente es el mejor auditor de la Calidad, él exige el nivel que está dispuesto a pagar por ella, pero no más. Por tanto, debemos de cuantificar cuál es el nivel de Calidad que nos exige para poder planificar la Calidad de los productos semielaborados que se generen a lo largo del proceso de producción del producto o servicio final.

Al analizar las necesidades de nuestros clientes, deberemos tener en cuenta también la previsible evolución de sus necesidades y tendencias en cuanto a características. Deberemos tener en cuenta la evolución tecnológica del entorno de producción de nuestros productos para suministrarlos con el nivel tecnológico adecuado. No debemos olvidar tampoco el nivel de Calidad de nuestros competidores, debiendo elaborar productos cuyas características y funcionalidades sean competitivas con las de nuestros competidores, así como su calidad.

La Calidad se ha convertido en el medio de subsistir dentro de un mercado competitivo, lo cual beneficia al consumidor final, es decir, a nosotros. Es el primer filtro lógico por el que las empresas prevalecen en el mercado, el segundo será la productividad que emplean para conseguir esa calidad.

La Calidad será el objetivo global a conseguir, y la Productividad nos vendrá por añadidura, nunca al revés.

16.2. DEFINICIONES PREVIAS

Vamos a citar algunas definiciones de varios autores que nos ayudarán a centrar lo que se entiende por calidad:

- J.M. JURAN: Adecuación al uso.
- P.B. CROSBY: Cumplimiento de unas especificaciones.
- W.E. DEMING: Un grado predecible de uniformidad y fiabilidad a bajo coste y adecuado. a las necesidades del mercado.
- G.TAGUCHI: Pérdidas mínimas para la sociedad en la vida del producto.
- FEIGENBAUM: Conjunto de características del producto de marketing, ingeniería, fabricación y mantenimiento a través del cual el producto en uso satisface las expectativas del cliente.
- P. DRUCKER: Calidad es lo que el cliente está dispuesto a pagar en función de lo que obtiene y valora.
- AEC (Asociación Española para la Calidad): Conjunto de propiedades y características de un producto o servicio que le confiere su aptitud para satisfacer necesidades establecidas o implícitas.

Los Sistemas de Información cada vez están más presentes en nuestra actividad y en las cosas que nos rodean y que usamos. Simplemente recordar que cuando vamos a un banco cualquier operación que hacemos tiene detrás un Sistema de Información, al hacernos un seguro, al comprar en un supermercado o en unos grandes almacenes, al pagar con nuestra tarjeta de crédito, en todos los casos hay un Sistema de Información que está controlando y gestionando esas operaciones. Incluso al arrancar nuestro coche hay un software que chequea los puntos vitales del mismo.

En este capítulo vamos a centrar nuestro foco en la Calidad del Software y podemos recordar la definición que encontramos en Pressman:

- "Concordancia con los requisitos funcionales y de rendimiento explícitamente establecidos, *con los estándares de desarrollo explícitamente documentados* y con las características implícitas que se espera de todo software desarrollado profesionalmente."

En esta definición podemos destacar qué se entiende por calidad, el cumplimiento de los requerimientos que se han establecido (normalmente por el usuario o el cliente) y las "características implícitas" que debe cumplir todo software hecho profesionalmente aparte de su realización según unos determinados estándares. Es decir, que

además de cumplir con las especificaciones que nos ha dado el cliente o el usuario, debe cumplir con otras características que se dan por sobreentendido que están dentro del "saber hacer" de un buen profesional y que no están específicamente explicitadas.

En muchas ocasiones, esta circunstancia no se da, y algunos desarrolladores de dudosa profesionalidad se parapetan tras la frase: "de eso no se dieron especificaciones", para ocultar una falta de previsión o una carencia de habilidad para obtener del usuario en las entrevistas la información necesaria para completar y complementar los requerimientos funcionales.

16.3. INTRODUCCIÓN

Al decidir acometer la realización de un producto software, deberemos hacer una planificación, y entre otros, habrá que hacer un Plan de Calidad específico para ese producto.

En el centro de producción de software, deberá haber un Plan General de Calidad en el que estarán las especificaciones para poder definir cada uno de los Planes específicos de nuestros desarrollos en función de los atributos de Calidad que deseamos implementar en el software.

En este Plan se definen las actividades de Calidad que se tienen que realizar, en qué momentos tiene que intervenir la función de Aseguramiento de la Calidad, que a diferencia del Control de Calidad intervendrá proponiendo y supervisando los procesos de calidad a realizar en la fase de generación de los distintos componentes, adherencia a estándares, y la intensidad de aplicación de la misma según la criticidad de los productos y el nivel de riesgos que se haya encontrado en la evaluación del sistema.

Dentro de este capítulo, como no podría ser menos, nos vamos a referir a una serie de normas que afectan a su contenido, y en algunos casos incorporaremos algunos de sus párrafos o apartados completos.

En el caso de los procesos de revisiones de calidad, tenemos la norma IEEE Standard 1028 for Software Reviews and Audits.

El objeto de esta norma es definir los requerimientos para los procesos de revisión y auditoría. No está dentro de su cometido el establecer cuándo se necesita realizar un proceso de revisión o de auditoría, quedando determinado este aspecto dentro de los Planes de Aseguramiento de la Calidad específicos de cada Organización, según se ha indicado anteriormente.

En dicha norma da las siguientes definiciones:

16.3.1. Revisión

Es una evaluación del elemento o elementos software o estado del proyecto que investiga las discrepancias con los resultados planificados y las mejoras recomendadas. Esta evaluación sigue un proceso formal (por ejemplo, proceso de revisión de gestión, proceso de revisión técnica, proceso de inspección de software, o proceso de *walkthrough).*

16.3.2. Elemento software

Es un producto entregable o un documento producido durante el proceso o adquirido durante el desarrollo o mantenimiento del software. Algunos ejemplos pueden ser:

1. Documentos de Planificación del proyecto (por ejemplo, planes del desarrollo del software y planes de verificación y validación del software).
2. Especificaciones de requerimientos y diseño del software.
3. Documentación del esfuerzo de las pruebas.
4. Documentación suministrable al cliente.
5. Código fuente de los programas.
6. Representación de las soluciones software implementadas en el firmware.
7. Informes (por ejemplo, revisiones, auditorías y estado del proyecto) y datos (por ejemplo, detección de defectos, pruebas).

16.3.3. Auditoría

Es una evaluación independiente de los procesos, los productos software, el progreso del proyecto o el cómo se realiza el trabajo, que investiga la coincidencia con los estándares, líneas guía, especificaciones y procedimientos basados en criterios objetivos que incluyen los documentos que especifican:

1. La forma o contenido de los productos a producir.
2. Los procesos en los que los productos deben ser producidos.
3. Cómo debe ser medida la adherencia con los estándares o líneas guía.

También incluimos otras definiciones según la EEA[1].

16.3.4 Concepto de evaluación según la EEA[1]

Es el proceso de recolección y análisis de información, y a partir de ella presentar las recomendaciones que facilitarán la toma de decisiones. Las decisiones resultantes de esta evaluación o valoración pueden dar lugar a:

- Autorización para proceder con un proyecto.
- Aprobación para incluir en las listas a nuevos contratistas o suministradores.
- Defensa de la aprobación de un contratista.

16.3.5 Concepto de Auditoría según la EEA[1]

Es una herramienta de valoración. Es un documento interpersonal de examen y análisis de evidencias objetivas. A los efectos del control de la calidad, una auditoría no incluye vigilancia o inspección con el objeto de un control de calidad.

Debe reconocer que sólo una muestra de la información disponible puede ser examinada. Que es importante que el tamaño de la muestra de la auditoría aporte la confianza suficiente en las recomendaciones finales.

16.4. CARACTERÍSTICAS DE LA CALIDAD SEGÚN ISO 9126

Antes de detallar los Procesos de Calidad, vamos a describir los componentes de una especificación de calidad del software según el modelo definido en la norma ISO 9126 y el modelo extendido ISO para la Calidad del Software.

16.4.1. Características

Según la citada norma ISO 9126, define las características de calidad como "Un conjunto de atributos del producto software a través de los cuales la calidad es descrita y evaluada". Las características de calidad del software pueden ser precisadas a través de múltiples niveles de subcaracterísticas.

Dicha norma define seis características:

Funcionalidad: Conjunto de atributos que se refieren a la existencia de un conjunto de funciones y sus propiedades específicas. Las funciones son tales que cumplen unos requerimientos o satisfacen unas necesidades implícitas.

[1] Guide to Software Quality Audit de la EEA, (Electronic Engineering Association).

Fiabilidad: Conjunto de atributos que se refieren a la capacidad del software de mantener su nivel de rendimiento bajo unas condiciones especificadas durante un período definido.

Usabilidad: Conjunto de atributos que se refieren al esfuerzo necesario para usarlo, y sobre la valoración individual de tal uso, por un conjunto de usuarios definidos o implícitos.

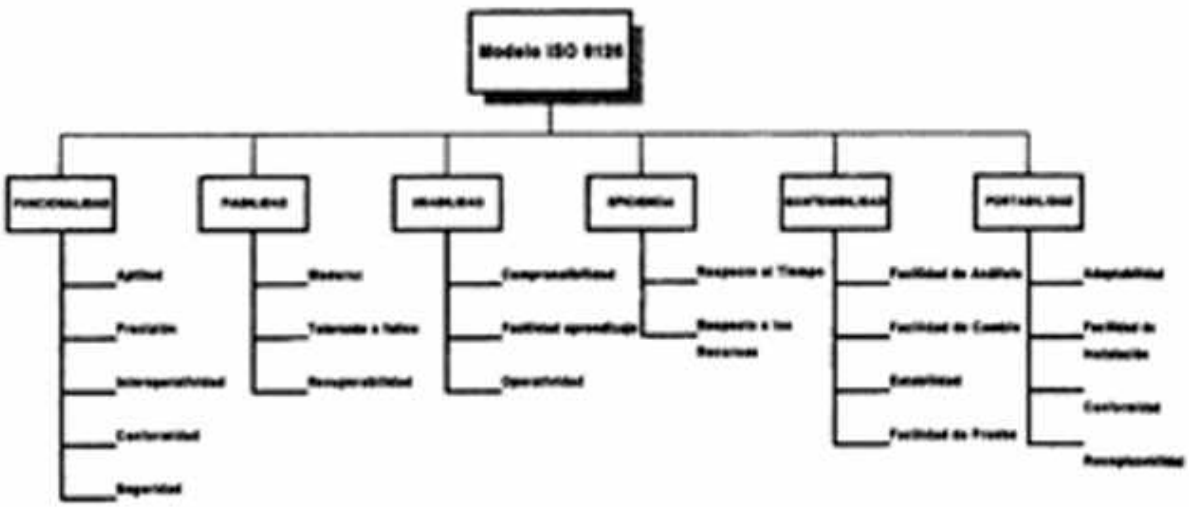
Eficiencia: Conjunto de atributos que se refieren a las relaciones entre el nivel de rendimiento del software y la cantidad de recursos utilizados bajo unas condiciones predefinidas.

Mantenibilidad: Conjunto de atributos que se refieren al esfuerzo necesario para hacer modificaciones especificadas.

Portabilidad: Conjunto de atributos que se refieren a la habilidad del software para ser transferido desde un entorno a otro.

La norma incluye un anexo en el que desglosa en un conjunto de subcaracterísticas cada una de las características anteriormente citadas. Este anexo puede considerarse informativo y no como parte oficial del estándar ISO 9126.

El prefijo sub nos hace destacar un importante aspecto del modelo ISO 9126: La calidad es modelizada en forma jerárquica. En la figura adjunta se incluye una representación de este modelo jerárquico.



16.4.2. Modelo ISO Extendido

El modelo ISO Extendido incluye al modelo ISO 9126 adicionando doce características más, según se expone en la figura adjunta.

La valoración de estas características es útil para que el usuario pueda definir los requerimientos del producto utilizando solamente las características que emplee en la práctica.

Para algunos tipos de productos, hay determinadas características que no son significativas, y las restantes no garantizan que con ellas comprendan todos los requerimientos de los productos, por lo que en cada caso habrá que completarlas con otras definiciones más específicas para esos productos o situaciones.

No obstante el modelo tiene el nivel de abstracción suficiente como para que sea adaptable en la mayoría de las situaciones, siendo, además, independiente de la tecnología.

Las características no pueden ser cuantificadas como tales, y para cuantificarlas en alguna forma, usaremos los "Indicadores".

Para usar los indicadores, deberemos definir un "Protocolo", de forma que mediante dicho protocolo podamos establecer la medida de la característica repetible. Este protocolo nos describirá los pasos que hay que dar para conseguir obtener esta medida de forma tal que en las mismas situaciones obtengamos idénticos resultados.

Los indicadores que se describen en el modelo ISO Extendido, sirven como punto de partida, no queriendo decir que esa lista sea completa. En ella se pretenden presentar ideas para poder definir las especificaciones de calidad, siendo muy importante seleccionar los indicadores que mejor se ajusten a la situación de nuestro proyecto o producto.

El protocolo de medida tiene como objetivo el reproducir los resultados de las mediciones de los indicadores. Según se ha indicado anteriormente, al describir los requerimientos de la calidad del software, se corre el peligro de una interpretación subjetiva del significado de calidad. Es, por tanto, de gran importancia acordar de una forma clara cómo medir los indicadores de forma que esta medida sea reproducible con los mismos resultados.

Ejemplo[2]:

Si deseamos medir el atributo **Facilidad de aprendizaje,** que podemos definir como el esfuerzo de los usuarios para aprender a manejar una aplicación.

Podríamos hacer una cuantificación fácil, si pudiéramos medir de una forma objetiva un factor de Facilidad de aprendizaje de 7 sobre 10, pero éste no sería muy descriptivo ni útil.

Podemos buscar un *indicador* de este atributo que estuviera presente en el producto software. Este indicador debe estar acompañado del *Protocolo* de medida que describa los pasos a dar para asegurar la repetitividad de la medida.

En este ejemplo hemos tomado como indicador el **tiempo medio de aprendizaje,** siendo el tiempo promedio que el usuario final de un determinado grupo necesita para aprender a trabajar con el producto software, más el tiempo necesario de tutelaje.

El protocolo sería:

1. Selección de un grupo representativo de usuarios.
2. Preparación de un curso para este grupo, diseñado para este producto software, o dar a este grupo la oportunidad de auto-enseñanza del producto.
3. Definición del tiempo del curso o de la auto-enseñanza, más el tiempo de tutelaje necesario para conseguir su manejo o pasar con éxito un test.
4. Cálculo del número medio de horas.

[2] "Specifying software quality with the extended ISO model" R.H.J. Van Zeist and P.R.H. Hendriks (Software Quality Jouinal).

Los valores obtenidos de las características se pueden representar en un diagrama de Kiviat según se muestra en la figura, en el que en cada radio nos mostraría el valor de una característica.

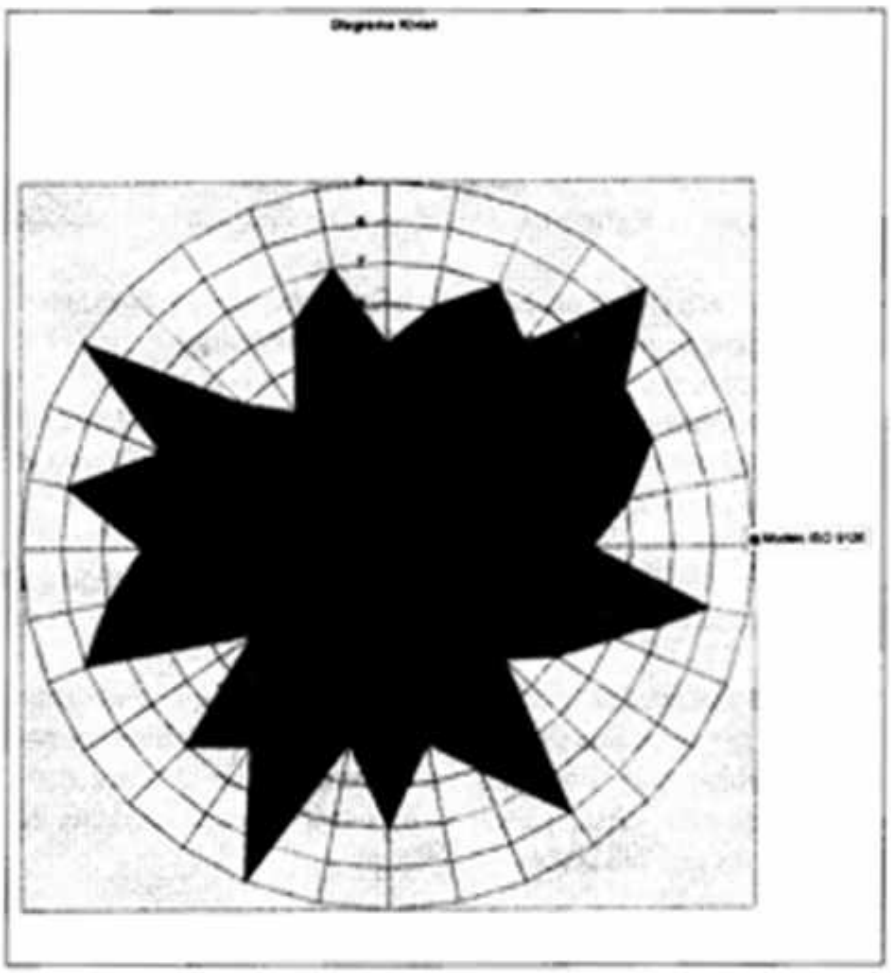
El valor de los indicadores depende del propósito de la especificación de calidad, pudiendo definirse diferentes valores. Es aconsejable usar una plantilla con estos valores. A continuación se expone un pequeño ejemplo de este tipo de plantilla[3].

Peor: El peor límite aceptable de la escala, tal como un fallo total del sistema.

Planificado: Valor esperado del indicador que se considera un éxito.

Récord: Máximo valor teórico o práctico de un indicador, valor límite pero no un requerimiento esperado.

Actual: Valor actual del indicador en el sistema que se está considerando a efectos de posibles comparaciones.



[3] "Software Engineering Management" T. Gilb (Addison-Wesley).

Como experiencia práctica del uso del modelo ISO Extendido tenemos la realizada por las compañías participantes en el proyecto QUINT (Quality in Information Technology)[4] cuyo primer proyecto empezó en 1991, siendo su objetivo el desarrollar un modelo y una guía para las especificaciones de calidad del software, participando todas las partes involucradas en la negociación sobre los requerimientos.

El segundo proyecto QUINT expandió los resultados del primero. En él participaron seis compañías bajo la dirección de los institutos de investigación SERC, TNO/TPD y FPIQM.

16.5. OBJETIVOS DE LAS AUDITORÍAS DE CALIDAD

Una auditoría de Calidad tiene como objetivo el mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar adversamente esa confianza.

Hay varias razones para realizar una auditoría:

- Establecer el estado de un proyecto.
- Verificar la capacidad de realizar o continuar un trabajo específico.
- Verificar qué elementos aplicables del programa o Plan de Aseguramiento de la Calidad han sido desarrollados y documentados.
- Verificar la adherencia de esos elementos con el programa o Plan de Aseguramiento de la Calidad.

El propósito y la actividad de la auditoría es recoger, examinar y analizar la información necesaria para tomar las decisiones de aprobación.

La auditoría debe tener capacidad para investigar la pericia técnica, el desarrollo del software o la capacidad del departamento de desarrollo, el esfuerzo disponible, el soporte del mantenimiento o la efectividad de la gestión.

En las auditorías debe acordarse el dirigirse a criterios específicos tales como la realización del código software.

Cuando se identifiquen los puntos débiles, los auditores deberán tomar una actitud positiva y utilizar sus conocimientos y experiencia para hacer recomendaciones constructivas. En realidad, una función del auditor es pactar la idoneidad de cualquier acción correctiva propuesta. Este papel, si es usado adecuadamente, es uno de los vínculos más valorados entre las partes.

[4] "QUINT Het specifieren van software-kwaliteit", Kluwer Bedrijfswetenschappen, Deventer, the Netherlands, ISBN 90 267 1808 X (1992).

16.6. PROCESOS DE CALIDAD

En el entorno económico actual, la característica más importante es la competitividad, lo que quiere decir que los precios a los que ofrezcamos nuestros productos a nuestros clientes deben ser iguales o más bajos que los de la competencia, pero con una calidad más alta. Para conseguirlo es necesario tener una estructura de costes adecuada y disponer de una estrategia de Calidad que afecte a todas las áreas de la entidad u organismo.

Para satisfacer los requisitos de calidad es necesario conocer las Necesidades del Cliente. Éstas vienen dadas por estos tres parámetros:

- Calidad de los productos y servicios.
- Plazo de entrega adecuado.
- Coste dentro de los límites fijados.

El establecimiento de acuerdos de Nivel de Servicio y el cumplimiento de sus requerimientos le dará un determinado grado de satisfacción, que deberemos saber medir sobre todo una vez pasado el período de estabilización del producto entregado.

Una de las principales características de los procesos de calidad es la repetitividad de los mismos. Todo proceso debe estar suficientemente definido como para que pueda ser repetido consiguiendo los mismos resultados cada vez que se realice el mismo proceso. La idea "Sigma" está unida a la variabilidad de un proceso.

Una vez alcanzada esta repetitividad de los procesos y teniendo elementos para medir los atributos de los productos obtenidos, trataremos de ir refinando el modelo del proceso para reducir los defectos entregados (definiendo defecto como cualquier variación de una característica establecida que origina el incumplimiento de las necesidades del cliente con la consiguiente insatisfacción del mismo).

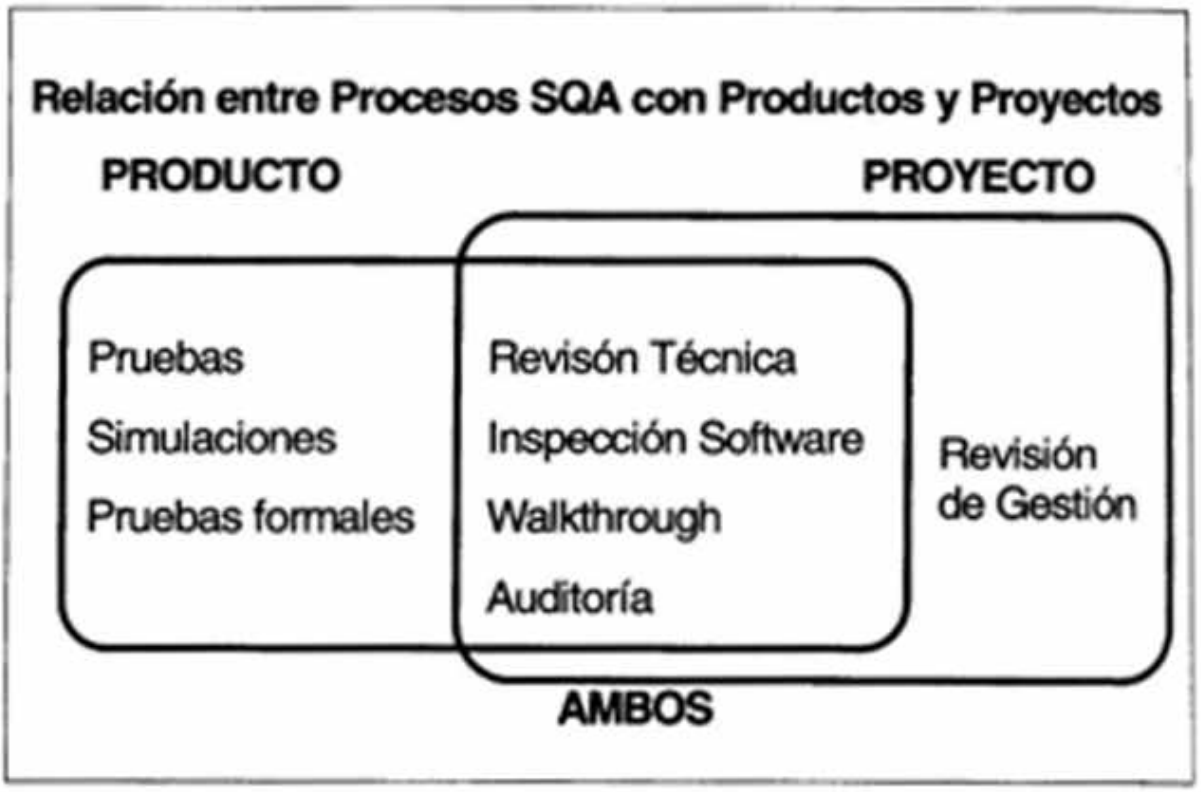
Como se ha indicado anteriormente, las revisiones y las auditorías pueden usarse para actividades de aseguramiento de la calidad, gestión de proyectos, gestión de la configuración o funciones de control singulares.

Según el estándar IEEE 1028, incluimos una tabla en la que se señalan los principales Procesos para conseguir Objetivos de Calidad.

Principales Procesos para conseguir Objetivos de Calidad

Objetivos	Principales Procesos que Incluye
Evaluación	Revisiones de Gestión, Revisiones Técnicas
Verificación	Inspecciones, *Walkthrough*
Validación	Pruebas
Conformidad, Confirmación	Auditoría

También en la figura siguiente se refleja la relación entre procesos y productos dentro de la actividad de Aseguramiento de la Calidad.



El examen de los aspectos técnicos y de gestión se realiza en varias fases durante el ciclo de vida del proyecto. El resultado son controles para permitir mejorar los métodos y asegurar la calidad del software y la posibilidad de conjugar las restricciones de tiempo y coste. La evaluación de los elementos software se realiza durante la generación de esos elementos y a su término. Esto asegura que los elementos terminados expresan correctamente las especificaciones de su "línea base".

Cualquier proceso estándar tiene unas condiciones como prerrequisitos; éstas son necesarias, aunque no son suficientes en sí mismas para que el proceso quede completado. Para las revisiones las auditorías las condiciones son:

Prerrequisitos en los Procesos de Revisión

El objetivo de una Revisión de un elemento software es evaluar el software o el estado, del proyecto para identificar las discrepancias sobre los resultados planificados y recomendar mejoras cuando sea apropiado.

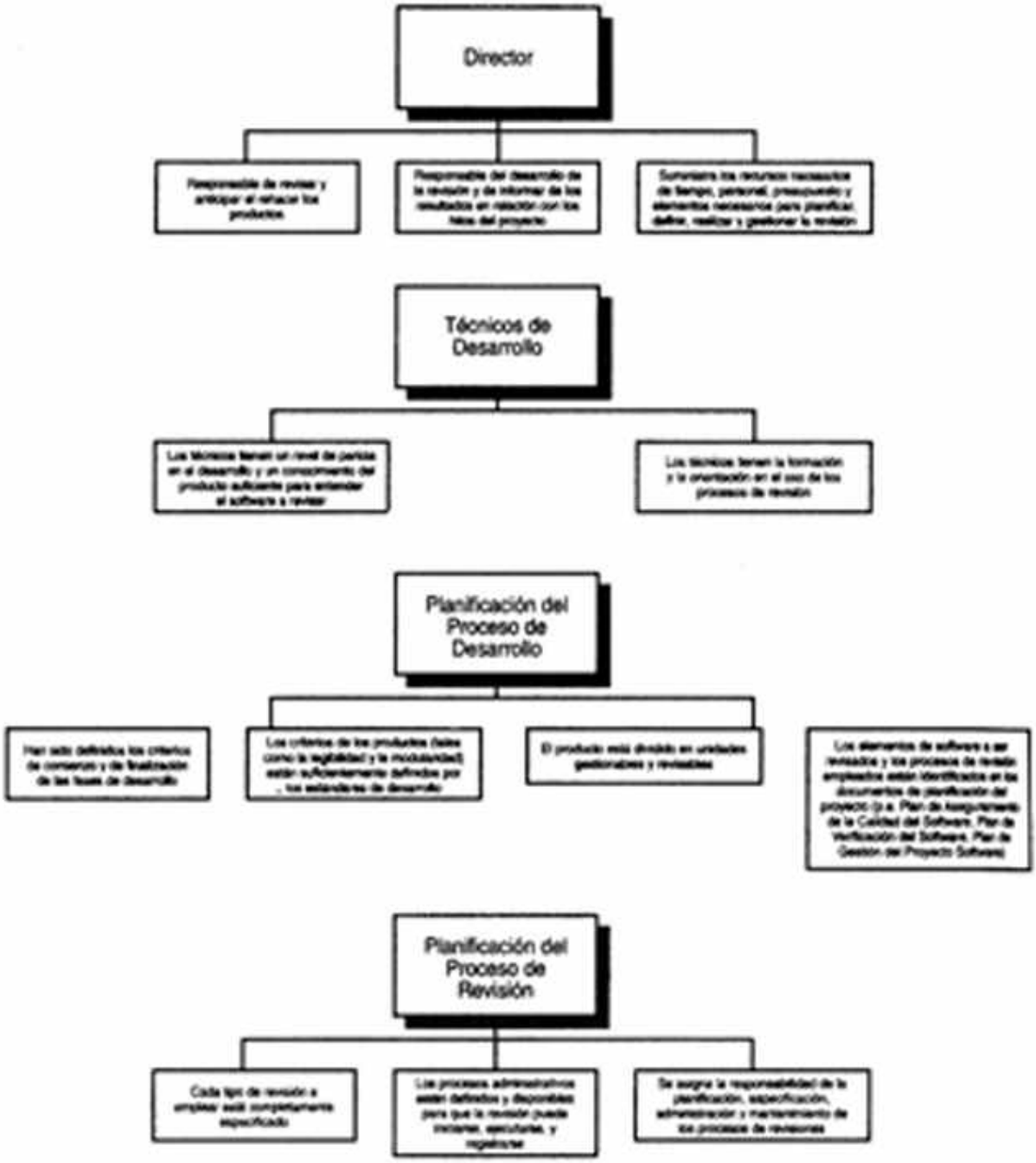
En la figura de la página siguiente se reflejan los prerrequisitos del Proceso de Revisión.

El objetivo de la auditoría del Software es suministrar una evaluación objetiva de los productos y los procesos para corroborar la conformidad con los estándares, las líneas guía, las especificaciones y los procedimientos. Los siguientes requerimientos son prerrequisitos para conseguir este objetivo:

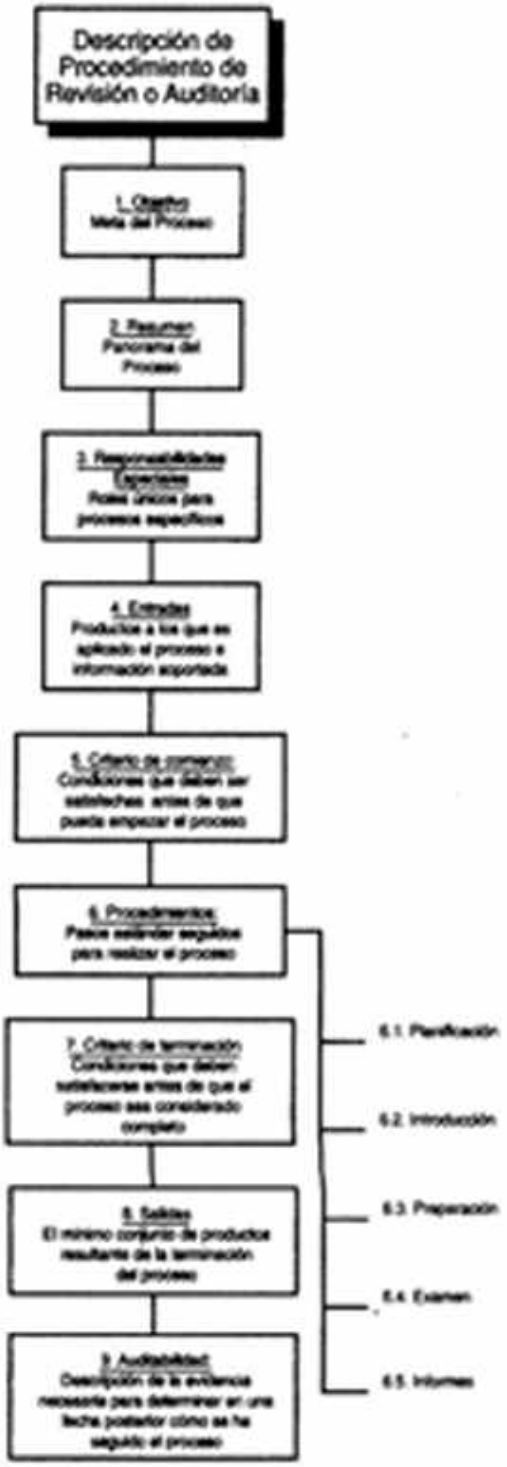
1. Objetivo de la auditoría, criterios existentes (por ejemplo, contratistas, requerimientos, planes, especificaciones, estándares) en relación con los elementos software y los procesos que puedan ser evaluados.

2. El personal de auditoría es seleccionado para promover los objetivos del grupo. Son independientes de cualquier responsabilidad directa para los productos y los procesos examinados y pueden provenir de una organización externa.

3. El personal de auditoría debe tener la suficiente autoridad que le permita una adecuada gestión con el fin de realizar la auditoría.



En la figura de la página siguiente se incluye una descripción esquemática del procedimiento a utilizar para planificar, preparar y realizar cualquier proceso de revisión o de auditoría, según el estándar IEEE 1028.



16.7. EL PROCESO DE AUDITORÍA DEL SOFTWARE

1. *Objetivo.* Según se ha indicado es proveer la confirmación de la conformidad de los productos y los procesos para certificar la adherencia con los estándares, líneas guía, especificaciones y procedimientos.

2. *Resumen.* La auditoría es realizada de acuerdo con los planes y procedimientos documentados. El plan de auditoría establece un procedimiento para dirigir la auditoría y para las acciones, de seguimiento sobre las recomendaciones de la auditoría.

Al realizar la auditoría, el personal de la auditoría evalúa los elementos software y los procesos para contrastarlos con los objetivos y criterios de la auditoría, tales como contratos, requerimientos, planes, especificaciones o procedimientos, líneas guía y estándares.

Los resultados de la auditoría son documentados y remitidos al director de la organización auditada, a la entidad iniciadora de la auditoría, y a cualquier organización externa identificada en el plan de auditoría. El informe incluye una lista de elementos no conformes u otros aspectos para las posteriores revisiones y acciones. Cuando sea estipulado en el plan de auditoría, las recomendaciones son informadas e incluidas en los resultados de la auditoría.

3. *Responsabilidades especiales.* Es responsabilidad del líder del equipo de auditoría el organizar y dirigir la auditoría y la coordinación de la preparación de los puntos del informe de auditoría. El líder del equipo deberá asegurar que el equipo de auditoría está preparado para llevar ésta, y que los procedimientos y los distintos puntos son realizados y reflejados en los informes de acuerdo con su alcance.

La entidad iniciadora de la auditoría es responsable para autorizar ésta. La dirección de la organización auditora asume la responsabilidad de la auditoría, y la asignación de los recursos necesarios para realizar dicha auditoría.

Aquellos cuyos productos y procesos son auditados suministrarán todos los materiales y recursos relevantes y corregirán o resolverán las deficiencias citadas por el equipo de auditoría.

4. *Entrada.* Se requieren las siguientes entradas para realizar la auditoría:

1. El propósito y alcance de la auditoría.
2. Criterios objetivos de la auditoría, tales como contratos, requerimientos, planes, especificaciones, procedimientos, líneas guía y estándares.
3. Los elementos software y los procesos a auditar y cualquier antecedente pertinente.
4. Información complementaria respecto a la organización responsable de los productos y los procesos a auditar (por ejemplo, organigramas de la organización).

5. *Criterio de comienzo.* La necesidad para que una auditoría se inicie debe ser por uno de los siguientes sucesos:

1. Se ha alcanzado un hito especial del proyecto. La auditoría es iniciada por planes previos (por ejemplo, el plan de aseguramiento de calidad, el plan de desarrollo del software).
2. Partes externas (por ejemplo, agencias reguladores o usuarios finales) demandando una auditoría en una fecha específica o en un hito del proyecto. Ésta puede ser por la realización de un requerimiento de un contrato o como prerrequisito a un acuerdo contractual.
3. Un elemento de la organización local (por ejemplo, el director del proyecto, la dirección funcional, ingeniería de sistemas, aseguramiento o control interno de la calidad) ha requerido la auditoría estableciendo una necesidad clara y específica.
4. Un hito especial del proyecto, fecha de calendario, u otro criterio ha sido alcanzado y dentro de la planificación de la organización de auditoría le corresponde la iniciación de una auditoría.

6. *Procedimientos:*

6.1. **Planificación.** La organización de auditoría debe desarrollar y documentar un plan de auditoría para cada auditoría. Este plan deberá apoyarse en el alcance de la auditoría identificando lo siguiente:

1. El proceso del proyecto a examinar (suministrado como entrada) y el tiempo de observación del equipo de auditoría.
2. Los requerimientos del software a examinar (suministrado como entrada) y su disponibilidad. Cuando se usa el muestreo, debe utilizarse una metodología estadística válida al respecto para establecer los criterios de selección y el tamaño de la muestra.
3. Los informes serán identificados (informes de resultados, y opcionalmente el informe de recomendaciones y definido su formato general). Si las recomendaciones son requeridas o excluidas, debe ser indicado explícitamente.
4. Distribución de informes.
5. Requerimientos de las actividades de seguimiento.
6. Requerimientos: actividades necesarias, elementos y procedimientos para cubrir el alcance de la auditoría.
7. Objetivos y criterios de auditoría: proveen las bases para determinar las coincidencias (suministradas como entrada).
8. Procedimientos de auditoría y listas de comprobación.
9. Personal de auditoría: número requerido, perfiles, experiencia y responsabilidades.
10. Organizaciones involucradas en la auditoría (por ejemplo, la organización cuyos productos y procesos están siendo auditados).
11. Fecha, hora, lugar, agenda y la audiencia a quien se dirige la sesión de introducción (opcional).

El líder del equipo de auditoría asegurará que su equipo está preparado e incluye los miembros con la experiencia y pericia necesaria.

La notificación de la auditoría a las organizaciones involucradas debe realizarse con una anterioridad razonable, excepto en el caso de las auditorías no anunciadas. La notificación deberá ser hecha por escrito y deberá incluir el alcance la identificación de los procesos y productos a auditar, así como la identificación de los auditores.

6.2. **Introducción.** Opcionalmente es recomendable hacer una reunión introductoria con la organización a auditar en el momento del arranque para examinar las fases de la auditoría. La reunión de introducción encabezada por el líder del equipo de auditoría, abordará lo siguiente:

1. Introducción sobre los acuerdos existentes (por ejemplo, alcance de la auditoría, planificación, contratos afectados).
2. Introducción de la producción y procesos a ser auditados.
3 Introducción del proceso de auditoría, sus objetivos y sus salidas.
4. Contribuciones esperadas de la organización auditada al proceso de auditoría (número de personas a entrevistar, facilidades para reuniones, etc.).
5. Planificación específica de la auditoría.

6.3. **Preparación.** Los siguientes puntos son requeridos para la preparación del equipo de auditoría:

1. Entender la organización: es esencial para identificar las funciones y las actividades realizadas por la organización auditada, así como para identificar las responsabilidades funcionales.
2. Entender los productos y los procesos: es prerrequisito para el equipo de auditoría conocer los procesos y los productos a auditar mediante lecturas e informes.
3. Entender los objetivos y criterios de la auditoría: es importante que el equipo de auditoría esté familiarizado con el objetivo de la auditoría y los criterios usados en ella.
4. Preparación para el informe de auditoría: es importante seleccionar el mecanismo administrativo de información que será usado durante la auditoría para ir confeccionando el informe siguiendo el diseño determinado en el plan de auditoría.
5. Detalle del plan de auditoría: seleccionar el método apropiado para cada paso en el programa de auditoría.

Adicionalmente el líder del equipo de auditoría deberá hacer los preparativos necesarios para:

1. Orientar a su equipo y formarlo si es necesario.
2. Preparar lo necesario para las entrevistas de la auditoría.
3. Preparar los materiales, documentos y herramientas necesarias según los procedimientos de auditoría.
4. Identificar los elementos software a auditar (por ejemplo, documentos, archivos informáticos, personal a entrevistar).
5. Planificar las entrevistas.

6.4. **Examen.** Los elementos que han sido seleccionados para auditarse deberán ser valorados en relación con el objetivo y criterios de la auditoría. Las evidencias deberán ser examinadas con la profundidad necesaria para determinar si esos elementos cumplen con los criterios especificados.

La auditoría será la adecuada para conseguir:

1. Revisar los procedimientos e instrucciones.
2. Examinar la estructura de descomposición de los trabajos.
5. Examinar las evidencias de la implantación y lo equilibrado del control.
4. Entrevistar al personal para averiguar el estado y el funcionamiento de los procesos y el estado de los productos.
5. Examinar cada documento.
6. Comprobar cada elemento.

6.5. **Informes.** A continuación del examen de auditoría, el equipo auditor deberá emitir un borrador del informe de auditoría a la organización auditada para su revisión y comentarios.

El equipo auditor podrá rehacer el informe de auditoría antes de que se tenga el resultado formal del informe. Estas adaptaciones se harán de acuerdo con la revisión del borrador del informe y resolverán cualquier mal entendido o ambigüedad mientras se mantiene la objetividad y exactitud. Esto también sirve para asegurar la fácil utilización del informe dándole consistencia en los detalles e incluyendo cualquier nueva información verificada. La práctica recomendada es involucrar a los representantes de la organización auditada en la revisión de los resultados de la auditoría.

Involucrando a la organización auditada se contribuye a mejorar la calidad del informe mediante la interacción y la posible aportación de cualquier evidencia adicional.

El grupo de auditoría organizará una conferencia posterior a la auditoría para revisar con los técnicos de la organización auditada las deficiencias, fallos y (si es aplicable) las recomendaciones. Los comentarios y los puntos abordados por la organización auditada, deberán ser resueltos.

El informe final de la auditoría debe ser preparado, aprobado y distribuido por el líder del equipo de auditoría a las organizaciones especificadas en el plan de auditoría.

6.6. **Criterio de terminación.** Una auditoría debe ser considerada terminada cuando:

1. Se ha examinado cada elemento dentro del alcance de la auditoría.
2. Los resultados han sido presentados a la organización auditada.
3. La respuesta al borrador de los resultados ha sido recibida y evaluada.
4. El resultado final ha sido formalmente presentado a la organización auditada y a la entidad iniciadora.
5. El informe final ha sido preparado y enviado a los receptores designados en el plan de auditoría.
6. El informe de recomendaciones, si el plan lo requiere, ha sido preparado y enviado a los receptores designados en el plan de auditoría.
7. Se han realizado todas las acciones de seguimiento incluidas en el alcance de la auditoría (o en el contrato).

6.7. **Salidas.** Como un marco estándar para los informes, el informe borrador de auditoría y el informe final de auditoría, deberán contener como mínimo, lo siguiente:

1. *Identificación de la auditoría.* Título del informe, organización auditada, organización auditora y fecha de la auditoría.

2. *Alcance.* Alcance de la auditoría, incluyendo la enumeración de los estándares, especificaciones, prácticas y procedimientos que constituyen su objetivo y el criterio contra el cual será dirigida la auditoría de los elementos software y de los procesos a auditar.

3. *Conclusiones.* Un resumen e interpretación de los resultados de la auditoría incluyendo los puntos clave de los aspectos no conformes.

4. *Sinopsis.* Un listado de todos los elementos software auditados, los procesos y los elementos asociados.

5. *Seguimiento.* El tipo y el cronograma de las actividades de seguimiento de la auditoría.

Adicionalmente, cuando lo estipule el plan de auditoría, las recomendaciones deberán enviarse a la organización auditada o a la entidad que inicie la auditoría. Las recomendaciones irán en un informe separado de los resultados.

6.8. **Auditabilidad.** Los materiales que documentan el proceso de auditoría deben ser mantenidos por la organización auditora durante un período estipulado después de la auditoría e incluyendo lo siguiente:

1. Todos los programas de trabajo, listas de comprobación, etc. con todos sus comentarios.
2. El equipo de técnicos.
3. Comentarios de las entrevistas así como de las observaciones.
4. Evidencias de pruebas de conformidad.
5. Copias de los elementos examinados con sus comentarios.
6. Informes borradores con las respuestas de la organización auditada.
7. Memorándum del seguimiento si es necesario.

16.8. AUDITORÍA DE SISTEMAS DE CALIDAD DE SOFTWARE

El propósito de la auditoría de un Sistema de Calidad, o un programa de evaluación de la calidad, es suministrar una valoración independiente sobre la conformidad de un Plan de Aseguramiento de la Calidad del Software.

Específicamente el objetivo es determinar, basándose en evidencias observables y verificables, que:

1. La documentación del programa de calidad del software establecida por la organización de desarrollo recoge como mínimo los elementos básicos del estándar ANSI/IEEE 730 u otro estándar apropiado.
2. La organización de desarrollo del software sigue el programa de calidad de software por ellos documentado.

El Plan de Aseguramiento de la Calidad del Software debe incorporar todos los objetivos y los criterios de actuación organizativos; estándares internos y procedimientos; procesos requeridos por la legislación, contratos u otras políticas; conformidad con el estándar ANSI/IEEE 730 u otro estándar apropiado para el aseguramiento de la calidad del software.

16.9. PROCESO DE ASEGURAMIENTO DE LA CALIDAD DESCRITO POR ISO 12207

Para realizar cualquier proceso de auditoría, es imprescindible conocer la actividad que se va auditar, por tanto, no debe extrañar al lector que vayamos intercalando descripciones de los procesos de calidad y los de desarrollo a lo largo del texto, en este caso lo que al respecto describe la norma ISO 12207.

La norma ISO/IEC 12207 "Information technology – Software life cycle processes" 1995, no podríamos dejar de citarla en este capítulo, ya que es una importante norma para el proceso de desarrollo del software y para los procesos de calidad.

Estructura de la norma ISO/IEC 12207

En la figura anterior se muestra la estructura de dicha norma en la que vemos los Procesos Primarios del Ciclo de Vida, los de Soporte y los Organizativos. El número que figura antes de cada proceso corresponde al apartado donde se describe el mismo en la norma.

De ella vamos a describir dos de los procesos más relacionados con nuestro tema, como son el Proceso de Aseguramiento de la Calidad y el Proceso de Auditoría, que consideramos que contribuyen a completar una perspectiva más amplia del tema que nos ocupa.

El apartado 6.3 relativo a los Procesos de Aseguramiento de la Calidad dice:

Los Procesos de Aseguramiento de la Calidad sirven para suministrar la seguridad de que durante el ciclo de vida del proyecto los productos y los procesos están de acuerdo con los requerimientos especificados y se adhieren a los planes establecidos. Al ser imparcial, el aseguramiento de la calidad necesita tener libertad organizativa y autoridad de las personas directamente responsables del desarrollo de los productos software o los que realizan los procesos en el proyecto. El aseguramiento de la calidad puede ser interno o externo, dependiendo de si la evidencia de la calidad de los productos o los procesos se va a demostrar a la dirección del suministrador o al cliente. El aseguramiento de la calidad puede hacer uso de los resultados de otros procesos de Soporte, tales como Verificación, Validación, Revisiones Conjuntas, Auditorías y Resolución de Problemas.

Este proceso de aseguramiento de la calidad se compone de las cuatro actividades que describimos a continuación:

16.9.1. Implementación del proceso

Esta actividad tiene las siguientes tareas:

- El proceso de aseguramiento de la calidad debe establecerse adaptado al proyecto. Los objetivos de este proceso de aseguramiento de la calidad serán asegurar que los productos software y los procesos utilizados para conseguir estos productos software cumplen con los requerimientos establecidos y se adaptan a los planes previstos.

- Los procesos de aseguramiento de la calidad deben ser coordinados con los procesos indicados de Verificación, Validación, Revisión Conjunta y Auditoría.

- El plan para dirigir los procesos, actividades y tareas de aseguramiento de la calidad debe ser desarrollado, documentado, implementado y mantenido durante el tiempo de duración del contrato. Este plan deberá incluir lo siguiente:

  a) Estándares de calidad, metodologías, procedimientos, y herramientas para realizar las actividades de aseguramiento de la calidad (o sus referencias a la documentación oficial de la organización).
  b) Procedimientos para la revisión y coordinación del contrato.
  c) Procedimientos para identificar, recoger, cumplimentar, mantener y acceder a los registros de calidad.
  d) Recursos, planes, y responsabilidades para dirigir las actividades de aseguramiento de calidad.
  e) Determinadas actividades y tareas de los procesos de soporte, tales como Verificación, Validación, Revisiones Conjuntas, Auditorías y Resolución de Problemas.

- Las actividades y tareas planificadas de aseguramiento de la calidad deben realizarse. Cuando son detectados problemas o no conformidades con los requerimientos contractuales, deben ser documentados y servir de entrada al Proceso de Resolución de Problemas. Deben prepararse y mantenerse los registros de estas actividades y tareas, su realización, los problemas y su resolución.

- Los registros de las actividades y tareas de aseguramiento de la calidad deben estar disponibles al cliente así como especificados en el contrato.

- Deberá cerciorarse de que las personas responsables de asegurar la concordancia con los requerimientos del contrato tienen la libertad

organizativa, los recursos y la autoridad para permitir evaluaciones objetivas e iniciar, efectuar, resolver y verificar la resolución de problemas.

16.9.2. Aseguramiento del producto

Esta actividad tiene las siguientes tareas:

- Deberá asegurar que aquellos planes requeridos por el contrato están documentados, cumplen con el contrato, son mutuamente consistentes, y están siendo ejecutados como se requiere.
- Deberá asegurar que aquellos productos software y su documentación cumplen con el contrato y están de acuerdo con los planes.
- En la preparación para el suministro de los productos software, deberá asegurarse de que satisfacen completamente los requerimientos contractuales y son aceptables para el cliente.

16.9.3. Aseguramiento del proceso

Esta actividad tiene las siguientes tareas:

- Deberá asegurar los procesos del ciclo de vida del software (suministro, desarrollo, operación, mantenimientos y soporte, incluyendo el aseguramiento de la calidad) empleados para que el proyecto esté de acuerdo con el contrato y se ajuste a los planes.
- Deberá asegurar que las prácticas internas de ingeniería de software, entorno de desarrollo y librerías están de acuerdo con el contrato.
- Deberá asegurar que los requerimientos aplicables del contrato principal son pasados al subcontratista, y que los productos software del subcontratista satisfacen los requerimientos del contrato principal.
- Deberá asegurar que al cliente y a las otras partes se les aporta el soporte y la cooperación requeridos de acuerdo con el contrato, las negociaciones y los planes.
- Deberá asegurar que los productos software y los procesos medidos están de acuerdo con los estándares y procedimientos establecidos.

- Deberá asegurar que el personal técnico asignado tiene el perfil y los conocimientos necesarios para conseguir cumplir los requerimientos del proyecto y que recibe la formación que pudiera necesitar.

16.9.4. Aseguramiento de la calidad de los sistemas

Esta actividad tiene la siguiente tarea:

- Las actividades adicionales de gestión de calidad deberán asegurar su concordancia con la cláusula de ISO 9001 según especifique el contrato.

16.10. PROCESO DE AUDITORÍA DESCRITO POR ISO 12207

El proceso de auditoría sirve para determinar la adherencia con los requerimientos, los planes y el contrato cuando es apropiado. Este proceso puede ser empleado por cualquiera de las dos partes, donde una de ellas (parte auditora) audita los productos software o las actividades de la otra parte (parte auditada).

Este proceso se compone de dos actividades:

16.10.1. Implementación del proceso

Esta actividad tiene las siguientes tareas:

- Las auditorías deben realizarse en determinados hitos, según lo especificado en los planes del proyecto.

- El personal auditor no debe tener ninguna responsabilidad directa en los productos software ni en las actividades que auditan.

- Todos los recursos requeridos para llevar la auditoría deben ser pactados por las partes, éstos incluyen personal de soporte, locales, hardware, software, herramientas y elementos complementarios.

- Las partes deberán ponerse de acuerdo en cada auditoría sobre: agenda; productos software (y resultados de las actividades) a revisar; alcance de la auditoría y procedimientos; y criterios de comienzo y de terminación de la auditoría.

- Los problemas detectados durante la auditoría deben ser registrados y tratados en el Proceso de Resolución de Problemas.

- Después de completar la auditoría, los resultados de ésta deben ser documentados y entregados a la parte auditada, quien deberá acusar recibo a la parte auditora de cualquier problema detectado en la auditoría y en la resolución de problemas planificada.

- Las partes deberán ponerse de acuerdo sobre los resultados de la auditoría y sobre cualquier punto de acción, responsabilidades y criterios de cierre.

16.10.2. Auditoría

Esta actividad tiene la siguiente tarea:

La auditoría deberá ser dirigida para asegurar que:

a) Los productos software codificados (tal como un elemento software) reflejarán lo diseñado en la documentación.

b) Los requerimientos de la revisión de aceptación y de pruebas prescritos por la documentación son adecuados para la aceptación de los productos software.

c) Los datos de prueba cumplen con la especificación.

d) Los productos software fueron sucesivamente probados y alcanzaron sus especificaciones.

e) Los informes de pruebas son correctos y las discrepancias entre los resultados conseguidos y lo esperado han sido resueltas.

f) La documentación del usuario cumple con los estándares tal como se ha especificado.

g) Las actividades han sido llevadas de acuerdo con los requerimientos aplicables, los planes y el contrato.

h) El coste y el cronograma se ajustan a los planes establecidos.

16.11. CONCLUSIONES

Hemos pretendido hacer una semblanza de los aspectos que consideramos más importantes para hacer una Auditoría de Calidad, tratando de soportarlos en diversos estándares y normas que en la mayoría de los casos hemos insertado traduciéndolos directamente de las mismas para no adulterarlos con una posible subjetividad. Con

esto consideramos que nos puede permitir tener una visión más amplia a través de los distintos enfoques que dan dichas normas sobre las Auditorías de Calidad.

Aunque somos conscientes de que el abordar una auditoría sólo con este bagaje no es suficiente. Un buen auditor en Tecnologías de la Información necesita tener una amplia experiencia en las distintas funciones de dicha actividad, estar muy al día en las distintas metodologías, procesos y herramientas que se emplean, de forma que le sea fácil detectar los defectos en los planes, en los productos y en los procesos, así como estar capacitado para poder proponer recomendaciones.

Reconocemos que no es una tarea fácil, pero precisamente por ello es altamente gratificante el alcanzar un éxito que satisfaga los intereses, en muchas ocasiones contrapuestos, de las partes involucradas, consiguiendo de la entidad auditada el reconocimiento de la profesionalidad del auditor al conseguir detectar los problemas existentes y proponer soluciones, y de la parte que promovió la auditoría el conseguir que se pueda conocer en dónde residían los problemas que no permitían alcanzar los objetivos deseables.

Pero debemos recordar que esta actividad no es un arte, sino una técnica, y como tal debe seguirse un orden y un método en el que nada se da por supuesto si no existe una evidencia objetiva que lo acredita. En ese conjunto de evidencias se apoyaran nuestras conclusiones, y de nuestra experiencia y *know how* saldrán las recomendaciones a proponer.

16.12. LECTURAS RECOMENDADAS

Cohen, L. *Inspection Moderators Handbook.* Maynard, M. A: Digital Equipment Corporation, 1991.

Freedman D. P. y Weinberg G. M. *Handbook of Walkthroughs, Inspections, and Technical Reviews, 1990.*

IEIE 1028 "Standard for Software Reviews and Audits".

16.13. CUESTIONES DE REPASO

1. Elabore su propia definición de "calidad".

2. ¿Qué características de la calidad define la norma ISO 9126?

3. Objetivos de las auditorías de la calidad.

4. ¿Qué prerrequisitos se exigen a los técnicos de desarrollo en un proceso de revisión?

5. Resuma las principales fases del proceso de auditoría software.

6. ¿Cómo se incluyen los procesos de auditoría en la norma ISO/IEC 12207?

7. Diferencias entre aseguramiento del producto y aseguramiento del proceso.

8. Elementos a incluir en un plan para el aseguramiento de la calidad.

9. ¿Qué conocimientos se requieren para poder llevar a cabo con éxito una auditoría de la calidad?

10. ¿Cómo explicaría a un director de informática las ventajas de llevar a cabo una auditoría de la calidad?

CAPÍTULO 17

AUDITORÍA DE LA SEGURIDAD

Miguel Ángel Ramos González

17.1. INTRODUCCIÓN

Para muchos la seguridad sigue siendo el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, aunque después se hayan ido ampliando los objetivos.

Ya sabemos que puede haber seguridad sin auditoría, puede existir auditoría de otras áreas, y queda un espacio de encuentro: la auditoría de la seguridad (figura 17.1), y cuya área puede ser mayor o menor según la entidad y el momento.

Figura 17.1. Encuentro entre seguridad y auditoría

Lo cierto es que cada día es mayor la **importancia de la información,** especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la

revelación de la información, y otras incidencias, tienen un impacto mucho mayor que hace unos años: de ahí la necesidad de protecciones adecuadas que se evaluarán o recomendarán en la auditoría de seguridad.

(También es cierto que en muchos casos tan necesario o más que la protección de la información puede ser que las inversiones en sistemas y tecnologías de la información estén alineadas con las estrategias de la entidad, huyendo del enfoque de la tecnología por la tecnología.)

Las áreas que puede abarcar la Auditoría Informática las recogía el autor de este capítulo en su tesis doctoral en 1990, y en líneas generales vienen a coincidir con las expuestas en esta obra.

En realidad, debemos ir hablando más de **Auditoría en Sistemas de Información** que sólo de Auditoría Informática, y no se trata de un juego de palabras sino de una actualización acorde con el nuevo enfoque y las áreas que llega a cubrir, y lejos ya de la denominación en inglés que seguimos viendo en muchos libros y artículos actuales –algunos citados en la bibliografía– EDP Audit, auditoría en proceso electrónico de datos (Electronic Data Processing).

La nueva denominación abarca globalmente los sistemas de información: desde la planificación, el alineamiento con las estrategias de las entidades, hasta los sistemas de información y el aprovechamiento de las tecnologías de la información aportan ventajas competitivas a la entidad, la gestión de los recursos, e incluso la medida de **la rentabilidad** de todo ello, que es quizá el único punto que personalmente temo cuando se nos sugiere a la hora de establecer objetivos de la auditoría.

Algunas entidades tienen detallados sus costes en la contabilidad analítica, pero ¿cómo cuantificar en algunas semanas las ventajas y los beneficios –algunos intangibles y difícilmente cuantificables– si la propia entidad no ha podido hacerlo en toda su existencia?

Como se indica en la figura 17.2, adaptada de la obra de Emilio del Peso y el propio Miguel A. Ramos *Confidencialidad y Seguridad de la Información: La LORTAD y sus aplicaciones socioeconómicas*, la **auditoría viene a ser el control del control.** (Recordemos que LORTAD significa Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal.)

Volviendo a la seguridad, aunque solemos oír varias expresiones como seguridad informática, seguridad de los sistemas y tecnologías de la información, **seguridad –o protección– de la información,** puestos a elegir, y sin llegar a descartar ninguna, nos quedaríamos con la última, ya que los datos y la información son los activos más estratégicos y valiosos relacionados con los sistemas y el uso de las tecnologías de la información.

Figura 17.2. Auditoría como control del control

La expresión seguridad informática, que es la más usada, puede llegar a relacionarse, sólo con los equipos y los entornos técnicos, como si la información en otros soportes y ambientes no requiriera protección, cuando son las propias operaciones de la entidad, el negocio en entidades con ánimo de lucro, lo que requiere protección.

Si no existen suficientes y adecuadas medidas de protección se puede perder información vital, o al menos no estar disponible en el momento requerido (pensemos en diagnósticos de pacientes muy graves o en control de vuelos), las decisiones tomadas pueden ser erróneas, o se pueden incumplir contratos e incluso la propia legislación, lo que puede traducirse en grandes multas en el caso de infracciones graves, o lo que es aún peor: la inmovilización de los archivos prevista en la LORTAD.

Debe evaluarse en la auditoría si los **modelos de seguridad** están en consonancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones, porque no se puede auditar con conceptos, técnicas o recomendaciones de hace algunos años (que en realidad no son tantos).

En cuanto a la **justificación de la auditoría,** que no parece necesaria en una obra de este tipo, sólo decir que tanto la normativa como la auditoría son necesarias: una auditoría no basada en políticas de la entidad auditada (además de las normas para realizar la auditoría) sería subjetiva y hasta peligrosa (aunque en sistemas de información es una situación habitual, que no normal); y la existencia de normativa sin auditoría podría equivaler a la no-existencia de la Guardia Civil de Tráfico, lo que incrementaría los accidentes e iría convirtiendo la circulación en caótica y peligrosa.

La realidad es que no se conocen datos completos y fiables sobre el nivel de protección de las entidades en España respecto a sistemas de información y vendrían bien algunas estadísticas.

En definitiva, como decía un cliente: "No pasan más cosas porque Dios es bueno", y podemos añadir, que no conocemos la mayor parte de las que pasan, porque ya se ocupan las entidades afectadas de que no se difundan.

Volviendo al **control,** los grandes grupos de controles son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación:

- Controles **directivos,** que son los que establecen las bases, como las políticas, o la creación de comités relacionados o de funciones: de administración de seguridad o auditoría de sistemas de información interna.

- Controles **preventivos,** antes del hecho, como la identificación de visitas (seguridad física) o las contraseñas (seguridad lógica).

- Controles **de detección,** como determinadas revisiones de accesos producidos o la detección de incendios.

- Controles **correctivos,** para rectificar errores, negligencias o acciones intencionadas, como la recuperación de un archivo dañado a partir de una copia.

- Controles **de recuperación,** que facilitan la vuelta a la normalidad después de accidentes o contingencias, como puede ser un plan de continuidad adecuado.

Podemos hablar de **Objetivos de Control** respecto a la seguridad, que vienen a ser declaraciones sobre el resultado final deseado o propósito a ser alcanzado mediante las protecciones y los procedimientos de control, objetivos como los recogidos en la *publicación COBIT (Control Objectives for Information and Related Technologies)* de ISACA (Information Systems Audit and Control Association/Foundation).

Cada entidad ha de definir sus propios objetivos de control, en cuanto a seguridad y otras áreas, y crear y mantener un Sistema de Control Interno (funciones, procesos, actividades, dispositivos...) que puedan garantizar que se cumplen los objetivos de control.

Los auditores somos, en cierto modo, los **"ojos y oídos" de la Dirección,** que a menudo no puede, o no debe, o no sabe, cómo realizar las verificaciones o evaluaciones. (En cuanto a los ojos sigue existiendo en algunos sectores la figura clásica del veedor.)

En los informes se recomendará la implantación o refuerzo de controles, y en ocasiones incluso que se considere la supresión de algún control, si resulta redundante o ya no es necesario.

El **sistema de control interno** ha de basarse en las políticas, y se implanta con apoyo de herramientas, si bien encontramos a menudo en las auditorías que lo que existe es más bien la implantación parcial de controles de acceso lógico a través de paquetes o sistemas basada en el criterio de los técnicos, pero no sustentada en normativa, o bien habiendo partido ésta de los propios técnicos, sin aprobaciones de otro nivel.

La realidad es que el control interno no está generalizado en España fuera de los procesos que implican gastos, y especialmente pagos, pero existen otros riesgos tan importantes o más que las pérdidas monetarias directas, relacionados con la gestión adecuada de los recursos informáticos o con la propia protección de la información, que podrían suponer responsabilidades y pérdidas muy importantes para la entidad.

Cuando existe un sistema de control interno adecuado, los procesos de auditoría, especialmente si son periódicos, son revisiones necesarias pero más rápidas, con informes más breves; si el sistema de control interno es débil, la auditoría llevará más tiempo y esfuerzo, su coste será mayor, y las garantías de que se pongan en marcha las recomendaciones son mucho menores; en ocasiones la situación dista tanto de la ideal como la del paciente que se somete a un chequeo después de varios años sin control.

Finalmente, queremos indicar que por la lógica limitación de espacio no ha sido posible detallar más los puntos, ni incluir listas, que en todo caso sin estar referidas a ningún entorno y sector concreto y, por tanto, sin tener pesos, pueden dar resultados dudosos si quien las usa no sabe adaptarlas e interpretar sus resultados.

17.2. ÁREAS QUE PUEDE CUBRIR LA AUDITORÍA DE LA SEGURIDAD

Se incluyen las que con carácter general pueden formar parte de los objetivos de una revisión de la seguridad, si bien ésta puede abarcar sólo parte de ellas si así se ha determinado de antemano.

En una auditoría de otros aspectos –y, por tanto, en otros capítulos de esta misma obra– pueden también surgir revisiones solapadas con la seguridad; así, a la hora de revisar los desarrollos, normalmente se verá si se realizan en un entorno seguro y protegido, y lo mismo a la hora de revisar la explotación, o el área de técnica de sistemas, las redes, la informática de usuario final, las bases de datos... y en general cualquier área, salvo que expresamente se quiera pasar por alto la seguridad y

concentrarse en otros aspectos como pueden ser la gestión, costes, nivel de servicio, cumplimiento de procedimientos generales, calidad, o cualquier otro.

Volviendo a las áreas, las que se citan pueden ser objeto de la auditoría de seguridad, si bien en cada caso se habrán fijado los objetivos que más interesen, no considerando o por lo menos no con el mismo énfasis otros, si bien debiendo quedar claro y por escrito cuáles son esos objetivos, tanto cuando se trate de una auditoría interna como externa, en cuyo caso puede mediar un contrato o al menos una propuesta y carta de aceptación.

Las **áreas** generales citadas, algunas de las cuales se amplían después, son:

- Lo que hemos denominado controles directivos, es decir, los fundamentos de la seguridad: políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como que existen sistemas y métodos de evaluación periódica de riesgos.

- El desarrollo de las políticas: procedimientos, posibles estándares, normas y guías, sin ser suficiente que existan estas últimas.

- Que para los grupos anteriores se ha considerado el marco jurídico aplicable, aspecto tratado en otros capítulos de esta obra, así como las regulaciones o los requerimientos aplicables a cada entidad: del Banco de España en el caso de las entidades financieras, del sector del seguro, los de la Comunidad Autónoma correspondiente, tal vez de su Ayuntamiento, o de la casa matriz las multinacionales o que formen parte de un grupo. Otro aspecto es el cumplimiento de los contratos.

- Amenazas físicas externas: inundaciones, incendios, explosiones, corte de líneas o de suministros, terremotos, terrorismo, huelgas...

- Control de accesos adecuado, tanto físicos como los denominados lógicos, para que cada usuario pueda acceder a los recursos a que esté autorizado y realizar sólo las funciones permitidas: lectura, variación, ejecución, borrado, copia... y quedando las pistas necesarias para control y auditoría, tanto de accesos producidos al menos a los recursos más críticos como los intentos en determinados casos.

- Protección de datos: lo que fije la LOPD en cuanto a los datos de carácter personal bajo tratamiento automatizado, y otros controles en cuanto a los datos en general, según la clasificación que exista, la designación de *propietarios* y los riesgos a que estén sometidos.

- Comunicaciones y redes: topología y tipo de comunicaciones, posible uso de cifrado, protecciones ante virus, éstas también en sistemas aislados aunque el impacto será menor que en una red.

- El entorno de Producción, entendiendo como tal Explotación más Técnica de Sistemas, y con especial énfasis en el cumplimiento de contratos en lo que se refiera a protecciones, tanto respecto a terceros cuando se trata de una entidad que presta servicios, como el servicio recibido de otros, y de forma especial en el caso de la subcontratación total o *outsourcing*.

- El desarrollo de aplicaciones en un entorno seguro, y que se incorporen controles en los productos desarrollados y que éstos resulten auditables.

- La continuidad de las operaciones.

No se trata de áreas no relacionadas, sino que **casi todas tienen puntos de enlace y partes comunes:** comunicaciones con control de accesos, cifrado con comunicaciones y soportes, datos con soportes y con comunicaciones, explotación con varias de ellas, y así en otros casos.

17.3. EVALUACIÓN DE RIESGOS

Se trata de identificar los riesgos, cuantificar su **probabilidad** e **impacto,** y analizar medidas que los eliminen –lo que generalmente no es posible– o que disminuyan la probabilidad de que ocurran los hechos o mitiguen el impacto.

Para evaluar riesgos hay que considerar, entre otros factores, el tipo de información almacenada, procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal aplicable, el sector de la entidad, la entidad misma y el momento.

Para ello los auditores disponemos de listas, que normalmente incluimos en hojas de cálculo, o bien usamos paquetes, y tal vez en el futuro sistemas exentos. El problema sigue siendo la adaptación de los puntos a cada caso, y asignar el **peso** que puede tener cada uno de los puntos.

Desde la perspectiva de la auditoría de la seguridad es necesario revisar si se han considerado las **amenazas,** o bien evaluarlas si es el objetivo, y de todo tipo: errores y negligencias en general, desastres naturales, fallos de instalaciones, o bien fraudes o delitos, y que pueden traducirse en daños a: personas, datos, programas, redes, instalaciones, u otros activos, y llegar a suponer un peor servicio a usuarios internos y externos éstos normalmente clientes, imagen degradada u otros difícilmente

cuantificables, e incluso pérdida irreversible de datos, y hasta el fin de la actividad de la entidad en los casos más graves.

Para ello es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles, que serán los que preferentemente intentarán usar quienes quieran acceder de forma no autorizada.

Debemos pensar que las medidas deben considerarse como **inversiones en seguridad,** aunque en algunos casos se nos ha dicho que no es fácil reflejarlas como activos contables ni saber cuál es su **rentabilidad;** podemos estar de acuerdo, pero ¿cuál es la rentabilidad de blindar la puerta de acceso a nuestro domicilio o la de instalar un antirrobo en nuestro automóvil? Esa rentabilidad la podemos determinar si los dispositivos o controles han servido para evitar la agresión, y a veces habrá constituido simplemente una medida disuasorio, sobre todo en seguridad lógica, y no llegaremos a conocer su efecto positivo.

En todo caso debemos transmitir a los auditados que, además, la seguridad tiene un impacto favorable en la imagen de las entidades (aunque esto sólo no suela justificar las inversiones), y tanto para clientes y posibles como para los empleados. Unos y otros pueden sentirse más protegidos, así como sus activos.

La protección no ha de basarse sólo en dispositivos y medios físicos, sino en formación e información adecuada al personal, empezando por la mentalización a los directivos para que, en cascada, afecte a todos los niveles de la pirámide organizativa.

El **factor humano** es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados, ya que es muy crítico: si las personas no quieren colaborar de poco sirven los medios y dispositivos aunque sean caros y sofisticados.

Además, es conveniente que haya cláusulas adecuadas en los contratos, sean de trabajo o de otro tipo, especialmente para quienes están en funciones más críticas.

Es necesaria una separación de funciones: es peligroso que una misma persona realice una transacción, la autorice, y revise después los resultados (un diario de operaciones, por ejemplo), porque podría planificar un fraude o encubrir cualquier anomalía, y sobre todo equivocarse y no detectarse; por ello deben intervenir funciones/personas diferentes y existir controles suficientes.

En un proceso de auditoría, por tanto, se evaluarán todos estos aspectos y otros, por ejemplo si la seguridad es realmente una preocupación corporativa no es suficiente que exista presupuesto para ello; si las personas a diferentes niveles están mentalizadas, pues es necesaria una **cultura de la seguridad;** y si hay un comité que

fije o apruebe los objetivos correspondientes y en qué medida se alcanzan, qué modelo de seguridad se quiere implantar o se ha implantado, qué políticas y procedimientos existen: su idoneidad y grado de cumplimiento, así como la forma en que se realiza el desarrollo de aplicaciones, si el proceso se lleva a cabo igualmente en un entorno seguro con separación de programas y separación en cuanto a datos, si los seguros cubren los riesgos residuales, y si está prevista la continuidad de las operaciones en el caso de incidencias.

Una vez identificados y medidos los **riesgos,** lo mejor sería poder **eliminarlos,** pero ya hemos indicado que normalmente lo más que conseguimos es **disminuir** la probabilidad de que algo se produzca o bien su impacto: con sistemas de detección, de extinción, mediante revisiones periódicas, copiando archivos críticos, exigiendo una contraseña u otros controles según los casos.

Algunos manuales hablan de **transferir los riesgos,** por ejemplo contratando un seguro pero debemos recordar que si se pierden los datos la entidad aseguradora abonara el importe estipulado –si no puede acogerse a alguna cláusula en letra pequeña– pero la entidad seguirá sin recuperar los datos.

Otra posibilidad es **asumir los riesgos,** pero debe hacerse a un nivel adecuado en la entidad, y considerando que puede ser mucho mayor el coste de la inseguridad que el de la seguridad, lo que a veces sólo se sabe cuando ha ocurrido algo. ¿Cuál es el riesgo máximo admisible que puede permitirse una entidad? Alguna vez se nos ha hecho la pregunta, y depende de lo crítica que sea para la entidad la información así como disponer de ella, e incluso puede depender del momento: es un tema tan crítico que no puede generalizarse.

Algunos de los riesgos se han podido asumir de forma temporal, por estar en proceso de cambio las plataformas, las aplicaciones o las instalaciones, o por no existir presupuesto ante las grandes inversiones necesarias; en todos los casos debe constar por escrito que se asumen y quién lo hace, y ha de ser alguien con potestad para hacerlo, ya que a menudo son técnicos intermedios quienes asumen la responsabilidad sin poder hacerlo, o bien los directivos señalan a los técnicos cuando ocurre algo sin querer asumir ninguna responsabilidad.

Si la entidad auditada está en medio de un proceso de implantación de la seguridad, la evaluación se centrará en los objetivos, los planes, qué proyectos hay en curso y los medios usados o previstos.

La evaluación de riesgos puede ser global: todos los sistemas de información, centros y plataformas, que puede equivaler a un chequeo médico general de un individuo, y que es habitual la primera vez que se realiza, o bien cuando se ha producido el nombramiento de algún responsable relacionado, o cuando una entidad compra otra, pero puede producirse también una evaluación parcial de riesgos, tanto

por áreas como por centros, departamentos, redes o aplicaciones, así como previa a un proyecto, como puede ser una aplicación a iniciar.

A menudo en la auditoría externa se trata de saber si la entidad, a través de funciones como administración de la seguridad, auditoría interna, u otras si las anteriores no existieran, ha evaluado de forma adecuada los riesgos, si los informes han llegado a los destinatarios correspondientes y si se están tomando las medidas pertinentes, así como si el proceso se realiza con la frecuencia necesaria y no ha constituido un hecho aislado.

En estos casos se debe considerar la **metodología** que se sigue para evaluar los riesgos más que las **herramientas,** aunque sin dejar de analizar éstas, y si se han considerado todos los riesgos –al menos los más importantes– y si se han medido bien, ya que sobre todo cuando la evaluación se hace de forma interna por técnicos del área de sistemas de información, suelen minimizar los riesgos porque llevan años conviviendo con ellos o simplemente los desconocen.

La seguridad no es, un tema meramente técnico, aunque sean muy técnicas algunas de las medidas que haya que implantar.

Es necesaria la designación de **propietarios** de los activos, sobre todo los datos (por delegación de los titulares), y que son quienes pueden realizar la clasificación y autorizar las reglas de acceso; un buen propietario se interesará por los riesgos que puedan existir, por lo que promoverá o exigirá la realización de auditorías y querrá conocer, en términos no técnicos, la sustancia de los informes.

Al hablar de seguridad siempre se habla de sus tres dimensiones clásicas: confidencialidad, integridad y disponibilidad de la información, y algunos controles van más dirigidos a tratar de garantizar alguna de estas características.

La **confidencialidad:** se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos de los clientes o empleados de una entidad fuera cedido a terceros?, ¿cuál podría ser su uso final?, ¿habría una cadena de cesiones o ventas incontroladas de esos datos?

La LORTAD y la LOPD han influido positivamente en concienciarnos respecto a la confidencialidad.

La **integridad:** consiste en que sólo los usuarios autorizados puedan variar (modificar o borrar) los datos. Deben quedar pistas para control posterior y para auditoría.

Pensemos que alguien introdujera variaciones de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara de forma aleatoria parte de los domicilios de algunos clientes.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían "viciadas" (corruptas decimos a veces), lo que haría difícil la reconstrucción.

La **disponibilidad:** se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que estén autorizadas.

El disponer de la información después del momento necesario puede equivaler a la falta de disponibilidad. Otro tema es disponer de la información a tiempo sin que ésta sea correcta, e incluso sin saberse, lo que puede originar la toma de decisiones, erróneas.

Más grave aún puede ser la ausencia de disponibilidad absoluta por haberse producido algún desastre. En ese caso, a medida que pasa el tiempo el impacto será mayor, hasta llegar a suponer la falta de continuidad de la entidad como ha pasado en muchos de los casos producidos (más de un 80% según las estadísticas).

Debe existir además **autenticidad:** que los datos o información sean auténticos, introducidos o comunicados por usuarios auténticos y con las autorizaciones necesarias.

17.4. FASES DE LA AUDITORÍA DE SEGURIDAD

Con carácter general pueden ser:

- Concreción de los objetivos y delimitación del alcance y profundidad de la auditoría, así como del período cubierto en su caso, por ejemplo revisión de accesos del último trimestre; si no se especifica, los auditores deberán citar en el informe el período revisado, porque podría aparecer alguna anomalía anterior, incluso de hace mucho tiempo, y llegarse a considerar una debilidad de la auditoría.

- Análisis de posibles fuentes y recopilación de información: en el caso de los internos este proceso puede no existir.

- Determinación del plan de trabajo y de los recursos y plazos en caso necesario, así como de comunicación a la entidad.
- Adaptación de cuestionarios, y a veces consideración de herramientas o perfiles de especialistas necesarios, sobre todo en la auditoría externa.
- Realización de entrevistas y pruebas.
- Análisis de resultados y valoración de riesgos.
- Presentación y discusión del informe provisional.
- Informe definitivo.

17.5. AUDITORÍA DE LA SEGURIDAD FÍSICA

Se evaluarán las protecciones físicas de datos, programas, instalaciones, equipos, redes y soportes, y por supuesto habrá que considerar a las personas: que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector, por ejemplo por convenio o normativa específica; y si bien todos estos aspectos suelen ser comunes con las medidas generales de la entidad, en una auditoría de sistemas de información nos preocupamos especialmente por quienes están en el área o de los daños que puedan afectar a los usuarios de los sistemas si entra dentro dé la auditoría.

Las **amenazas** pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones.

(Hay algo más que no recogemos en los informes, pero convencidos de que se trata de una amenaza real sí lo comentamos verbalmente a veces en la presentación del informe o en cursos a sabiendas de que produce comentarios: la lotería; si toca en un área un premio importante, juegan todos el mismo número, y no existen sustitutos o no hay una documentación adecuada –pensemos en un grupo que mantiene una aplicación– se puede originar un problema importante, y la, prevención no es fácil porque no se puede impedir el hecho.)

Desde la perspectiva de las **protecciones físicas** algunos aspectos a considerar son:

- Ubicación del centro de procesos, de los servidores locales, y en general de cualquier elemento a proteger, como puedan ser los propios terminales, especialmente en zonas de paso, de acceso público, o próximos a ventanas en plantas bajas. Protección de computadores portátiles, incluso fuera de las oficinas: aeropuertos, automóviles, restaurantes...

- Estructura, diseño, construcción y distribución de los edificios y de sus plantas.

- Riesgos a los que están expuestos, tanto por agentes externos, casuales o no, como por accesos físicos no controlados.

- Amenazas de fuego (materiales empleados); riesgos por agua: por accidentes atmosféricos o por averías en las conducciones; problemas en el suministro eléctrico, tanto por caídas como por perturbaciones.

- Controles tanto preventivos como de detección relacionados con los puntos anteriores, así como de acceso basándose en la clasificación de áreas según usuarios, incluso según día de la semana y horario.

- Además del acceso, en determinados edificios o áreas debe controlarse el contenido de carteras, paquetes, bolsos o cajas, ya que podrían contener explosivos, así como lo que se quiere sacar del edificio, para evitar sustituciones o sustracción de equipos, componentes, soportes magnéticos, documentación u otros activos.

  El control deberá afectar a las visitas, proveedores, contratados, clientes... y en casos más estrictos igualmente a los empleados; los ex empleados se deberán considerar visitas en todo caso.

- Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no físicas, todo bajo un sistema de inventario, así como protección de documentos impresos y de cualquier tipo de documentación clasificada.

  Es fácil y barato obtener copias magnéticas periódicas de datos y de programas frente al perjuicio que nos puede causar el no haberlo hecho; es mucho más difícil o caro, o no es posible, obtener copias con igual valor de otros objetos o activos como obras de arte.

Todos los puntos anteriores pueden, además, estar cubiertos por seguros.

17.6. AUDITORÍA DE LA SEGURIDAD LÓGICA

Es necesario verificar que cada usuario sólo pueda acceder a los recursos a los que le autorice el propietario, aunque sea de forma genérica, según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución... trasladando a los sistemas lo que representaríamos en una **matriz de accesos** en la que figuraran los **sujetos:** grupos de usuarios o sistemas, los **objetos** que puedan ser accedidos con mayor o menor **granularidad:** un disco, una aplicación, una base de datos, una librería de programas, un tipo de transacción, un programa, un tipo de campo... y para completar la tripleta, las posibilidades que se le otorgan: lectura, modificación, borrado, ejecución...

Desde el punto de vista de la auditoría es necesario revisar cómo se identifican y sobre todo autentican los usuarios, cómo han sido autorizados y por quién, y qué ocurre cuando se producen transgresiones o intentos: quién se entera y cuándo y qué se hace.

En cuanto a autenticación, hasta tanto no se abaraten más y generalicen los sistemas basados en la **biométrica,** el método más usado es la **contraseña,** cuyas características serán acordes con las normas y estándares de la entidad, que podrían contemplar diferencias para según qué sistemas en función de la criticidad de los recursos accedidos.

Algunos de los aspectos a evaluar respecto a las **contraseñas** pueden ser:

- Quién asigna la contraseña: inicial y sucesivas.
- Longitud mínima y composición de caracteres.
- Vigencia, incluso puede haberlas de un solo uso o dependientes de una función tiempo.
- Control para no asignar las "x" últimas.
- Número de intentos que se permiten al usuario, e investigación posterior de los fallidos: pueden ser errores del usuario o intentos de suplantación.
- Si las contraseñas están cifradas y bajo qué sistema, y sobre todo que no aparezcan en claro en las pantallas, listados, mensajes de comunicaciones o corrientes de trabajos (JCL en algunos sistemas).
- Protección o cambio de las contraseñas iniciales que llegan en los sistemas, y que a menudo aparecen en los propios manuales.

- Controles existentes para evitar y detectar caballos de Troya: en este contexto se trata de un programa residente en un *PC* que emulando un terminal simule el contenido de la pantalla que recoge la identificación y contraseña del usuario, grabe la contraseña y devuelva control al sistema verdadero después de algún mensaje simulado de error que normalmente no despertará las sospechas del usuario.

- La no-cesión, y el uso individual y responsable de cada usuario, a partir de la normativa.

Siempre se ha dicho que la contraseña ha de ser difícilmente imaginable por ajenos y fácilmente recordable por el propio usuario, y este último aspecto se pone en peligro cuando un mismo usuario ha de identificarse ante distintos sistemas, para lo que puede asignar una misma contraseña, lo que supone una vulnerabilidad si la protección es desigual, por ser habitual que en pequeños sistemas o aplicaciones aisladas las contraseñas no están cifradas o lo estén bajo sistemas vulnerables; si opta por asignar varias contraseñas puede que necesite anotarlas.

La solución más adecuada por ahora puede consistir en utilizar **sistemas de identificación únicos** ***(single sign-on)*** que faciliten la administración y el acceso, permitiéndolo o no a según qué usuarios/sistemas/funciones, o bien adoptar cualquier otro tipo de solución que, con garantías suficientes, pueda propagar la contraseña entre sistemas.

En la auditoría debemos verificar que el proceso de altas de usuarios se realiza según la normativa en vigor, y que las autorizaciones requeridas son adecuadas, así como la gestión posterior como variaciones y bajas, y que los usuarios activos siguen vigentes, y si se revisa cuáles son inactivos y por qué, por ejemplo contrastando periódicamente con la base de datos de empleados y contratados. Debiera estar previsto bloquear a un usuario que no accediera en un período determinado, ¿35 días?

Otra posible debilidad que debe considerarse en la auditoría es si pueden crearse **situaciones de bloqueo** porque sólo exista un administrador, que puede estar ausente de forma no prevista, por ejemplo por haber sufrido un accidente, e impedir la creación nuevos usuarios en un sistema de administración centralizada y única; en más de una ocasión, según de qué entorno se trate hemos recomendado la existencia de algún usuario no asignado con perfil especial y contraseña protegida que pueda utilizar alguien con autoridad en caso de emergencia: todas sus operaciones deberán quedar registradas para control y auditoría.

17.7. AUDITORÍA DE LA SEGURIDAD Y EL DESARROLLO DE APLICACIONES

Todos los desarrollos deben estar autorizados a distinto nivel según la importancia del desarrollo a abordar, incluso autorizados por un comité si los costes o los riesgos superan unos umbrales; se revisará la participación de usuarios, y de los auditores internos si la auditoría es externa, a qué librerías pueden acceder los desarrolladores, si hay separación suficiente de entornos, la metodología seguida, ciclos de vida, gestión de los proyectos, consideraciones especiales respecto a aplicaciones que traten datos clasificados o que tengan transacciones económicas o de riesgo especial, términos de los contratos y cumplimiento, selección y uso de paquetes, realización de pruebas a distintos niveles y mantenimiento posterior, así como desarrollos de usuarios finales.

El pase al entorno de explotación real debe estar controlado, no descartándose la **revisión de programas** por parte de técnicos independientes, o bien por auditores preparados, a fin de determinar la ausencia de "caballos de Troya", bombas lógicas y similares, además de la calidad.

Otro aspecto es la **protección de los programas,** al menos desde dos perspectivas: de los programas, que sean propiedad de la entidad, realizados por el personal propio o contratado su desarrollo a terceros, como el uso adecuado de aquellos programas de los que se tenga licencia de uso.

17.8. AUDITORÍA DE LA SEGURIDAD EN EL ÁREA DE PRODUCCIÓN

Las entidades han de cuidar especialmente las medidas de protección en el caso de **contratación** de servicios: desde el posible marcado de datos, proceso, impresión de etiquetas, distribución, acciones comerciales, gestión de cobros, hasta el *outsourcing* más completo, sin descartar que en el contrato se prevea la revisión por los auditores, internos o externos, de las instalaciones de la entidad que provee el servicio.

También debe revisarse la protección de **utilidades** o programas especialmente peligrosos, así como el control en generación y cambios posteriores de todo el software de sistemas, y de forma especial el de control de accesos.

Otro aspecto a revisar es el control de los formularios críticos.

La gestión de problemas y cambios y la calidad son aspectos que también tienen que ver con la seguridad.

17.9. AUDITORÍA DE LA SEGURIDAD DE LOS DATOS

Es un aspecto que puede entenderse dentro de la Producción y las Comunicaciones, pero que merece ser tratado de forma específica. Decíamos que los datos y la información pueden llegar a constituir el activo más crítico para la entidad, hasta el punto de que en muchas multinacionales la función genérica de administración de seguridad tiene la denominación de Data Security.

Los datos, además de alfanuméricos, pueden consistir en imágenes de planos, en otros diseños u objetos, gráficos, acústicos, y otros, y estar almacenados en medios y soportes diversos.

La protección de los datos puede tener varios enfoques respecto a las características: la confidencialidad, disponibilidad e integridad. Puede haber datos **críticos en cuanto a su confidencialidad**, como datos médicos u otros especialmente sensibles para la LOPD (sobre religión, sexo, raza...), otros datos cuya criticidad viene dada **por la disponibilidad**: si se pierden o no se pueden utilizar a tiempo pueden causar perjuicios graves y, en los casos más extremos poner en peligro la continuidad de la entidad, y finalmente otros datos críticos **atendiendo a su integridad**, especialmente cuando su pérdida no puede detectarse fácilmente o una vez detectada no es fácil reconstruirlos.

Aunque los libros no suelen citarlo así, nos gusta hablar de controles en los diferentes puntos del **ciclo de vida de los datos,** que es lo que ha de revisarse en la auditoría:

- Desde el origen del dato, que puede ser dentro o fuera de la entidad, y puede incluir preparación, autorización, incorporación al sistema: por el cliente, por empleados, o bien ser captado de otra forma, y debe revisarse cómo se verifican los errores.

- Proceso de los datos: controles de validación, integridad, almacenamiento: que existan copias suficientes, sincronizadas y protegidas.

- Salida de resultados: controles en transmisiones, en impresión, en distribución, *en servicios contratados de manipulación y en el envío; conciliación previa de* salidas con entradas, por personas *diferentes, para detectar errores y posibles* intentos de fraude.

- Retención de la información y protección en función de su clasificación: destrucción de los diferentes soportes que la contengan cuando ya no sea necesaria, o bien desmagnetización.

Es necesaria la **designación de propietarios,** clasificación de los datos, restricción de su uso para pruebas, inclusión de **muescas** para poder detectar usos no autorizados, así como aprovechar las posibilidades de protección, control y auditoría del Sistema de Gestión de Bases de Datos que se esté utilizando.

En cuanto a la **clasificación** de datos e información debe revisarse quién la ha realizado y según qué criterios y estándares; no suele ser práctico que haya más de cuatro o cinco niveles. En ocasiones la denominación sin clasificar se aplica tanto a los datos que no requieren protección –en ocasiones incluso conviene divulgarlos– cómo a los que están pendientes de clasificar, por lo que es necesario diferenciar las dos situaciones. También es conveniente que se distinga por categorías, asociadas a áreas funcionales o proyectos.

Aquellos soportes que contengan datos o información de los niveles más críticos estarán especialmente protegidos, incluso cifrados. Entre esos soportes pueden estar: magnéticos, papel, comunicaciones, correo electrónico, fax, e incluso voz.

En algunas entidades tienen etiquetas o carátulas para diferenciar soportes, listados, y documentos cuyo contenido está especialmente clasificado, lo que en ocasiones puede llegar a alertar incluso a distancia a quienes no estén autorizados.

Respecto a **cliente-servidor** es necesario verificar los controles en varios puntos, y no sólo en uno central como en otros sistemas, y a veces en plataformas heterogéneas, con niveles y características de seguridad muy diferentes, y con posibilidad de transferencia de archivos o de captación y exportación de datos que pueden perder sus protecciones al pasar de una plataforma a otra.

En el caso del contenido de archivos y bases de datos, las etiquetas debieran acompañarles incluso en extracciones parciales que variaran de plataforma, lo que en la actualidad no está plenamente conseguido en todos los casos cuando en las redes intervienen plataformas y sistemas que no se entienden bien entre sí en cuanto a seguridad; aunque en este momento hay intentos de cierta normalización y van apareciendo herramientas que van permitiendo la protección en entornos heterogéneos.

También pueden usarse bases de datos distribuidas, lo que puede añadir complejidad al sistema y a los controles a establecer.

La información del nivel más alto de clasificación normalmente se entregará (o dejará ver) bajo controles estrictos, incluso anotando qué se entregó o enseñó, a quiénes, cuándo, y con la autorización de quién si este extremo es necesario.

En la auditoría, si entra en los objetivos, se analizará la destrucción de la información clasificada: tipo de destructora, tamaño de las partículas, y especialmente dónde se almacena hasta su destrucción, que suele ser un punto débil.

En el caso de soportes magnéticos éstos habrán de ser destruidos, desmagnetizados de forma adecuada, o sometidos a varias grabaciones diferentes antes de su nueva utilización.

En una ocasión hemos recomendado en una auditoría que las copias que recibieran distintos directivos no fueran idénticas –sin afectar a su contenido sustancial– a fin de poder detectar el origen de fugas o copias, que al parecer se sospechaba que se venían produciendo.

En el caso de ser necesario el transporte de datos clasificados debe realizarse por canales seguros, y si es en soporte magnético o por transmisión deben ir cifrados, además de la posibilidad de transportar soportes magnéticos en compartimentos cerrados y que la llave no esté en poder de los transportistas o esté protegida.

17.10. AUDITORÍA DE LA SEGURIDAD EN COMUNICACIONES Y REDES

En las políticas de la entidad debe reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la entidad y no deben usarse para otros fines no autorizados, por seguridad y por productividad, tal vez salvo emergencias concretas si así se ha especificado, y más bien para comunicaciones por voz.

En función de la clasificación de los datos se habrá previsto el uso de **cifrado**, que en la auditoría se evaluará o se llegará a recomendar, y se revisarán la generacion, longitud, comunicación, almacenamiento y vigencia de las claves, especialmente de las maestras.

Cada usuario sólo debe recibir en el menú lo que pueda seleccionar realmente.

Los usuarios tendrán restricción de accesos según dominios, únicamente podrán cargar los programas autorizados, y sólo podrán variar las configuraciones y componentes los técnicos autorizados.

Deberán existir protecciones de distinto tipo, y tanto preventivas como de detección, ante posibles accesos sobre todo externos, así como frente a virus por diferentes vías de infección, incluyendo el correo electrónico.

Se revisarán especialmente las redes cuando existan repercusiones económicas porque se trate de transferencia de fondos o comercio electrónico.

Algunos de los puntos complementarios a revisar son:

- Tipos de redes y conexiones.
- Información y programas transmitidos, y uso de cifrado.
- Tipos de transacciones.
- Tipos de terminales y protecciones: físicas, lógicas, llamada de retorno.
- Protección de transmisiones por fax si el contenido está clasificado, si bien es preferible evitar el uso de este medio en ese caso.
- Protección de conversaciones de voz en caso necesario.
- Transferencia de archivos y controles existentes.
- Consideración especial respecto a las conexiones externas a través de pasarelas *(gateway)* y encaminadores *(routers)*, así como qué controles existen.
- Ante la generalización de modalidades avanzadas de proceso, empiezan a preocupar y a ser objeto de auditoría aspectos como:

  Internet e Intranet: separación de dominios e implantación de medidas especiales, como normas y cortafuegos *(firewall)*, y no sólo en relación con la seguridad sino por accesos no justificados por la función desempeñada, como a páginas de ocio o eróticas, por lo que pueden suponer para la productividad.

  El **correo electrónico,** tanto por privacidad (PGP, Pretty Good Privacy se está usando mucho) y para evitar virus como para que el uso del correo sea adecuado y referido a la propia función, y no utilizado para fines particulares, como se ha intentado hacer en muchas entidades y no siempre con éxito, con otros recursos anteriores como teléfono, fax, fotocopiadoras, o el uso de los propios computadores.

  Otro de los aspectos que preocupan es la **protección de programas,** y tanto la prevención del uso no autorizado de programas propiedad de la entidad o de los que tengan licencia de uso, como la carga o transmisión de otros de los que no se tenga licencia o simplemente para los que no exista autorización interna.

También preocupa el **control sobre las páginas web**: quién puede modificarlo y desde dónde, porque se han dado casos desagradables en alguna entidad que impactan muy negativamente en su imagen, y no tanto por los que lo ven directamente, sino por la publicidad que en los medios se puede dar a estos hechos. Finalmente preocupan también los riesgos que puedan existir en el **comercio electrónico,** aunque se están empezando a utilizar sistemas fiables como SET (Secure Electronic Transaction).

En relación con todo ello, y para facilitar el control y la auditoría, es necesario que queden registrados los accesos realizados a redes exteriores y protegidos esos registros, así como la fecha y hora y el usuario o sistema, y el tipo de información transferida y en qué sentido.

17.11. AUDITORÍA DE LA CONTINUIDAD DE LAS OPERACIONES

Es uno de los puntos que nunca se deberían pasar por alto en una auditoría de seguridad, por las consecuencias que puede tener el no haberlo revisado o haberlo hecho sin la suficiente profundidad: no basta con ver un manual cuyo título sea Plan de Contingencia o denominación similar, sino que es imprescindible conocer si funcionaría con las garantías necesarias y cubriría los requerimientos en un tiempo inferior al fijado y, con una duración suficiente.

Hablamos de **Plan de Contingencia o Plan de Continuidad**, frente a otras denominaciones que en principio descartamos como Recuperación de Desastres o Plan de Desastres (sí nos parece adecuada Plan de Recuperación ante Desastres, pero las incidencias a prever son también de otros niveles).

En la auditoría es necesario **revisar** si existe tal plan, si es completo y actualizado, si los diferentes procesos, áreas y plataformas, o bien si existen planes diferentes según entornos, evaluar en todo caso su idoneidad, así como los resultados de las pruebas que se hayan realizado, y si permite garantizar razonablemente que en caso necesario, y a través de los medios alternativos, propios o contratados, podría permitir la reanudación de las operaciones en un tiempo inferior al fijado por los responsables del uso de las aplicaciones, que a veces son también los propietarios de las mismas pero podrían no serlo.

Si las revisiones no nos aportan garantías suficientes debemos sugerir pruebas complementarias o hacerlo constar en el informe, incluso indicarlo en el apartado de limitaciones.

Es necesario verificar que la solución adoptada es adecuada: centro propio, ajeno, compartido o no... y que existe el oportuno contrato si hay participación de otras entidades aunque sean del mismo grupo o sector. No está de más revisar si en el caso de una incidencia que afectara a varias entidades geográficamente próximas la solución prevista daría el servicio previsto a la auditada.

Un punto fundamental en la revisión es la existencia de **copias actualizadas** de los **recursos vitales** en un lugar distante y en condiciones adecuadas tanto físicas como de protección en cuanto a accesos; entre dichos recursos estarán: bases de datos y archivos, programas (mejor si existen también en versión fuente), JCL (Job Control Language) o el equivalente en cada sistema, la documentación necesaria, formularios críticos y consumibles –o garantías de que se servirían a tiempo–, documentación, manuales técnicos, direcciones y teléfonos, los recursos de comunicaciones necesarios: datos y voz, y cualesquiera otros requeridos para funcionar con garantías.

Otros aspectos que hemos encontrado como **debilidades** a veces son: que exista copia del propio plan fuera de las instalaciones primarias, que esté previsto ejecutar determinado software en un equipo alternativo, con identificación específica diferente de la del equipo primario que es el inicialmente autorizado; y que se tenga copia accesible del contrato, tanto para demostrar algo al proveedor como para verificar los términos pactados.

Dentro de la **criticidad de las aplicaciones** se puede distinguir entre las más críticas, con impacto muy alto en el negocio y sin alternativa, otras con alternativas, e incluso diferenciando si con costes altos o inferiores, y aquellas cuya interrupción, al menos en un número de días fijado, no tiene casi incidencia, y habrá que distinguir qué tipos de consecuencias e impacto, en función del sector y entidad, y día del mes en que ocurriera el incidente, y tal vez la hora en algunos casos.

Frente a lo que venía siendo la previsión de contingencias en estos años pasados, centrándose sólo en el host como gran servidor, hoy en día, con la clara tendencia a **entornos distribuidos,** es necesario considerar también éstos en la previsión de las contingencias.

Es necesario en la auditoría conocer las características del centro o sistema alternativo, y debe revisarse si la capacidad de proceso, la de comunicación y la de almacenamiento del sistema alternativo son suficientes, así como las medidas de protección.

Debe existir un manual completo y exhaustivo relacionado con la continuidad en el que se contemplen diferentes tipos de incidencias y a qué nivel se puede decidir que se trata de una contingencia y de qué tipo.

A pesar de la importancia del tema y de las consecuencias nefastas que se pueden derivar si no se han previsto las contingencias, es un tema no exigido por ley en España, si bien parece sobradamente justificada su existencia para defender los intereses de los accionistas, clientes, proveedores, empleados, o ciudadanos en general según qué tipo de entidad sea; en algún caso se nos ha preguntado al incluirlo en el informe como una recomendación, ¿pero qué me obliga a tener el plan? Afortunadamente es un punto fácil de explicar y que la Alta Dirección suele entender y aceptar.

17.12. FUENTES DE LA AUDITORÍA

Las fuentes estarán relacionadas con los objetivos, y entre ellas pueden estar:

- Políticas, estándares, normas y procedimientos.
- Planes de seguridad.
- Contratos, pólizas de seguros.
- Organigrama y descripción de funciones.
- Documentación de aplicaciones.
- Descripción de dispositivos relacionados con la seguridad.
- Manuales técnicos de sistemas operativos o de herramientas.
- Inventarios: de soportes, de aplicaciones.
- Topología de redes.
- Planos de instalaciones.
- Registros: de problemas, de cambios, de visitas, de accesos lógicos producidos.
- Entrevistas a diferentes niveles.
- Archivos.
- Programas.
- La observación: no figura en los manuales pero la consideramos importante.
- Actas de reuniones relacionadas.
- Documentación de planes de continuidad y sus pruebas.
- Informes de suministradores o consultores.

A menudo los clientes nos ofrecen a los auditores externos los informes de los internos o de otros externos anteriores, si bien nosotros en concreto preferimos utilizarlos cuando ya está en vías el borrador de nuestro informe para no vernos influidos.

17.13. EL PERFIL DEL AUDITOR

El perfil que se requiere para llevar a cabo auditorías de sistemas de información no está regulado, pero es evidente que son necesarias una **formación** y sobre todo una **experiencia** acordes con la función, e incluso con las áreas a auditar: seguridad física, sistemas operativos concretos, determinados gestores de bases de datos o plataformas,

e incluso lenguajes si hubiera que llegar a revisar programas, además de ser imprescindibles en el perfil otras características o circunstancias comunes, como independencia respecto a los auditados, madurez, capacidad de análisis y de síntesis, un interés no meramente económico.

En el seno de la citada ISACA existe un certificado relacionado: CISA (Certified Information Systems Auditor).

A la hora de crear la función de auditoría interna de sistemas de información se suele plantear si se forma a auditores ya expertos en otras áreas: auditoría de cuentas normalmente, o si se forma a técnicos del área de informática, o si se contrata a auditores de otra entidad, ya experimentados; cada opción tiene sus ventajas e inconvenientes, entre los que pueden estar:

- Los auditores de otras áreas serán expertos en técnicas generales como entrevista, y en redactar informes, pero desconocerán las particularidades y riesgos de las tecnologías de la información.

- Los informáticos y expertos en áreas relacionadas no serán expertos en técnicas generales y en control (salvo que provengan de administración de seguridad), si bien puede ser más fácil que aprendan estos aspectos que enseñar —especialmente mantener al día– a un auditor general respecto a novedades tecnológicas.

- Quien venga de otra entidad puede no tener ni unos inconvenientes ni otros, e incluso puede conocer el sector; y hay una ventaja más: no conoce a las personas que tendrá que entrevistar, lo cual es positivo, pero no siempre se quieren incorporar recursos externos.

Otro aspecto es **dónde ubicar** la **función:** encontramos con frecuencia que está dentro del área de Informática o Sistemas de Información o Tecnologías: en definitiva dentro del área auditada por lo que no tiene la independencia necesaria. Es preferible que esté dentro de la auditoría general o que sea una función staff de algún directivo por encima de las áreas objeto de auditoría.

Se incluye un cuadro (véase la figura 17.3) con algunas recomendaciones en cuanto a pautas de conducta.

QUÉ PUEDEN/DEBEN HACER LOS AUDITORES	QUÉ NO DEBEN HACER LOS AUDITORES
Ser independientes y objetivos	Actuar en beneficio propio por encima del interés del cliente
Recomendar	Obligar, forzar, amenazar
Ser competentes en la materia (seguridad)	Asumir encargos para los que no estén preparados
Basar sus informes en verificaciones y evidencias	Basarlos en suposiciones
Verificar que se evalúan periódicamente riegos o bien evaluarlos	Revisar la seguridad "día a día" o administrarla (son funciones de otros)
Conocer perfiles de usuarios	Realizar gestión perfiles de usuarios
Conocer criterios y prácticas sobre contraseñas	Gestión/asignación contraseñas o conocerlas
Verificar que las aplicaciones se desarrollan y mantienen según normas y se incorporan controles	Realizar funciones de análisis o gestionar proyectos
Revisar codificación de programas (seguridad y calidad) y las pruebas realizadas, o bien probarlos	Codificar programas
Revisar la documentación (aplicaciones, programas)	Realizar la documentación
Verificar que siguen los procedimientos	Escribir procedimientos
Responsabilizarse del contenido de sus informes	Aceptar presiones de sus jefes o clientes y que el informe no sea veraz
Evaluar riesgos e informes	Garantizar que no se puedan realizar/haber realizado delitos, fraudes o errores
Sustentar los informes con papeles de trabajo	Enzarzarse en discusiones de diferencias de opiniones
Estar al día en cuanto a avances, riesgos, metodologías	Auditar con técnicas, métodos o recomendaciones obsoletos

Figura 17.3. Pautas de conducta de los auditores

17.14. TÉCNICAS, MÉTODOS Y HERRAMIENTAS

En cada proceso de auditoría se fijan los objetivos, ámbito y profundidad, lo que sirve para la planificación y para la consideración de las fuentes, según los objetivos, así como de las técnicas, métodos y herramientas más adecuados. El factor sorpresa puede llegar a ser necesario en las revisiones, según lo que se quiera verificar.

Como métodos y técnicas podemos considerar los cuestionarios, las entrevistas, la observación, los muestreos, las CAAT (Computer Aided Auditing Techniques), las

utilidades y programas, los paquetes específicos, las pruebas, la simulación en paralelo con datos reales y programas de auditor o la revisión de programas.

17.15. CONSIDERACIONES RESPECTO AL INFORME

En él se harán constar los antecedentes y los objetivos, para que quienes lean el informe puedan verificar que ha habido una comunicación adecuada, así como qué metodología de evaluación de riesgos y estándares se ha utilizado, y una breve descripción de los entornos revisados para que se pueda verificar que se han revisado todas las plataformas y sistemas objeto de la auditoría.

Debe incluirse un resumen **para la Dirección** en términos no técnicos.

Dependiendo de los casos será preferible agrupar aspectos similares: seguridad física, seguridad lógica... o bien clasificar los puntos por centros o redes, especialmente en entidades grandes si existen responsables diferentes: en caso de duda será un punto a comentar previamente con quienes van a recibir el informe, ya que con frecuencia prefieren entregar, a cada uno la parte que más le afecta, así como planificar y controlar área por área o por departamentos la implantación de medidas.

En **cada punto** que se incluya debe explicarse por qué es un incumplimiento o una debilidad, así como alguna recomendación, a veces abarcando varios puntos.

El informe ha de ser necesariamente revisado por los auditados, así como discutido si es necesario antes de emitir el definitivo.

En muchos casos, bien en el propio informe o en otro documento, se recogen las respuestas de los auditados, sobre todo cuando la auditoría es interna.

La entidad decide qué acciones tomar a partir del informe, y en el caso de los auditores internos éstos suelen hacer también un seguimiento de las implantaciones.

Los auditados siempre buscan un informe lo más benigno posible, mientras que los auditores nos proponemos llegar a un informe veraz y útil; estos diferentes puntos de vista a veces crean conflictos en el proceso de auditoría y en la discusión del informe.

En algunos casos los informes se han usado para comparar la seguridad de diferentes delegaciones, sucursales, o empresas de un mismo grupo, o bien filiales de una multinacional, pero si los entornos no son homogéneos las comparaciones pueden no ser muy útiles y llegar a distorsionar.

Con frecuencia quienes han pedido la auditoría quieren conocer la **calificación respecto a seguridad,** además de disponer de un informe complementario o resumen en términos no técnicos; quieren saber si están aprobados en seguridad, así como los riesgos más destacados.

Es necesario, por tanto, diferenciar puntos muy graves, graves, memorables... u otra clasificación, en definitiva establecer algunas **métricas de seguridad** y clasificar los puntos según su importancia y prioridad, que pueden ser reconsideradas por la Dirección de la entidad a la hora de implantar las medidas, y en algunos casos se puede llegar a entregar una lista provisional de proyectos de implantación.

En ocasiones, en el caso de auditoría externa, los clientes que no conocen los límites, habituales de la auditoría sobreentienden que una vez finalizada ésta los auditores daremos una asistencia más propia de consultores, y que incluso llevaremos a cabo implantaciones, redactaremos normas, o que al menos en los informes especificaremos las soluciones: nombre de la herramienta que refuerza la seguridad en su entorno por ejemplo, cuando a menudo esto requiere un estudio que se sale de los límites e incluso de la independencia propios de la auditoría. Por ello, es importante que se delimiten las responsabilidades y los productos a entregar que son objeto de una auditoría externa en el contrato o propuesta.

Algunos de los puntos importantes que pueden llegar a estar en los informes respecto a seguridad, y sin que, se pueda generalizar porque dependerá de la entidad, sector y circunstancias, pueden ser la ausencia de:

- Copias de activos críticos en cuanto a continuidad, *en lugar diferente* y distante.
- Cumplimiento de la legislación aplicable así como de las políticas y normas internas: en el caso de la legislación incluso pueden producirse sanciones, y en el caso concreto de la LOPD la inmovilización de archivos como hemos indicado.
- Diferenciación de entornos de desarrollo y producción, en cuanto a datos y programas, y control de accesos.
- Involucración de la Alta Dirección, preferentemente a través de algún comité.
- Motivación de los empleados y directivos en relación con la seguridad.
- Evaluación periódica y adecuada de riesgos.
- Segregación de funciones, así como una organización adecuada.

Es, frecuente también que quienes han pedido la auditoría quieran conocer después en qué medida se han resuelto los problemas, a partir de las decisiones tomadas, a través de los informes de los auditores internos o de quienes implanten las medidas.

Otro deseo frecuente es querer conocer la **evolución de la situación** en el tiempo, ya que aparecen nuevos riesgos, se reproducen otros, y algunos pueden variar de clasificación en función del cambio de plataformas u otros.

Para ello es útil mostrar en algún informe –principalmente los auditores internos–, algunos cuadros que muestren la evolución, que en algunos casos ha sido útil para demostrar la rentabilidad de una función como administración de la seguridad o auditoría interna o para evaluar la utilidad de un plan de seguridad.

17.16. CONTRATACIÓN DE AUDITORÍA EXTERNA

Incluimos el epígrafe porque consideramos su utilidad en función de las preguntas que a veces se nos hacen y de los casos que hemos llegado a conocer: si no se sigue un proceso de selección adecuado de auditores externos no se pueden garantizar los resultados y se puede llegar al desencanto al recibir el informe, lo que puede suponer no llegar a conocer las posibilidades reales de la auditoría de sistemas de información, sobre todo en un tema tan delicado como la seguridad, o bien tener una visión pobre y desfigurada, como les ocurre a algunos a partir de experiencias atípicas.

Algunas **consideraciones** pueden ser:

- La entidad auditora ha de ser independiente de la auditada en el caso de una auditoría externa: si está ofreciendo otros servicios a la vez, o piensa ofrecerlos en el futuro, o incluso a veces si ha sido proveedora en el pasado, a menudo puede encontrar dificultades internas para entregar un informe veraz y completo.

  En ocasiones los propios auditores lo han llegado a comunicar, por ética.

- Las personas que vayan a realizar el trabajo han de ser independientes y competentes, según el objetivo: sistemas operativos o plataformas concretas, por lo que no está de más examinar sus perfiles e incluso mantener alguna entrevista, sin descartar preguntar por sorpresa en una reunión qué aspectos revisarían y qué técnicas usarían en el entorno que se les describa.

- No es tan común pedir referencias de otros trabajos similares como en el caso de consultaría pero se puede hacer, aunque para ello los auditores debieran pedir permiso previo a sus clientes.

- La auditoría ha de encargarse a un nivel suficiente, normalmente Dirección General o Consejero Delegado, y a este nivel recibir los informes, porque si no a veces no se cuenta con el respaldo suficiente en las revisiones, y en todo caso puede que si el informe no es favorable quede escondido, y se ha perdido el dinero y a veces la oportunidad.

- Finalmente, a título de curiosidad, en una ocasión se nos pidió que no figurara la palabra auditoría en el informe final, porque había aversión por el término, por asociarse en la entidad a los auditores con los verdugos: no es un caso aislado y es impropio.

- Recordemos que puede ser necesario dar o mostrar a los auditores todo lo que necesiten para realizar su trabajo, pero nada más, e incluso lo que se les muestre o a lo que se les permita acceder puede ser con restricciones: sólo parte de una base de datos, epígrafes de algunas actas, o simplemente mostrarles documentación, que no pueden copiar o no pueden sacar de las instalaciones del cliente: se puede exigir una cláusula de confidencialidad, y raramente se les deben mostrar datos reales confidenciales de clientes, proveedores, empleados u otros, aunque se haga en la práctica con frecuencia.

  En caso de duda o de conflicto puede decidir un comité de auditoría o el propio de Dirección.

17.17. RELACIÓN DE AUDITORÍA CON ADMINISTRACIÓN DE SEGURIDAD

Hemos encontrado en más de una ocasión que la misma persona tenía las funciones; de administración de seguridad y auditoría (informática) interna, lo cual puede parecer bien a efectos de productividad, pero no es admisible respecto a segregación de funciones, siendo preferible, si la entidad no justifica que dos personas cumplan en exclusiva ambas funciones, que se cubra sólo una, o bien que la persona realice otras funciones complementarias pero compatibles, como podrían ser algunas relacionadas con calidad.

En entidades grandes la función consta además de corresponsales funcionales o autonómicos.

La función de Administración de Seguridad en parte será interlocutora en los procesos de auditoría de seguridad, si bien los auditores no podemos perder nuestra necesaria independencia, ya que debemos evaluar el desempeño de la función de administración de seguridad, desde si sus funciones son adecuadas y están respaldadas

por algún documento aprobado a un nivel suficiente, hasta el cumplimiento de esas funciones y si no hay conflicto con otras.

La función de auditoría de sistemas de información y la de administración de seguridad pueden ser complementarias, si bien sin perder su independencia: se trata de funciones que contribuyen a una mayor y mejor protección, y resultan como anillos protectores, como se muestra en la figura 17.4.

Figura 17.4. Funciones de auditoría de SI y auditoría de seguridad como "anillos protectores"

Ambas funciones han de mantener contactos periódicos y prestarse cierta asistencia técnica.

Normalmente Administración de seguridad habrá de implantar las recomendaciones de los auditores una vez fijadas las prioridades por la Dirección de la entidad.

Administración de Seguridad puede depender del área de Sistemas de Información, sobre todo si existe Auditoría de SI interna, pero si puede estar en peligro su desempeño quizá sea preferible que tenga otra dependencia superior, o al menos una dependencia funcional de áreas usuarias como puede ser de Dirección de Operaciones o similar; la existencia de un comité de Seguridad de la Información, o bien de una función de Seguridad Corporativa puede resultar útil.

En ocasiones los administradores de seguridad tienen casi exclusivamente una función importante pero que sólo forma una parte de su cometido: la administración del paquete de control de accesos: RACF, Top Secret, u otros, con frecuencia por haber sido técnicos de sistemas, y en ocasiones porque siguen siéndolo, lo que representa una gran vulnerabilidad y no siempre bien aceptada cuando la hemos recogido en los informes de auditoría.

Por otra parte, si la persona que oficialmente administra la seguridad únicamente incorpora usuarios y asigna contraseñas iniciales en uno de los sistemas, generalmente el más importante, se trata de una labor necesaria pero en absoluto la única, dándose a veces una carencia de objetivos de seguridad, de modelos, de planes de seguridad, así como de seguimiento de transgresiones.

Otra situación que se suele producir respecto al paquete de control de accesos, y a veces coexistiendo con la señalada, es la que indicábamos: coincidencia de los roles de administración de seguridad y auditoría interna en la misma persona, relativamente comprensible porque son papeles que hay que asignar en los sistemas o paquetes. Hemos conocido situaciones de cierta tensión cuando los administradores han tenido que crear usuarios con perfil de auditor –por ejemplo cuando éstos asumen sus funciones respecto al paquete– y quitarse ese perfil a sí mismos.

Ambas funciones han de tener una dependencia jerárquica adecuada, una descripción de funciones idónea, y que las personas cuenten con formación y experiencia acordes y estén motivadas; cuando a alguien se le asigna una de estas funciones para que no desaparezca del área o incluso de la entidad, como consecuencia de reorganizaciones o absorciones, difícilmente va a cumplir bien su papel. Finalmente, que ambas funciones, sin perder de vista su cometido, quieran colaborar para conseguir un buen nivel de protección.

Volviendo brevemente a la formación y experiencia, hemos encontrado vulnerabilidades de distinta índole en individuos con un conocimiento técnico de los sistemas muy profundo, y probablemente mayores vulnerabilidades cuando se da el caso contrario: aquellos que administran o revisan sin saber qué hacen, cómo lo hacen, si afecta en el rendimiento, o si sus recomendaciones o imposiciones respecto a la seguridad impactan gravemente en la productividad o crean situaciones de verdadero bloqueo o de auténtica burocracia.

17.18. CONCLUSIONES

Aunque aún no se ha producido en España el despegue de la auditoría ni de la seguridad que esperamos desde hace años, lo cierto es que se han dado avances

significativos, y cabe esperar que siga esta tendencia y las entidades vayan entendiendo cada vez más la utilidad de la protección de la información y de la auditoría.

También es cierto que han surgido bastantes entidades suministradoras que han incluido la seguridad y la auditoría entre sus posibles servicios, o simplemente han aceptado trabajos, en ambos casos sin disponer de expertos, lo que con frecuencia ha supuesto un desencanto en la entidad auditada, y a veces resultados penosos, que no benefician ni a la profesión ni a la auditoría misma.

Por otra parte, y así lo hemos indicado en el capítulo, los auditados finales, y más los responsables de las áreas que sus colaboradores, siguen en muchos casos sin entender la esencia y utilidad de la auditoría, y su obsesión es evitarla y, cuando ya es inevitable, a veces eludirla o al menos no resultar entrevistados: como que el proceso no fuera con ellos (es del responsable hacia abajo, pero exclusiva, como nos dijo un Director de Sistemas de Información en una ocasión), o tal vez para poder alegar que ellos no han facilitado la información que figura en el informe final.

En otras ocasiones han preparando a los entrevistados respecto a qué deben decir y qué no en cuanto a riesgos o controles existentes, e incluso han hecho que todas las entrevistas se mantuvieran en su despacho y en su presencia, como nos pasó en una auditoría de seguridad ciertamente delicada, por lo que los auditores a veces hemos de ser algo psicólogos sin formación para ello e interpretar lo que se nos dice, lo que se nos quiere decir, y distinguir la versión oficial de la realidad, interpretar silencios y miradas, entrevistar a varias personas y llegar a evidencias por distintos medios.

Por otra parte, hemos podido verificar que la auditoría, su filosofía, así como sus técnicas y métodos, interesan cada vez más a los responsables de Sistemas de Información, a veces para conocer cómo pueden evaluar los auditores sus áreas, pero a menudo saber cuáles pueden ser los riesgos y qué controles implantar.

Lo que ellos mismos pueden realizar no se puede considerar una auditoría, más por falta de independencia que por desconocimiento de las técnicas, pero sí pueden constituir unos autodiagnósticos muy útiles, especialmente cuando se realizan con ayuda de listas o herramientas adaptadas o adaptables al entorno.

Los cambios en la tecnología influyen en qué auditar y en cómo auditar. En efecto, en los últimos años han ido apareciendo áreas nuevas, como las mencionadas de comercio electrónico, cliente-servidor, orientación a objetos, entornos multiplataforma, teletrabajo y *outsourcing*, además de otros sistemas operativos o nuevas versiones de los mismos, lo que viene a suponer novedad en los riesgos y en las medidas y la necesidad imperiosa por parte de los auditores de estar muy al tanto: como otros técnicos relacionados con las tecnologías de la información tenemos la servidumbre –o el placer y la oportunidad- de estar permanentemente informados.

Aunque las implantaciones de la seguridad van siendo más sofisticadas y llegando a áreas o aspectos casi desconocidos hace años, esto no implica que estén plenamente resueltos los más básicos: encontramos bastantes deficiencias en controles físicos, no tanto porque no existan cuanto por las brechas o descuidos que se pueden encontrar.

Más preocupante aún es la inexistencia de controles básicos, como en relación con la segregación de funciones, separación de entornos o casi ausencia de normativa.

La auditoría en sistemas de información no está suficientemente implantada en la mayoría de las entidades españolas, si bien supondría una mayor garantía de que las cosas se hacen bien y como la entidad quiere: en general hay coincidencia entre ambos puntos. Puede ser también una profesión con futuro cuando la auditoría despegue.

Como función aporta al auditor un conocimiento privilegiado del área de Sistemas de Información con una perspectiva muy amplia.

La forma de realizar el trabajo va variando y se está llegando a aplicar el control por excepción y la teleauditoría.

En cuanto a nuevas áreas, surge el auge del **comercio electrónico,** el control de **páginas WEB:** la revisión de quien autoriza, varía y controla los contenidos: en las entidades por seguridad y productividad, y en los hogares, aunque esto se sale de la auditoría y queda en el control para evitar que los menores accedan a contenidos con violencia o pornografía.

Por lo que se ha incluido en el capítulo se presenta de forma breve, como corresponde a obra general que abarca los diferentes aspectos de la auditoría, por lo que hemos resumido el contenido del material de cursos propios tanto sobre Auditoría de la Seguridad como sobre diferentes aspectos de la propia Seguridad.

17.19. LECTURAS RECOMENDADAS

EDP Auditing. AUERBACH, 1997.

Data Security Management. AUERBACH, 1997.

Datapro Reports on Information Security. DATAPRO. McGraw-Hill, 1997.

ISACA (Information Systems Audit and Control Association/Foundation) *COBIT: Control Objectives for Information and Related Technology.* Abril, 1996.

(*) Las tres primeras obras son de actualización permanente.

17.20. CUESTIONES DE REPASO

1. La seguridad de la información en España: situación ¿se conocen realmente los riesgos? Perspectivas.
2. El perfil del auditor en seguridad de sistemas de información.
3. Estándares para la auditoría de la seguridad.
4. La comunicación a auditados y el factor sorpresa en auditorías de seguridad.
5. ¿Qué debe hacer el auditor si se le pide que omita o varíe algún punto en su informe?
6. Auditoría de la seguridad en las próximas décadas: nuevos riesgos, técnicas y herramientas.
7. Equilibrio entre seguridad, calidad y productividad.
8. ¿Qué es más crítico: datos, programas, personas, comunicaciones, instalaciones...?
9. Relaciones entre Administración de Seguridad y Auditoría de Sistemas de Información interna y externa.
10. Cálculo de la rentabilidad de la auditoría de seguridad.

CAPÍTULO 18

AUDITORÍA DE REDES

José Ignacio Boixo Pérez-Holanda

18.1. TERMINOLOGÍA DE REDES. MODELO OSI

Para poder auditar redes, lo primero y fundamental es utilizar el mismo vocabulario (más bien jerga) que los expertos en comunicaciones que las manejan. Debido a la constante evolución en este campo, un primer punto de referencia es poder referirse a un modelo comúnmente aceptable. El modelo común de referencia, adoptado por ISO *(International Standards Organization)* se denomina Modelo OSI *(Open Systems Interconection)*, y consta de estas siete capas:

7	Aplicación	Es donde la aplicación que necesita comunicaciones enlaza, mediante *API (Application Program Interface)* con el sistema de comunicaciones.
6	Presentación	Define el formato de los datos que se van a presentar a la aplicación.
5	Sesión	Establece los procedimientos de aperturas y cierres de sesión de comunicaciones, así como información de la sesión en curso.
4	Transporte	Comprueba la integridad de los datos transmitidos (que no ha habido pérdidas ni corrupciones).
3	Red	Establece las rutas por las cuales se puede comunicar el emisor con el receptor, lo que se realiza mediante el envío de paquetes de información.
2	Enlace	Transforma los paquetes de información en tramas adaptadas a los dispositivos físicos sobre los cuales se realiza la transmisión.
1	Físico	Transforma la información en señales físicas adaptadas al medio de comunicación.

La potencia del modelo OSI proviene de que cada capa no tiene que preocuparse de qué es lo que hagan las capas superiores ni las inferiores; cada capa se comunica con su igual en el interlocutor, con un protocolo de comunicaciones específico. Entre cada par de capa N y capa N-1 está perfectamente definido el paso de la información, que se produce *dentro* de la misma máquina, con métodos clásicos de programación en local.

Para establecer una comunicación, la información atraviesa descendentemente la pila formada por las siete capas, atraviesa el medio físico y asciende a través de las siete capas en la pila de destino. Por tanto, cada capa tiene unos métodos prefijados para comunicarse con las inmediatamente inferior y superior.

De esta manera, se aíslan los protocolos que se utilizan en unas capas con los protocolos que se utilizan en otras. Por ejemplo, es posible transmitir tráfico TCP/IP (capas superiores), a través de Ethernet o Token-Ring indistintamente (capas inferiores), gracias a esta independencia entre capas.

Este método de especificar a qué capas corresponde cada protocolo de comunicaciones resulta muy útil a efectos didácticos, pues rápidamente se tiene una visión del alcance y utilidad del protocolo o elemento de comunicaciones en cuestión.

Como regla mnemónica para recordar fácilmente el orden de las siete capas OSI, suele utilizarse la frase "Formemos Esta Red y Todos Seremos Pronto Amigos" (Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación).

En los niveles inferiores, habitualmente hasta el nivel tres, es donde se definen las redes LAN (Local Area Network), MAN (Metropolitan Area Network) y WAN (Wide Area Network). Las funcionalidades de estos tres tipos de redes son similares, variando fundamentalmente la distancia que son capaces de salvar entre el emisor y el receptor (LAN: dentro de un edificio, MAN: dentro de un campus o zona urbana, WAN: cualquier distancia), siendo la velocidad inversamente proporcional a la distancia.

La red LAN más extendida, Ethernet, está basada en que cada emisor envía, cuando desea, una trama al medio físico, sabiendo que todos los destinatarios están permanentemente en escucha. Justo antes de enviar, el emisor se pone a la escucha, y si no hay tráfico, procede directamente al envío. Si al escuchar detecta que otro emisor está enviando, espera un tiempo aleatorio antes de volverse a poner a la escucha. Según crece el tráfico, se incrementa la probabilidad de que dos emisores hayan escuchado que el medio está libre y se pongan a transmitir simultáneamente. En ese caso, se habrá producidos una colisión y las tramas enviadas se destruirán mutuamente, creándose una alteración que es percibido físicamente como colisión de tramas. Cada emisor procede entonces a dar la trama como no enviada y a esperar un

tiempo aleatorio antes de ponerse de nuevo a escuchar, exactamente igual que cuando el medio estaba ocupado. Las tecnologías de Ethernet (10 Megabits por segundo - Mbps), Fast Ethernet (100 Mbps) y Giga Ethernet (1.000 Mbps) se basan en el mismo principio, incrementando sucesivamente la velocidad de transmisión. La Ethernet fue normalizada por el norteamericano Institute of Electric and Electronic Engineers con el nombre IEEE 802.3.

El cable que físicamente conecta a equipos Ethernet se denomina segmento. En vez de tender un único cable que recorra todos los equipos del segmento, se suele tender un cable por equipo y juntar todos los cables en un concentrador pasivo ("lau") o activo ("hub"). Cada segmento admite un número máximo de equipos, por lo que los segmentos han de ser conectados entre sí mediante dispositivos que hagan que la información pase del segmento origen al segmento de destino, pero confinando en cada segmento la información que no deba salir de él y así evitar anegar los segmentos adyacentes.

La LAN Token-Ring, desarrollada por IBM, está normalizada como IEEE 802.5, tiene velocidades de 4 y 16 Mbps y una mejor utilización del canal cuando se incrementa el tráfico. La FDDI es otra LAN, basada en transmisión a través de fibras ópticas, a velocidades de centenas de Mbps, que se suele utilizar para interconectar segmentos de LAN.

Para redes WAN, está muy extendido el X.25. Se basa en fragmentar la información en paquetes, habitualmente de 128 caracteres. Estos paquetes se entregan a un transportista habitualmente público que se encarga de ir enviándolos saltando entre diversos nodos intermedios hacia el destino. En cada nodo se lleva una cuenta con el nodo inmediato (colateral), para saber que cada paquete se ha recibido correctamente, o si hubo fallo, proceder a su retransmisión. Para su transmisión, cada paquete recibe una cabecera y una cola, y así queda convertida en una trama con control de tráfico y de errores entre cada pareja colateral de nodos. Mediante este salto de nodo a nodo se puede establecer tráfico a cualquier distancia a velocidades típicas de decenas de Kbps.

El Frame-Relay es básicamente lo mismo que el X.25, pero, aprovechando que la fiabilidad entre nodos es muy alta, sólo se comprueba que los paquetes han sido transportados sin errores cuando son recibidos en el destinatario; esto ahorra multitud de comprobaciones en los nodos intermedios, incrementando la velocidad hasta el orden de los cientos de Kbps.

El ATM (Asynchronus Transfer Mode/modo de transferencia asíncrono) utiliza un concepto de alguna manera similar a Frame Relay, con tramas de 53 caracteres (cinco de cabecera y 48 de información a transportar), que se conmutan en nodos

especialmente diseñados, con lógica prácticamente cableada, a muy alta velocidad, desde los cien Mbps.

18.2. VULNERABILIDADES EN REDES

Todos los sistemas de comunicación, desde el punto de vista de auditoría, presentan en general una problemática común: La información transita por lugares físicamente alejados de las personas responsables. Esto presupone un compromiso en la seguridad, ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información.

En las redes de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente tres tipos de incidencias:

1ª Alteración de bits. Por error en los medios de transmisión, una trama puede sufrir variación en parte de su contenido. La forma más habitual de detectar, y corregir en su caso, este tipo de incidencias, es sufijar la trama con un Código de Redundancia Cíclico (CRC) que detecte cualquier error y permita corregir errores que afecten hasta unos pocos bits en el mejor de los casos.

2ª Ausencia de tramas. Por error en el medio, o en algún nodo, o por sobrecarga, alguna trama puede desaparecer en el camino del emisor al receptor. Se suele atajar este riesgo dando un número de secuencia a las tramas.

3ª Alteración de Secuencia. El orden en el que se envían y se reciben las tramas no coincide. Unas tramas han adelantado a otras. En el receptor, mediante el número de secuencia, se reconstruye el orden original.

Por causas dolosas, y teniendo en cuenta que es físicamente posible interceptar la información, los tres mayores riesgos a atajar son:

1º Indagación. Un mensaje puede ser leído por un tercero, obteniendo la información que contenga.

2º Suplantación. Un tercero puede introducir un mensaje espurio que el receptor cree proveniente del emisor legítimo.

3º Modificación. Un tercero puede alterar el contenido de un mensaje.

Para este tipo de actuaciones dolosas, la única medida prácticamente efectiva en redes MAN y WAN (cuando la información sale del edificio) es la criptografía. En

redes LAN suelen utilizarse más bien medidas de control de acceso al edificio y al cableado, ya que la criptografía es muy onerosa todavía para redes locales.

Dada la proliferación de equipos que precisan comunicación de datos dentro de los edificios, es muy habitual plantearse sistemas de cableado integral en vez de tender un cable en cada ocasión. Esto es prácticamente un requisito en edificios con cierto volumen de usuarios.

Los sistemas de cableado suelen dividirse según su ámbito. En cada planta o zona se tienden cables desde un armario distribuidor a cada uno de los potenciales puestos. Este cableado se denomina habitualmente de " planta". Estos armarios están conectados a su vez, entre sí y con las salas de computadores, denominándose a estas conexiones cableado "troncal". Desde las salas de computadores parten las líneas hacia los transportistas de datos (Telefónicas o PTTs), saliendo los cables al exterior del edificio en lo que se denomina cableado de " ruta".

El cableado de planta suele ser de cobre, por lo que es propenso a escuchas ("pinchazos") que pueden no dejar rastro. El cableado troncal y el de ruta cada vez más frecuentemente se tienden mediante fibras ópticas, que son muy difíciles de interceptar, debido a que no provocan radiación electromagnética y a que la conexión física a una fibra óptica requiere una tecnología delicada y compleja.

En el propio puesto de trabajo puede haber peligros, como grabar/retransmitir la imagen que se ve en la pantalla, teclados que guardan memoria del orden en que se han pulsado las teclas, o directamente que las contraseñas estén escritas en papeles a la vista.

Dentro de las redes locales, el mayor peligro es que alguien instale una "escucha" no autorizada. Al viajar en claro la información dentro de la red local, es imprescindible tener una organización que controle estrictamente los equipos de escucha, bien sean éstos físicos ("sniffer") o lógicos ("traceadores"). Ambos escuchadores, físicos y lógicos, son de uso habitual dentro de cualquier instalación de cierto tamaño. Por tanto, es fundamental que ese uso legítimo esté controlado y no devenga en actividad espuria.

El riesgo de interceptar un canal de comunicaciones, y poder extraer de él la información, tiene unos efectos relativamente similares a los de poder entrar, sin control, en el sistema de almacenamiento del computador.

Hay un punto especialmente crítico en los canales de comunicaciones que son las contraseñas de usuario. Mientras que en el sistema de almacenamiento las contraseñas suelen guardarse cifradas, es inhabitual que los terminales u computadores personales sean capaces de cifrar la contraseña cuando se envía al computador central o al servidor.

Por tanto, alguien que intercepte la información puede hacerse con las contraseñas claro. Además, dado que las carátulas iniciales donde se teclea la contraseña siempre las mismas, se facilita la labor de los agentes de interceptación, pues proporcionan un patrón del paquete de información donde viaja la contraseña a interceptar.

18.3. PROTOCOLOS DE ALTO NIVEL

Como protocolos de alto nivel, los más importantes por orden de aparición en la industria son: SNA, OSI, Netbios, IPX y TCP/IP.

SNA

System Network Architecture. Fue diseñado por IBM a partir de los años setenta, al principio con una red estrictamente jerarquizado, y luego pasando a una estructura más distribuida, fundamentalmente con el tipo de sesión denominado LU 6.2.

El SNA se encuentra fundamentalmente en los computadores centrales IBM, donde sigue gozando de un extraordinario vigor, especialmente para comunicación con terminales no inteligentes de tipo 3270, y para sesiones establecidas entre computadores centrales y componentes software IBM.

OSI

Fue diseñado por el antiguo Comité Consultivo Internacional de Teléfonos y Telégrafos –CCITT–, actualmente Unión Internacional de Telecomunicaciones –ITU– básicamente compuesto por las compañías telefónicas nacionales (llamadas PTT). Se diseñaron todas las capas, desde los medios físicos hasta las aplicaciones como trasferencia de archivos o terminal virtual. Donde ha tenido éxito es en el protocolo de Red X.25 y en el correo electrónico X.400.

Netbios

Este protocolo fue el que se propuso, fundamentalmente por Microsoft, para comunicar entre sí computadores personales en redes locales. Es una extensión a red ("net") del "Basic Input/Output System" del sistema operativo DOS. Está más orientado a la utilización en LAN, siendo bastante ágil y efectivo.

IPX

Es el protocolo propietario de Novell que, al alcanzar en su momento una posición de predominio en el sistema operativo en red, ha gozado de gran difusión. Su suerte está ligada a la de ese fabricante.

TCP/IP

(Transfer Control Protocol/Internet Protocol). Diseñado originalmente en los años setenta, para sobrevivir incluso a ataques nucleares contra los EE.UU., e impulsado desde los ámbitos académicos, la enorme versatilidad de este protocolo y su aceptación generalizada le ha hecho el paradigma de protocolo abierto, siendo la base de interconexión de redes que forman la Internet. Es el protocolo que está imponiéndose, por derecho propio, como gran unificador de todas las redes de comunicaciones.

Lamentablemente, no existe una independencia *de facto* entre las aplicaciones y los protocolos de alto nivel. Es todavía poco habitual que los clásicos programas de computador central IBM se usen con protocolo distinto de SNA. Por su parte el TCP/IP posee una gran cantidad de aplicaciones, ampliamente difundidas, pero que no pueden funcionar con otros protocolos.

Por ejemplo, la transmisión de archivos FTP *(File Transfer Protocol),* el correo electrónico SMTP *(Simple Mail Transfer Protocol)* o el terminal virtual Telnet han de correr precisamente sobre una "pila" de protocolo TCP/IP. Se establece así una retroalimentación donde las utilidades refuerzan al protocolo TCP/IP, que se vuelve cada vez más atractivo para que los desarrolladores escriban nuevas utilidades a él orientadas. Además, precisamente por su apertura, el TCP/IP es el preferido por organismos reguladores y grandes empresas, pues permiten evitar, al ser abierto, la dependencia de ningún fabricante en concreto.

Una solución que está teniendo éxito es "encapsular" un protocolo sobre otro. Así, el Netbios puede ser transportado sobre TCP/IP; la capa inferior, Netbeui, puede ser sustituida por TCP/IP, quedando el Netbios "encapsulado" sobre TCP/IP. Sin embargo, han de tenerse muy en cuenta las vulnerabilidades que se crean al encapsular. En el caso de Netbios sobre TCP/IP son vulnerabilidades serias, pues facilitan el tomar control remoto de recursos que se pensó que sólo se accederían en local, confiando, al menos en parte, en la protección física.

Al ser los sistemas de comunicaciones, procesos "sin historia", donde no se almacenan permanentemente datos de ningún tipo, los sistemas de recuperación se ven especialmente beneficiados por esta característica. Si una sesión cae, una vez que se

vuelve a establecer la sesión, el incidente queda solucionado. Es responsabilidad de la aplicación volver a reinicializar si la interrupción se produjo en mitad de una unidad de proceso.

Por ejemplo, si la interrupción de la sesión se ha producido a mitad de una transferencia de archivo, será misión de la aplicación, cuando la sesión se reanude, determinar si vuelve a comenzar la transmisión del archivo desde el principio o si reutiliza la parte que ya se ha transmitido.

Si es una persona quien ha sufrido el incidente, cuando se reanude la sesión deberá volver a identificarse con su nombre de usuario y contraseña, comprobando hasta qué punto la aplicación en la que estaba operando recogió los últimos datos que introdujeron.

Esta restricción fundamental, de que los sistemas de comunicaciones no almacenan datos, permite una mayor facilidad a la hora de duplicar equipamiento. Dado que una vez cerrada la sesión no queda ninguna información a retener (salvo obviamente estadísticas y pistas de auditoría), la sesión, al reanudarse, puede utilizar la misma o diferente ruta. Si existen diversos nodos y diversos enlaces entre ellos, la caída de un nodo sólo ha de significar la interrupción de las sesiones que por él transiten, que se podrán reiniciar a través de los restantes nodos. Por ello, es una norma generalmente aceptada, al menos en redes de cierto tamaño, tener nodos y enlaces replicados para prevenir situaciones de contingencia.

Una vez más, el protocolo TCP/IP demuestra en este caso su utilidad. Al haber sido este protocolo diseñado para encontrar rutas remanentes, inclusive ante caídas masivas, está especialmente bien orientado para facilitar la reestructuración de una red ante fallos de parte de sus componentes, sean éstos líneas, nodos o cualquier otro tipo de equipamiento. Cada vez más se está orientando los equipos de red a manejar prioritariamente tráfico TCP/IP y añadir facilidades de gestión de sobrecargas, rutas alternativas, tratamientos de contingencias y todo tipo de situaciones que acontecen en una red en funcionamiento.

18.4. REDES ABIERTAS (TCP/IP)

Ante el auge que está tomando el protocolo TCP/IP, como una primera clasificación de redes, se está adoptando la siguiente nomenclatura para las redes basadas en este protocolo:

- Intranet: Es la red interna, privada y segura de una empresa, utilice o no medios de transporte de terceros.

- Extranet: Es una red privada y segura, compartida por un conjunto de empresas, aunque utilice medios de transporte ajenos e inseguros, como pudiera ser Internet.

- Internet: Es la red de redes, "metared" a donde se conecta cualquier red que se desee abrir al exterior, pública e insegura, de alcance mundial, donde puede comunicar cualquier pareja o conjunto de interlocutores, dotada además de todo tipo de servicios de valor añadido. Infovía es la Internet que soporta Telefónica, con peculiaridades fundamentalmente comerciales.

El mayor peligro que representa un acceso TCP/IP no autorizado viene precisamente por la mayor virtud del TCP/IP: su amplia disponibilidad de utilidades. Dada la estandarización de las utilidades TCP/IP, es muy razonable suponer que cada máquina con acceso TCP/IP tenga "puertos abiertos", que a su vez tienen direcciones normalizadas donde encontrar transmisores de archivos, servidores de correo, terminales virtuales y todo tipo de servicios de utilidad. Una ausencia de protección significaría que un tercero puede utilizar estos servicios normalizados, de común existencia en cualquier máquina, en beneficio propio.

Un dispositivo específicamente dedicado a la protección de una Intranet ante una Extranet, y fundamentalmente ante Internet, es el cortafuegos (Firewall). Ésta es una máquina dedicada en exclusiva a leer cada paquete que entra o sale de una red para permitir su paso o desecharlo directamente. Esta autorización o rechazo está basada en unas tablas que identifican, para cada pareja de interlocutores (bien sea basado en el tipo de interlocutor o inclusive en su identificación individual) los tipos de servicios que pueden ser establecidos. Para llevar a cabo su misión, existen diversas configuraciones, donde se pueden incluir encaminadores (routers), servidores de proximidad (proxy), zonas desmilitarizadas, bastiones, y demás parafernalia, a veces copiada de modelos militares.

Las políticas de protección en un cortafuegos suelen denominarse desde "paranoicas" hasta "promiscuas", pasando por todo tipo de gamas intermedias. Dícese de la política paranoica cuando está prohibido absolutamente todo, requiriéndose una autorización específica para cada servicio en concreto entre cada par de interlocutores concretos. Dícese de política promiscua cuando todo está autorizado, identificándose específicamente aquellos servicios concretos entre parejas concretas de interlocutores que se prohíben. Lo más habitual es autorizar específicamente servicios (por ejemplo, correo electrónico) para ciertos tipos genéricos de usuarios (por ejemplo, a todos), otros servicios (por ejemplo, terminal virtual) a ciertos usuarios específicos (por ejemplo, servidor de terminales virtuales) y el resto no autorizarlo.

Figura 18.1. Protección de una red Intranet

Para proteger la red interna "Intranet" del exterior suele utilizarse el esquema expuesto en la figura 18.1, o bien variaciones del mismo. Se parte de la base de que la información que viaja entre la Intranet y el exterior ha de atravesar la "zona desmilitarizada" (DMZ de sus siglas inglesas), pasando por dos encaminadores. Un encaminadór protege los accesos desde el exterior hacia la zona desmilitarizada (encaminador externo) y otro protege los accesos desde la zona desmilitarizada hacia la Intranet (encaminador interno). En la zona desmilitarizada se instalan aquellos servicios a los que haya que acceder desde el exterior y desde el interior, en una máquina especialmente segura, denominada *bastión,* que debe ser dedicada exclusivamente a este fin.

Por ejemplo, un servidor proxy accede a un servidor Internet, recuperando la información que haya solicitado un usuario interno, y almacenándola para que pueda ser recuperada desde la Intranet. De esta manera se evita una conexión directa desde una máquina interna a un servidor Internet. Del mismo modo, el correo electrónico podría recibirse en un servidor instalado en la zona desmilitarizada y reexpedirse hacia el interior. El objetivo es evitar establecer sesiones directas entre una máquina Intranet y una maquina externa. Los encaminadores impedirán que se establezcan conexiones de este tipo, salvo aquellas que específicamente se determinen. El encaminador externo sólo permitirá que atraviese tráfico autorizado entre el exterior y el bastión, y el encaminador interno hará lo propio con el tráfico entre el bastión y la red interna.

Este esquema de protección puede ser simplificado, a costa de disminuir funcionalidades y solidez, prescindiendo en primer lugar del encaminador interno, y en segundo lugar del bastión. Abrir al exterior, sin protección, una red interna, queda fuera de la buena práctica informática.

El peligro más clásico es que un extraño se introduzca desde el exterior hacia la red interna. Dado que las técnicas para saltar los procedimientos de seguridad son públicas y se puede acceder a ellas desde Internet, una primera preocupación debiera ser, periódica, controlada y preventivamente, intentar saltar los procedimientos de seguridad antes de que un extraño los ponga a prueba.

Para comprobar los controles de acceso desde el exterior, así como las vulnerabilidades en la red interna, cortafuegos, servidores, etc. existen programas específicos ya comercializados, como por ejemplo SAFEsuite, Satan, Cops... que facilitan esta tarea, comprobando las vulnerabilidades ya conocidas. Las nuevas versiones de estos programas, que aparecen regularmente, incluyen comprobaciones de las nuevas debilidades detectadas. Como en el caso de los anti-virus, se deben tener estos programas actualizados a fecha reciente.

Un primer ataque es conseguir la identificación de un usuario. Para ello pueden utilizarse técnicas de indagación, leyendo el tráfico hasta encontrar nombres de usuario y contraseñas, poner a prueba la buena fe de los usuarios mandándoles un mensaje del tipo "soy su administrador, por favor, cambie su contraseña a *manzana*" o directamente intentar encontrar identificaciones habituales de usuarios ("prueba", "opel", "master"...), o que ya vienen por defecto en muchos sistemas.

Aunque los archivos de contraseñas están cifrados, habitualmente utilizando como clave de cifrado de cada contraseña la propia contraseña, como los métodos de cifra se conocen, existen programas que son capaces de probar miles de contraseñas usuales ya cifradas para ver si corresponden con alguna del archivo de contraseñas cifradas. Por ello es fundamental evitar que los archivos con las contraseñas cifradas caigan en manos de terceros.

En los sistemas distribuidos, se suele utilizar la técnica de "confianza entre nodos", de manera que si un usuario está autorizado para el nodo A, y solicita desde el nodo A un servicio al nodo B, como el nodo B "confía" en que el nodo A ya ha hecho la autenticación del usuario, el nodo B admite la petición del usuario sin exigirle la contraseña. Un intruso que sea capaz de entrar en un nodo puede por tanto entrar en todos los nodos que "confíen" en el nodo ya accedido.

También aparece diversa "fauna maligna" como "gusanos", mensajes de correo electrónico que se reproducen y acaban por colapsar la red; "caballos de Troya", programas aparentemente "inocuos" que llevan código escondido; virus, que se autocopian de un programa/documento "infectado" a otros programas/documentos "limpios"; "puertas falsas", accesos que muchas veces se quedan de la etapa de instalación/depuración de los sistemas.

18.5. AUDITANDO LA GERENCIA DE COMUNICACIONES

Cada vez más las comunicaciones están tomando un papel determinante en el tratamiento de datos, cumpliéndose el lema "el computador es la red" .

No siempre esta importancia queda adecuadamente reflejada dentro de la estructura, organizativa de proceso de datos, especialmente en organizaciones de tipo "tradicional", donde la adaptación a los cambios no se produce inmediatamente. Mientras que comúnmente el directivo informático tiene amplios conocimientos de proceso de datos, no siempre sus habilidades y cualificaciones en temas de comunicaciones están a la misma altura, por lo que el riesgo de deficiente anclaje de la gerencia de comunicaciones en el esquema organizativo existe. Por su parte, los informáticos a cargo de las comunicaciones suelen autoconsiderarse exclusivamente técnicos, obviando considerar las aplicaciones organizativas de su tarea.

Todos estos factores convergen en que la auditoría de comunicaciones no siempre se practique con la frecuencia y profundidad equivalentes a las de otras áreas del proceso de datos.

Por tanto, el primer punto de una auditoría es determinar que la función de gestión de redes y comunicaciones esté claramente definida, debiendo ser responsable, en general, de las siguientes áreas:

- Gestión de la red, inventario de equipamiento y normativa de conectividad.
- Monitorización de las comunicaciones, registro y resolución de problemas.
- Revisión de costes y su asignación de proveedores y servicios de transporte, balanceo de tráfico entre rutas y selección de equipamiento.
- Participación activa en la estrategia de proceso de datos, fijación de estándares a ser usados en el desarrollo de aplicaciones y evaluación de necesidades en comunicaciones.

Como objetivos del control, se debe marcar la existencia de:

- Una gerencia de comunicaciones con autoridad para establecer procedimientos y normativa.
- Procedimientos y registros de inventarios y cambios.
- Funciones de vigilancia del uso de la red de comunicaciones, ajustes de rendimiento, registro de incidencias y resolución de problemas.

- Procedimientos para el seguimiento del coste de las comunicaciones y su reparto a las personas o unidades apropiadas.

- Procedimientos para vigilar el uso de la red de comunicaciones, realizar ajustes para mejorar el rendimiento, y registrar y resolver cualquier problema.

- Participación activa de la gerencia de comunicaciones en el diseño de las nuevas aplicaciones *on line* para asegurar que se sigue la normativa de comunicaciones.

Lista de control

Comprobar que:

* G.1. La gerencia de comunicaciones despache con el puesto directivo que en el organigrama tenga autoridad suficiente para dirigir y controlar la función.

* G.2. Haya coordinación organizativa entre la comunicación de datos y la de voz, en casa de estar separadas estas dos funciones.

* G.3. Existan descripciones del puesto de trabajo, competencias, requerimientos y responsabilidades para el personal involucrado en las comunicaciones.

* G.4. Existan normas en comunicaciones al menos para las siguientes áreas:

    - Tipos de equipamiento, como adaptadores LAN, que pueden ser instalados en la red.

    - Procedimientos de autorización para conectar nuevo equipamiento en la red.

    - Planes y procedimientos de autorización para la introducción de líneas y equipos fuera de las horas normales de operación.

    - Procedimientos para el uso de cualquier conexión digital con el exterior, como línea de red telefónica conmutada o Internet.

    - Procedimientos de autorización para el uso de exploradores físicos (sniffers) y lógicos (traceadores).

- Control físico de los exploradores físicos (sniffers), que deben estar guardados.

- Control de qué máquinas tienen instalados exploradores lógicos (traceadores), y de que éstos sólo se pueden invocar por usuarios autorizados.

* G.5. Los contratos con transportistas de información y otros proveedores tienen definidas responsabilidades y obligaciones.

* G.6. Existan planes de comunicaciones a largo plazo, incluyendo estrategia de comunicaciones de voz y datos.

* G.7. Existen, si fueren necesarios, planes para comunicaciones a alta velocidad, como fibra óptica, ATM, etc.

* G. 8. Se planifican redes de cableado integral para cualquier nuevo edificio o dependencia que vaya a utilizar la empresa.

* G.9. El plan general de recuperación de desastres considera el respaldo y recuperación de los sistemas de comunicaciones.

* G.10. Las listas de inventario cubren todo el equipamiento de comunicaciones de datos, incluyendo módems, controladores, terminales, líneas y equipos relacionados.

* G.11. Se mantienen los diagramas de red que documentan las conexiones físicas y lógicas entre las comunicaciones y otros equipos de proceso de datos.

* G.12. Se refleja correctamente, en el registro de inventario y en los diagramas de red, una muestra seleccionada de equipos de comunicaciones, de dentro y de fuera de la sala de computadores.

* G.13. Los procedimientos de cambio para equipos de comunicaciones, así como para añadir nuevos terminales o cambios en direcciones, son adecuados y consistentes con otros procedimientos de cambio en las operaciones de proceso de datos.

* G.14. Existe un procedimiento formal de prueba que cubre la introducción de cualquier nuevo equipo o cambios en la red de comunicaciones.

* G.15. Para una selección de diversas altas o cambios en la red, de un período reciente, los procedimientos formales de control han sido cumplidos.

* G.16. Están establecidos ratios de rendimiento que cubren áreas como la de tiempos de respuesta en los terminales y tasas de errores.

* G.17. Se vigila la actividad dentro de los sistemas *on line* y se realizan los ajustes apropiados para mejorar el rendimiento.

* G.18. Existen procedimientos adecuados de identificación, documentación y toma de acciones correctivas ante cualquier fallo de comunicaciones.

* G.19. La facturación de los transportistas de comunicaciones y otros vendedores es revisada regularmente y los cargos con discrepancias se conforman adecuadamente.

* G.20. Existe un sistema comprensible de contabilidad y cargo en costes de comunicaciones, incluyendo líneas, equipos y terminales.

* G.21. Los gestores de comunicaciones están informados y participan en la planificación pre-implementación de los nuevos sistemas de información que puedan tener impacto en las comunicaciones.

* G.22. Las consideraciones de planificación de capacidad en comunicaciones son tomadas en cuenta en el diseño e implementación de nuevas aplicaciones.

18.6. AUDITANDO LA RED FÍSICA

En una primera división, se establecen distintos riesgos para los datos que circulan dentro del edificio de aquellos que viajan por el exterior. Por tanto, ha de auditarse hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes.

En general, muchas veces se parte del supuesto de que si no existe acceso físico desde el exterior a la red interna de una empresa las comunicaciones internas quedan a salvo. Debe comprobarse que efectivamente los accesos físicos provenientes del exterior han sido debidamente registrados, para evitar estos accesos. Debe también comprobarse que desde el interior del edificio no se intercepta físicamente el cableado ("pinchazo").

En caso de desastre, bien sea total o parcial, ha de poder comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar. Ya que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencias deben tener prevista la recuperación en comunicaciones.

Ha de tenerse en cuenta que la red física es un punto claro de contacto entre la gerencia de comunicaciones y la gerencia de mantenimiento general de edificios, que es quien suele aportar electricistas y personal profesional para el tendido físico de cables y su mantenimiento.

Como objetivos de control, se debe marcar la existencia de:

- Áreas controladas para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones, para evitar accesos físicos.
- Controles de utilización de los equipos de pruebas de comunicaciones, usados para monitorizar la red y su tráfico, que impidan su utilización inadecuada.
- Atención específica a la recuperación de los sistemas de comunicación de datos en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o a la red.

Lista de control

Comprobar que:

* F. 1. El equipo de comunicaciones se mantiene en habitaciones cerradas con acceso limitado a personas autorizadas.

* F.2. La seguridad física de los equipos de comunicaciones, tales como controladores de comunicaciones, dentro de las salas de computadores sea adecuada.

* F.3. Sólo personas con responsabilidad y conocimientos están incluidas en la lista de personas permanentemente autorizadas para entrar en las salas de equipos de comunicaciones.

* F.4. Se toman medidas para separar las actividades de electricistas y personal de tendido y mantenimiento de tendido de líneas telefónicas, así como sus autorizaciones de acceso, de aquéllas del personal bajo control de la gerencia de comunicaciones.

* F.5. En las zonas adyacentes a las salas de comunicaciones, todas las líneas de comunicaciones fuera de la vista.

* F.6. Las líneas de comunicaciones, en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos, estarán etiquetadas con un código gestionado por la gerencia de comunicaciones, y no por su descripción física o métodos sin coherencia.

* F.7. Existen procedimientos para la protección de cables y bocas de conexión que dificulten el que sean interceptados o conectados por personas no autorizadas.

* F.8. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.

* F.9. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicación de datos deben tener propósitos y funciones definidos.

* F.10. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitorizar líneas y fijar problemas incluyendo:

  - Procedimiento restringiendo el uso de estos equipos a personal autorizado.
  - Facilidades de traza y registro del tráfico de datos que posean los equipos de monitorización.
  - Procedimientos de aprobación y registro ante las conexiones a líneas de comunicaciones en la detección y corrección de problemas.

* F.11. En el plan general de recuperación de desastres para servicios de información presta adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.

* F.12. Existen planes de contingencia para desastres que sólo afecten a las comunicaciones, como el fallo de una sala completa de comunicaciones.

* F. 13. Las alternativas de respaldo de comunicaciones, bien sea con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.

* F.14. Las líneas telefónicas usadas para datos, cuyos números no deben ser públicos, tienen dispositivos/procedimientos de seguridad tales como retrollamada, códigos de conexión o interruptores para impedir accesos no autorizados al sistema informático.

18.7. AUDITANDO LA RED LÓGICA

Cada vez más se tiende a que un equipo pueda comunicarse con cualquier otro equipo, de manera que sea la red de comunicaciones el substrato común que les une. Leído a la inversa, la red hace que un equipo pueda acceder legítimamente a cualquier otro, incluyendo al tráfico que circule hacia cualquier equipo de la red. Y todo ello por métodos exclusivamente lógicos, sin necesidad de instalar físicamente ningún dispositivo. Simplemente si un equipo, por cualquier circunstancia, se pone a enviar indiscriminadamente mensajes, puede ser capaz de bloquear la red completa y, por tanto, al resto de los equipos de la instalación.

Es necesario monitorizar la red, revisar los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala. En general, si se quiere que la información que viaja por la red no pueda ser espiada, la única solución totalmente efectiva es la encriptación.

Como objetivos de control, se debe marcar la existencia de:

- Contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado a la red de comunicaciones.

- Facilidades de control de errores para detectar errores de transmisión y establecer las retransmisiones apropiadas.

- Controles para asegurar que las transmisiones van solamente a usuarios autorizados y que los mensajes no tienen por qué seguir siempre la misma ruta.

- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a transmisiones sensibles.

- Controles adecuados que cubran la importación o exportación de datos a través de puertas, en cualquier punto de la red, a otros sistemas informáticos.

Lista de control

Comprobar que:

* L.1. El software de comunicaciones, para permitir el acceso, exige código de usuario y contraseña.

* L.2. Revisar el procedimiento de conexión de usuario y comprobar que:

  - Los usuarios no pueden acceder a ningún sistema, ni siquiera de ayuda, antes de haberse identificado correctamente.

  - Se inhabilita al usuario que sea incapaz de dar la contraseña después de un número determinado de intentos infructuosos.

  - Se obliga a cambiar la contraseña regularmente.

  - Las contraseñas no son mostradas en pantalla cuando se teclean.

  - Durante el procedimiento de identificación, los usuarios son informados de cuándo fue su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados.

* L.3. Cualquier procedimiento del fabricante, mediante hardware o software, que permita el libre acceso y que haya sido utilizado en la instalación original, ha de haber sido inhabilitado o cambiado.

* L.4. Se toman estadísticas que incluyan tasas de errores y de retransmisión.

* L.5. Los protocolos utilizados, revisados con el personal adecuado de comunicaciones, disponen de procedimientos de control de errores con la seguridad suficiente.

* L.6. Los mensajes lógicos transmitidos identifican el originante, la fecha, la hora y el receptor.

* L.7. El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdidos, o retrasados.

* L.8. La arquitectura de comunicaciones utiliza indistintamente cualquier ruta disponible de transmisión para minimizar el impacto de una escucha de datos sensibles en una ruta determinada.

* L.9. Existen controles para que los datos sensibles sólo puedan ser impresos en las impresoras designadas y vistos desde los terminales autorizados.

* L.10. Existen procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

* L.11. Los archivos de registro son revisados, si es posible a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso.

* L.12. Existen análisis de riesgos para las aplicaciones de proceso de datos a fin de identificar aquellas en las que el cifrado resulte apropiado.

* L.13. Si se utiliza cifrado:

  - Existen procedimientos de control sobre la generación e intercambio de claves.
  - Las claves de cifrado son cambiadas regularmente.
  - El transporte de las claves de cifrado desde donde se generan a los equipos que las utilizan sigue un procedimiento adecuado.

* L.14. Si se utilizan canales de comunicación uniendo diversos edificios de la misma organización, y existen datos sensibles que circulen por ellos, comprobar que estos canales se cifran automáticamente, para evitar que una interceptación sistemática a un canal comprometa a todas las aplicaciones.

* L.15. Si la organización tiene canales de comunicación con otras organizaciones se analice la conveniencia de cifrar estos canales.

* L.16. Si se utiliza la transmisión de datos sensibles a través de redes abiertas como Internet, comprobar que estos datos viajan cifrados.

* L.17. Si en una red local existen computadores con módems, se han revisado los controles de seguridad asociados para impedir el acceso de equipos foráneos a la red local.

* L.18. Existe una política de prohibición de introducir programas personales o conectar equipos privados a la red local.

* L.19. Todas las "puertas traseras" y accesos no específicamente autorizados están bloqueados. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc., esto significa que los accesos para servicio remoto están inhabilitados o tienen procedimientos específicos de control.

* L.20. Periódicamente se ejecutan, mediante los programas actualizados y adecuados, ataques para descubrir vulnerabilidades, que los resultados se documentan y se corrigen las deficiencias observadas. Estos ataques deben realizarse independientemente a:

  - Servidores, desde dentro del servidor.
  - Servidores, desde la red interna.
  - Servidores Web, específicamente.
  - Intranet, desde dentro de ella.
  - Cortafuegos, desde dentro de ellos.
  - Accesos desde el exterior y/o Internet.

18.8. LECTURAS RECOMENDADAS

Andrew S. Tanenbaum. *Redes de computadores*. Prentice-Hall. Es el libro de referencia, por antonomasia, en comunicaciones.

Varios. *COAST. Computer Operations, Audit and Security Technology*. http://www.cs.purdue.edu/coast Un actualizado compendio de conocimientos sobre el tema, con hiperenlaces a lo más significativo del sector.

Steven L. Telleen. *Intranet Organization: Strategies for managing change*. Intranet Partners. http://www.intranetpartners.com/IntranetOrg. Enfoque muy orientado a la práctica empresarial cotidiana.

18.9. CUESTIONES DE REPASO

1. ¿Cuáles son los niveles del modelo OSI?
2. ¿Cuáles son las incidencias que pueden producirse en las redes de comunicaciones?
3. ¿Cuáles son los mayores riesgos que ofrecen las redes?
4. ¿Existe el riesgo de que se intercepte un canal de comunicaciones?
5. ¿Qué suele hacerse con las contraseñas de los usuarios?
6. ¿Cuáles son los protocolos más importantes de alto nivel?
7. Diferencias entre Internet, Intranet y Extranet.
8. ¿Qué es un "cortafuegos"?
9. ¿Qué es un "gusano"?
10. ¿Qué objetivos de control destacaría en la auditoría de la gerencia de comunicaciones?

CAPÍTULO 19

AUDITORÍA DE APLICACIONES

José María Madurga Oteiza

19.1. INTRODUCCIÓN

Qué duda cabe que una meticulosa y exhaustiva auditoría de una aplicación informática de relevancia en una empresa o entidad podría dar pie para poner en funcionamiento la práctica totalidad de la extensa gama de técnicas y rica metodología de la auditoría informática.

Debo, por tanto, aclarar de partida el alcance de este trabajo dentro del contexto de la obra en que se integra: al contar con capítulos específicos dedicados a numerosos aspectos técnicos y al resto de etapas de la vida de un sistema, incluso a su explotación y mantenimiento, mi exposición *se va a centrar en la fase final de la vida de la aplicación informática, la de su funcionamiento ordinario,* una vez superada la crítica etapa de su implantación, que habrá cerrado el ciclo precedido por las de concepción y desarrollo.

También he de confesar mi propósito de que prime la recopilación de experiencias recogidas en los trabajos de este tipo que he tenido ocasión de dirigir, sobre el rigor de una recapitulación de estándares de objetivos de control, que pueden ser localizados sin dificultad a través de numerosas fuentes. Dichas experiencias se han desenvuelto en aplicaciones de gran envergadura y complejidad: utilizadas por un considerable número de usuarios, con gran dispersión geográfica, diversidad de plataformas y compleja red de comunicaciones, lo que debiera haber permitido aflorar mayor número de problemas a tener en cuenta y a los que dar solución.

Así pues, el objeto de este trabajo consiste en *tratar de ayudar a planificar, preparar y llevar a cabo auditorías de aplicaciones en funcionamiento en cuanto al*

grado de cumplimiento de los objetivos para los que las mismas fueron creadas: con carácter general, éstos estarán en la línea de servir de eficaces herramientas operativas y de gestión que potencien la más eficiente contribución, por parte de las organizaciones usuarias de las aplicaciones, a la consecución de los objetivos generales de la empresa, grupo o entidad a la que pertenecen.

19.2. PROBLEMÁTICA DE LA AUDITORÍA DE UNA APLICACIÓN INFORMÁTICA

Una aplicación informática o sistema de información habitualmente persigue como finalidad:

- Registrar fielmente la información considerada de interés en torno a las operaciones llevadas a cabo por una determinada organización: magnitudes físicas o económicas, fechas, descripciones, atributos o características, identificación de las personas físicas y/o jurídicas que intervienen o guardan relación con cada operación, nombres, direcciones, etc.

- Permitir la realización de cuantos procesos de cálculo y edición sean necesarios a partir de la información registrada, pudiendo, por tanto, almacenar automáticamente más información que la de partida, aunque siempre basada en aquélla.

- Facilitar, a quienes lo precisen, respuesta a consultas de todo tipo sobre la información almacenada, diseñadas en contenido y forma para dar cobertura a las necesidades más comunes constatadas.

- Generar informes que sirvan de ayuda para cualquier finalidad de interés en la organización, presentando la información adecuada: se aplican –según convenga– criterios de selección, ordenación, recuento y totalización por agrupamientos, cálculos de todo tipo, desde estadísticos comunes (media, desviación típica, valores mínimo, máximo, primero y último, etc.), hasta los más sofisticados algoritmos.

Si este planteamiento se consigue trasladar con rigor a una aplicación informática y los usuarios la manejan con soltura y con profesionalidad, la organización a la que pertenecen contará con un importante factor de éxito en el desarrollo de su actividad.

Sin embargo, ni el rigor en la creación de la aplicación ni la profesionalidad en el uso de la misma pueden ser garantizados. Además la profesionalidad no inmuniza contra el cansancio y el estrés. Asumido está también que de humanos es equivocarse, cometer errores y omisiones involuntariamente. Y tampoco es imposible que en un

momento determinado un empleado descontento cometa errores intencionadamente o que otro, en apuros económicos, sucumba a la tentación de intentar un fraude perfecto si considera mínima la probabilidad de ser descubierto, tal y como funciona el sistema y la organización, que puede no estar dando muestras de ejercer un control interno riguroso.

Y no son éstas las únicas amenazas al normal cumplimiento de la finalidad de nuestra aplicación:

- La posibilidad de fallo en cualquiera de los elementos que intervienen en el proceso informático: software múltiple perteneciente a diferentes firmas, computador central y dispositivos periféricos, transmisión de datos (servidores, módems, líneas de comunicaciones, etc.) constituye otra fuente de posibles riesgos.

- La conexión cada vez más generalizada de las empresas a entornos abiertos como la Internet multiplica los riesgos que amenazan la confidencialidad e integridad de la información de nuestros sistemas. Y en este caso el número de interesados en descubrir debilidades que les abran las puertas para enredar y manipular la información a la que sean capaces de acceder no tiene límites.

Todas esas amenazas y cualquier otra que pueda ser identificada contra el correcto funcionamiento de nuestra aplicación y la consecución de sus objetivos, han debido ser objeto de un análisis minucioso ya desde la fase de su concepción. Para cada una de ellas se habrán debido estudiar las posibles medidas tendentes a eliminar los riesgos que entrañan o, cuando menos, a reducir la probabilidad de su materialización hasta niveles razonablemente asumibles, siempre teniendo en cuenta el costo de tales medidas (que no cuesten más las cintas que el manto, según el dicho popular).

Dichas medidas son fundamentalmente medidas de control interno que, con carácter general, consisten en los procedimientos para verificar, evaluar y tratar de garantizar que "todo" funciona como se espera: de acuerdo con las políticas, directrices, normas y procedimientos establecidos en los diferentes ámbitos de responsabilidad.

En el terreno de una aplicación informática, el control interno se materializa fundamentalmente en controles de dos tipos:

- ***Controles manuales***: a realizar normalmente por parte de personal del área usuaria: actuaciones previstas para asegurar que –en su caso– se preparan, autorizan y procesan todas las operaciones, se subsanan adecuadamente todos los errores, son coherentes los resultados de salida respecto a referencias disponibles sobre los datos de entrada, y las bases de datos que dan soporte a la aplicación mantienen en los niveles debidos diferentes indicadores de

medición de su integridad y totalidad (número de registros en archivos y/o tablas, de relaciones o índices, totales de magnitudes numéricas, conciliaciones, etc.).

- ***Controles automáticos***: incorporados a los programas de la aplicación que sirvan de ayuda para tratar de asegurar que la información se registre y mantenga completa y exacta, los procesos de todo tipo sobre la misma sean correctos y su utilización por parte de los usuarios respete los ámbitos de confidencialidad establecidos y permita poner en práctica principios generales de control interno como el referente a la segregación de funciones.

Controles que, según su finalidad, se suelen clasificar en:

- **Controles preventivos:** Tratan de ayudar a evitar la producción de errores a base de exigir el ajuste de los datos introducidos a patrones de formato y estructura (dato numérico, fecha válida, etc.), pertenencia a una lista de valores válidos o a un archivo maestro, rango entre límites determinados, incorporación de dígitos de control en datos clave (códigos de identificación, referencias de documentos, nomenclaturas, etc.) y, en general, cualquier criterio que ayude a asegurar la corrección formal y verosimilitud de los datos (la exactitud sólo puede garantizarla el usuario).

  Son de gran utilidad las comprobaciones de conjuntos de datos, buscando su compatibilidad, adecuación y coherencia (por ejemplo, una cuenta de cargo puede no ser compatible con un tipo de instalación).

- **Controles detectivos:** Tratan de descubrir a posteriori errores que no haya sido posible evitar.

- **Controles correctivos:** Tratan de asegurar que se subsanen todos los errores identificados mediante controles detectivos.

Y que pueden ser utilizados:

- En las transacciones de recogida o toma de datos.
- En todos los procesos de información que la aplicación realiza.
- En la generación de informes y resultados de salida.

Pues bien, como apuntábamos hace un momento, ya en el diseño de la aplicación se debió hacer un estudio a conciencia para seleccionar de entre los posibles, y teniendo en cuenta su costo frente a su previsible efectividad contra el riesgo que trata de contrarrestar, los controles considerados idóneos para cada situación planteada en los diferentes pasos de funcionamiento de la aplicación.

Este estudio debió ser propuesto por los responsables del área informática -contando siempre en el diseño con la participación de representantes de la organización usuaria-, *revisado por personal de auditoría interna,* y aprobado en última instancia por la dirección de la organización usuaria, máxima responsable de la aplicación.

Es importante recalcar la conveniencia de la participación de Auditoría interna (con un carácter más general que Auditoría informática) en la revisión de los controles diseñados durante el desarrollo de la aplicación. Sus recomendaciones deben ser consideradas -aunque la decisión final en caso de discrepancia debe radicar en la organización usuaria-. Lo que está fuera de toda duda es que sería tremendamente más costoso, tener que incluir cualquier control una vez finalizado el desarrollo, como modificación, porque se pusiera de manifiesto su necesidad como resultado de una auditoría posterior a la implementación.

La participación de Auditoría interna en el desarrollo de un sistema informático debe tener un alcance más amplio que el referente al sistema informático, ya que debe contemplar no sólo los riesgos relacionados con la aplicación, sino todos los que puedan afectar al proceso completo al que la misma sirve de Herramienta, pudiendo proponer: que la aplicación registre información específica, **"pistas de auditoría",** para facilitar la futura auditabilidad del proceso respecto a tales riesgos. Lo mismo cabe decir, en cuanto al requerimiento de pistas de auditoría, para facilitar las futuras auditorías informáticas de la aplicación.

Después de lo expuesto, podemos centrar la problemática de la auditoría de una aplicación: se trata de realizar una **revisión de la eficacia del funcionamiento de los controles diseñados para cada uno de los pasos de la misma frente a los riesgos que, tratan de eliminar o minimizar,** como medios *para asegurar la fiabilidad (totalidad y exactitud), seguridad, disponibilidad y confidencialidad de la información gestionada por la aplicación.*

Ello obliga a replantearse nuevamente, y con carácter previo, si los propios riesgos tenidos en cuenta en su momento son todos los posibles o se detectan otros nuevos: unos y otros deben ser evaluados, analizada la probabilidad de su materialización y sus consecuencias previsibles, de cara a reconsiderar si los controles implantados, tal como están actuando, superan con garantías de éxito la exposición a amenazas percibida en la situación actual.

Quede bien entendido que, por muy completa que resulte la revisión que hagamos de una aplicación informática y de los controles que incorpora, no es suficiente para garantizar la seguridad de la misma: ésta se consolida con la realización de una evaluación de los controles generales y una revisión de los controles de la función informática, que estarán recogidos en el Plan de trabajos de auditoría informática.

19.3. HERRAMIENTAS DE USO MÁS COMÚN EN LA AUDITORÍA DE UNA APLICACIÓN

Antes de nada conviene hacer hincapié en que la tremenda evolución de las tecnologías, en todo lo referente a los sistemas de información, obliga a un esfuerzo considerable de formación a todo el personal de auditoría interna, y en particular a los especialistas en auditoría informática. Este reto debe estar asumido por la dirección de Auditoría, que debe impulsar la respuesta adecuada al mismo, recogida en un ambicioso **plan de formación**, que incluya la atención a las nuevas tendencias y preocupaciones.

Ello no es óbice para que, dentro de la política de la empresa, se contemple la posibilidad de contratar la realización de determinadas auditorías informáticas muy especializadas *(outsourcing)* o personal auditor que participe en trabajos; pero siempre será conveniente que la dirección de todos los trabajos sea conducida, y con suficiente conocimiento general aun en los temas más especializados, por auditores de la propia empresa.

Haremos un recorrido por las herramientas más comúnmente utilizadas en la auditoría de la aplicación informática dentro del contexto que hemos delimitado en la introducción.

En ocasiones se podrán combinar varias a la vez; por ejemplo se puede, en una entrevista con otro propósito, aprovechar la ocasión para realizar una prueba de conformidad prevista, además de observar la utilización de la aplicación por el entrevistado e incluso, si éste estuviera interesado, rellenar o comentar una encuesta que se le había dirigido.

19.3.1. Entrevistas

De amplia utilización a lo largo de todas las etapas de la auditoría, las entrevistas deben cumplir una serie de requisitos:

- Las personas a entrevistar deben ser aquellas que más puedan aportar al propósito pretendido.
- La entrevista debe ser preparada con rigor de cara a sacar el máximo partido de ella.
- Para ello es indispensable escribir el guión de temas y apartados a tratar (no un cuestionario cerrado), para evitar que quede sin tratar algún asunto de interés;

también exige haber alcanzado el nivel de conocimientos sobre la aplicación necesario en ese momento para conducir con soltura la entrevista.

- Ha de ser concertada con los interlocutores con antelación suficiente, informándoles del motivo y las materias a tratar en ella, la duración aproximada prevista y, en su caso, solicitando la preparación de la documentación o información que pueda ser necesario aporten durante la misma; no debe faltar la invitación a colaborar con cuantas sugerencias estimen oportuno, no sólo sobre el propio objeto de la entrevista sino también con miras más amplias en relación con el proceso global desarrollado por la organización y la aplicación informática que apoya el proceso.

- Las jefaturas de las personas a entrevistar deben estar informadas de las actuaciones previstas; en general será positivo que sea el propio jefe quien comunique al interesado la necesidad de participar en la auditoría.

- Durante el desarrollo de la entrevista, el auditor tomará las anotaciones imprescindibles; lo más próximo posible a la finalización de la entrevista el auditor debe repasar sus anotaciones, completando con detalles que pueda recordar aquellas que pudieran haber quedado esbozadas, y reflexionando sobre las posibles implicaciones de las novedades o singularidades que el interlocutor haya podido aportar.

19.3.2. Encuestas

Pueden ser de utilidad tanto para ayudar a determinar el alcance y objetivos de la auditoría como para la materialización de objetivos relacionados con el nivel de satisfacción de los usuarios.

Con las lógicas salvedades, la mayor parte de los requisitos enumerados para las entrevistas son también de aplicación para las encuestas.

- En este caso, sin embargo, sí que hay que preparar un cuestionario que pueda ser contestado con la mayor rapidez a base de marcar las respuestas entre las posibles.

- Conviene que todas las preguntas vayan seguidas de un espacio destinado a observaciones, y no sólo las que soliciten descripción cuando la respuesta haya podido ser "Otros", caso de elección entre varias alternativas. Al final del cuestionario hay que solicitar sugerencias u observaciones abiertas, mejor en página exclusiva para ello, que pueda ser fotocopiada por quienes necesiten más espacio para sus comentarios.

- Aunque no puede ni debe exigirse la identificación personal del encuestado, sí debe hacerse de la organización a la que pertenece (Cuidado con los recuentos de resultados de la encuesta por organización que pudieran quedar con una única respuesta: no deben ser obtenidos, limitando, por tanto, la obtención de tales recuentos a la condición de contar con más de una respuesta en el agrupamiento.) Sin embargo, sí puede invitarse a que se identifique quien no tenga ningún inconveniente en ello, lo que permitiría contactos enriquecedores si la encuesta contestada plantea asuntos de interés.

19.3.3. Observación del trabajo realizado por los usuarios

Aunque por otros medios puede llegarse a comprobar que la aplicación funciona con garantías de exactitud y fiabilidad, es conveniente observar cómo algún usuario hace uso de aquellas transacciones más significativas por su volumen o riesgo: puede ayudar a detectar que, aunque el resultado final sea bueno y, por tanto, los controles establecidos sean efectivos, la eficiencia no esté en el nivel óptimo; no es infrecuente que un auditor experimentado identifique mejoras en este tipo de observaciones: desde carencias del usuario o vicios adquiridos que pueden denotar falta de formación, hasta mejoras de diseño que puedan aumentar la agilidad y productividad en el uso de la aplicación: recomendaciones de opciones o valores propuestos por defecto, simplificación de pasos, etc.

Debe aprovecharse esta oportunidad para probar también la efectividad de los controles de las transacciones en cuestión, solicitando la simulación de situaciones previsibles de error para comprobar si la respuesta del sistema es la esperada: intento de duplicar una operación real, de cometer errores de diferentes tipos en la introducción de cada uno de los datos, etc.

19.3.4. Pruebas de conformidad

De uso general en todo el campo de la auditoría, son actuaciones orientadas específicamente a comprobar que determinados procedimientos, normas o controles internos, particularmente los que merecen confianza de estar adecuadamente establecidos, se cumplen o funcionan de acuerdo con lo previsto y esperado, según lo descrito en la documentación oportuna.

La comprobación debe llevar a la evidencia a través de la inspección de los resultados producidos: registros, documentos, conciliaciones, etc. y/u observación directa del funcionamiento de un control ante pruebas específicas de su comportamiento.

- La evidencia de incumplimiento puede ser puesta de manifiesto a través de informes de excepción.

- Los testimonios de incumplimiento no implican evidencia pero, si parten de varias personas, es probable que la organización asuma como válidos dichos testimonios y, por tanto, las consecuencias que de los mismos pudieran derivarse de cara a posibles recomendaciones, ahorrando esfuerzos para tratar de conseguir su confirmación documental.

19.3.5. Pruebas substantivas o de validación

Orientadas a detectar la presencia o ausencia de errores o irregularidades en procesos, actividades, transacciones o controles internos integrados en ellos.

También pertenecen al dominio general de la auditoría.

Están especialmente indicadas en situaciones en las que no hay evidencia de que existan controles internos relevantes, suficientes como para garantizar el correcto funcionamiento del proceso o elemento considerado.

- Todo tipo de error o incidencia imaginable puede ser objeto de investigación en esta clase de pruebas. En el ámbito de la auditoría de una aplicación informática, irregularidades de diversa índole que pueden afectar a las transacciones:

  - Transacciones omitidas, no registradas en el sistema.
  - Duplicadas, registradas más de una vez.
  - Inexistentes indebidamente incluidas.
  - Registradas sin contar con las autorizaciones establecidas.
  - Incorrectamente clasificadas o contabilizadas en cuentas diferentes a las procedentes.
  - Transacciones con información errónea, desde su origen o por alteración posterior, que no refleja la realidad, con posibles consecuencias en:

    - El montante o fechas de devengo incorrectas de derechos y obligaciones de la empresa respecto a terceros.
    - La exactitud de las valoraciones contables o la falta de conciliación con ellas de la contenida en la Aplicación.
    - La exactitud de las mediciones físicas, con posible desajuste respecto a inventarias.

- Infinidad de recursos pueden ser utilizados para detectar indicios, en primera instancia, de posibles errores; indicios cuya presencia deberá llevar a profundizar en la investigación para constatar la existencia real de anomalías. Muchos de ellos se apoyan en la utilización del computador:

  - Análisis de ratios, así como fluctuaciones y tendencias en magnitudes que miden aspectos relacionados con la actividad desarrollada en los procesos.

  - Conciliaciones con partidas que a efectos de control puedan llevarse en la propia aplicación o de otros sistemas, como el económico-financiero.

  - Informes de excepción producidos por la propia aplicación para identificar situaciones que interesa sean objeto de revisión. Aparte de los de obtención rutinaria previstos en el sistema, debiera disponerse de otros específicos para la realización de auditorías, planteados desde la etapa de diseño para poder ejecutar a demanda.

- Otros recursos clásicos utilizados para la detección de errores o sus indicios son de ejecución manual. Normalmente se aplican sobre muestras, estadísticas y no estadísticas.

  - Para las primeras evidentemente son de aplicación las técnicas de muestreo estadístico, que deberán ser respetadas para el cálculo del tamaño de las muestras y su selección en función del nivel de significación y error máximo con que interese trabajar en cada caso.

  - Las muestras no estadísticas, dirigidas, basarán la selección en la búsqueda de las operaciones con mayor probabilidad de error y/o consecuencias más graves, previo análisis de las condiciones de la información disponible que permitan componer un indicador de priorización, asignando puntuaciones al cumplimiento de determinadas condiciones.

- Ejemplos de estos recursos de ejecución manual son: Arqueo, Inventario, Inspección, Comprobación con los documentos soporte de la transacción (factura, albarán, etc.) y Confirmación de saldos por parte de terceros (clientes y proveedores).

19.3.6. Uso del computador

- El uso de computadores constituye una de las herramientas más valiosas en la realización de la auditoría de una aplicación informática. Nos referimos tanto a los computadores personales, con los que el auditor informático debe estar

familiarizado manejando con soltura las técnicas de edición de textos y presentaciones, hoja de cálculo, gestor de bases de datos, correo electrónico, etc., como al computador u computadores sobre los que se explota la aplicación objeto de la auditoría.

- Existen en el mercado infinidad de productos de software concebidos para facilitar la tarea del auditor: Herramientas que permiten el acceso generalizado a la información contenida en archivos y bases de datos de forma transparente para el usuario y con independencia de las características de organización y modo de almacenamiento. Muchos de estos productos se presentan como "herramientas de auditoría", ya que incorporan facilidades típicas de esta función como pueden ser la generación de muestras estadísticas, edición de circularizaciones, etc.

- Sin restar su valor a estos productos, y desde la óptica del auditor interno, se pueden obtener resultados similares haciendo uso de herramientas disponibles en la organización y no necesariamente diseñadas para funciones de auditoría. Contando con una herramienta de interrogación, un lenguaje SQL *(Structured Query Language)*, se puede acceder a la información y seleccionar la que interese; su proceso posterior a través de un gestor de base de datos, tipo ACCESS o similar, ofrece un potencial de tratamiento prácticamente ilimitado.

- Las pistas de auditoría de que esté provista la aplicación deben constituir un apoyo importante a la hora de utilizar el computador para detectar situaciones o indicios de posible error. Lo mismo cabe decir de los informes de excepción, particularmente los diseñados específicamente para propósitos de auditoría.

- También hay que considerar la posibilidad de utilizar la propia aplicación, aplicando juegos de ensayo o transacciones ficticias preparadas por los auditores, para verificar la eficacia de los controles implantados. Este tipo de pruebas no es siempre recomendable, sobre todo si no ha sido prevista tal contingencia durante la etapa de diseño de la aplicación.

19.4. ETAPAS DE LA AUDITORÍA DE UNA APLICACIÓN INFORMÁTICA

19.4.1. Recogida de información y documentación sobre la aplicación

Antes de plantearnos el alcance de los trabajos de auditoría sobre aplicaciones informáticas necesitamos disponer de un conocimiento básico de la aplicación y de su entorno. Realizamos un estudio preliminar en el que recogemos toda aquella información que nos pueda ser útil para determinar los puntos débiles existentes y aquellas funciones de la aplicación que puedan entrañar riesgos.

A través de entrevistas con personal de los equipos responsables de la aplicación, tanto desde la organización usuaria como de la de Sistemas de Información, se inicia el proceso de recopilación de información y documentación que permitirá profundizar en su conocimiento hasta los niveles de exigencia necesarios para la realización del trabajo; y en una primera fase, hasta el nivel de aproximación suficiente para estar en disposición de establecer y consensuar los objetivos concretos de la auditoría.

El primer reto con el que nos encontramos es el de identificar las personas más adecuadas, en cada uno de los ámbitos de organización, para poder transmitir al responsable de la auditoría el conocimiento más amplio posible de la aplicación, sus fortalezas, posibles debilidades, riesgos e inquietudes suscitadas en torno a ella.

Identificadas dichas personas se intenta crear un ambiente de colaboración, con el fin de que transmitan al equipo auditor su visión personal de la situación, aportando cuantas sugerencias estimen de interés, además de suministrar la documentación que se les solicite y estén en disposición de proporcionar.

Para cubrir esta etapa del trabajo de auditoría resulta útil confeccionar unas guías que nos permitan seguir una determinada pauta en las primeras entrevistas y contengan la relación de documentos a solicitar todos aquellos que ayuden a:

- Adquirir una primera visión global del sistema: Descripción general de la aplicación, presentaciones que hayan podido realizarse de la aplicación con distintas finalidades a lo largo de su vida, Plan de Sistemas de la empresa, en lo que respecta a la aplicación a auditar; en él deberán figurar explícitamente sus objetivos, planes y presupuestos. (Un documento de gran trascendencia por su repercusión en la eficacia en el uso de la aplicación es el **"Manual de usuario"**: Concebido como soporte a la formación en el uso de la aplicación informática, debe ser claro, completo y estar bien estructurado para facilitar su

consulta. Es fundamental que esté actualizado al día y en mi opinión imprescindible que los usuarios puedan acceder a él a través de la red.)

- Conocer la organización y los procedimientos de los servicios que utilizan la aplicación. Mediante el examen de lista de personas o dichos servicios, organigrama de los mismos y dependencias funcionales entre ellos, bases de la organización y de la separación de funciones, grado de participación de los usuarios en el desarrollo y en las pruebas de la aplicación, medidas generales de control (protección física, protección lógica), política de formación y sensibilización de los usuarios, grado de satisfacción de los usuarios, etc.

- Describir el entorno en el que se desarrolla la aplicación: conocer recursos de computador central asignados, número de mini o micro computadores asignados total o parcialmente a la aplicación, cantidad de recursos periféricos asignados, configuración de la red y de las líneas de comunicaciones usadas, etc.

- Entender el entorno de software básico de la aplicación, identificando las seguridades que ofrece y los riesgos inducidos.

- Asimilar la arquitectura y características lógicas de la aplicación. Es necesario conocer los principales tratamientos y cómo están estructurados los datos: programas clave de la aplicación, lenguaje y método de programación, archivos maestros, bases de datos y diccionario de datos, modo de captura, de validación y de tratamiento de los datos, informes (listados) generados por la aplicación, así como la periodicidad de los diferentes tratamientos.

- Conocer las condiciones de explotación de la aplicación y los riesgos que se pueden dar. Es decir, si la aplicación la explotan directamente los usuarios o depende de los servicios informativos, volumen de capturas, volumen de información almacenada en los archivos maestros, seguridades de explotación (accesos, salvaguardias, etc.), planificación y organización general de la explotación, características generales; tiempos de respuesta, frecuencia y naturaleza de las incidencias, duración de los procesos *batch*.

- Conocer las condiciones de seguridad de que dispone la aplicación: controles que incorpora, definición de perfiles de acceso a los recursos y a la aplicación, existencia de pistas de auditoría, grado de automatización (mínima intervención humana), documentación.

- Disponer de información relativa a: Estadísticas de tiempos de explotación para cada proceso, de tiempos de respuesta de transacciones on line, de tiempos de reproceso por fallos o errores, tiempos dedicados al mantenimiento, informes de gestión de los accesos, informes de seguimiento

de las salidas, protecciones de los recursos asignados a la aplicación, perfiles de acceso a los recursos de la aplicación.

Resulta conveniente que el auditor solicite los documentos formalmente, facilitando su relación, y que éstos le sean suministrados en soporte informática en la medida de lo posible.

Hemos citado explícitamente sólo unos cuantos documentos, por problemas de espacio, relacionando los lugares comunes que deben cubrir. Adicionalmente cualquier informe, comunicación o acta de grupos de trabajo que puedan estar implicados en tareas de reingeniería de procesos, círculos de calidad, mejora permanente o cualquier otra iniciativa innovadora en el área de negocio a la que sirve la aplicación, serán de gran utilidad para el auditor en su cometido. Procederá en estos casos contactar con los responsables de tales proyectos, para potenciar las sinergias que surgirán, enriqueciendo los resultados de todos.

19.4.2. Determinación de los objetivos y alcance de la auditoría

El examen de los documentos recopilados y la revisión de los temas tratados a lo largo, de las entrevistas mantenidas, es decir, las observaciones tras el examen preliminar, la identificación de los puntos débiles y las funciones críticas, deben permitirle al auditor establecer su propuesta de objetivos de la auditoría de la aplicación y un plan detallado del trabajo a realizar. Entendemos que dedicando más recursos cuanto mayor fuera la debilidad o más graves las consecuencias de la amenaza que se somete a revisión.

Es de desear que los objetivos propuestos sean consensuados con el equipo responsable de la aplicación en la organización usuaria.

Es preciso conseguir una gran claridad y precisión en la definición de los objetivos de la auditoría y del trabajo y pruebas que se propone realizar, delimitando perfectamente su alcance de manera que no ofrezcan dudas de interpretación.

En la preparación del plan de trabajo trataremos de incluir:

- **La planificación de los trabajos y el tiempo a emplear,** orden en que se examinarán los diferentes aspectos, centros de trabajo en que se van a desarrollar las pruebas, cargas de tiempos y asignación de los trabajos entre los diferentes colaboradores del equipo.

- **Las herramientas y métodos,** entrevistas con los usuarios y los informáticos, servicios que se van a auditar, documentos que hay que obtener, etc.

- **El programa de trabajo detallado,** adaptado a las peculiaridades de cada aplicación, pero tratando de seguir un esquema tipo:

  - Identificación y clasificación de los objetivos principales de la auditoría.
  - Determinación de subobjetivos para cada uno de los objetivos generales.
  - Asociación, a cada subobjetivo de un conjunto de preguntas y trabajos a realizar teniendo en cuenta las particularidades del entorno y de la aplicación a auditar.

  - Desarrollo de temas como:

    - Modos de captura y validación.
    - Soportes de los datos a capturar
    - Controles sobre los datos de entrada.
    - Tratamiento de errores.
    - Controles sobre los tratamientos: secuencia de programas, valores característicos, controles de versión, exactitud de los cálculos, etc. Controles de las salidas: clasificación y verificación de las salidas; presentación, distribución, diseño y forma de los listados.
    - Pistas para control y auditoría.
    - Salvaguardias.

- **Tests de confirmación, tests sobre los datos y los resultados.** Aquellos que consideramos necesarios para asegurar que los controles funcionan como se han descrito y previsto, y que los controles internos son aplicados.

Ejemplos de objetivos de auditorías de aplicaciones

A modo de ejemplo, señalaremos las líneas maestras (no servirían como objetivos reales por incumplimiento de los requisitos enunciados) de algunos objetivos que pueden establecerse en este tipo de auditorías de aplicaciones informáticas:

1. Emitir opinión sobre el cumplimiento de los objetivos, planes y presupuestos contenidos en el Plan de Sistemas de Información sobre la aplicación a auditar

1.1. Cumplimiento de los plazos previstos en cada una de las fases del Proyecto: Estudio previo, Diseño, Programación, Pruebas, Conversión en su caso, Plan de formación e Implantación.

1.2. Cumplimiento de los presupuestos previstos en cada una de las fases enumeradas y para cada uno de los conceptos manejados: equipos, software, contratación exterior, personal propio, etc.

1.3. Cumplimiento de las previsiones de coste de funcionamiento normal de la aplicación y de su mantenimiento al nivel de desglose adecuado.

2. Evaluar el nivel de satisfacción de los usuarios del sistema, tanto de la línea operativa como de las organizaciones de coordinación y apoyo respecto a la cobertura ofrecida a sus necesidades de información

2.1. Nivel de cobertura de funcionalidades implementadas respecto al total de las posibles y deseables en opinión de los usuarios, incluyendo en el concepto de funcionalidad la posibilidad de obtención de informes de gestión y de indicadores de seguimiento de las actividades de la organización usuaria.

2.2. Nivel de satisfacción con el modo de operar las diferentes funcionalidades soportadas por la aplicación, incluyendo los diseños de pantallas e informes de salida, mensajes y ayudas: identificación de mejoras posibles.

2.3. Nivel de satisfacción con la formación recibida para el uso de la aplicación, utilidad del "Manual de usuario" y funcionamiento de los canales establecidos para la resolución de los problemas que surgen en el uso del sistema (¿Línea caliente?).

2.4. Nivel del satisfacción con los tiempos de respuesta de la aplicación y con la dotación de equipos informáticos y sus prestaciones.

2.5. Nivel de satisfacción con la herramienta de usuario para procesar información de la aplicación, en el caso de disponer de ella. (Caso de no estar operativo y haber indicios de su posible conveniencia, el objetivo podría ser el estudio de la conveniencia o no de su implantación.)

3. Emitir opinión sobre la idoneidad del sistema de control de accesos de la aplicación

3.1. Evaluar la eficacia y seguridad del Sistema de control de accesos diseñado. (Controles referentes a la identificación de usuario y palabra de paso y posibles intentos reiterados de acceso no autorizado.)

3.2. Analizar si la asignación de operaciones y funcionalidades permitidas a cada uno de los perfiles de usuario diseñados responde a criterios de necesidad para el desempeño del trabajo y segregación de funciones.

3.3. Comprobar que las asignaciones de perfiles a usuarios responden a los puestos que ocupan y se evita la asignación de perfiles a usuarios únicos en cada centro operativo.

4. Verificar el grado de fiabilidad de la información

4.1. Revisión de la eficacia de los controles manuales y programados de entrada, proceso y salida: seguimiento de varias operaciones concretas identificables a lo largo del ciclo completo de tratamiento.

4.2. Comprobación por muestreo de la exactitud de la información almacenada en los archivos de la aplicación con respecto a documentos originales.

4.3. Pruebas de validez y consistencia de datos de la aplicación mediante proceso informático de la Base de datos real con herramientas de usuario.

4.4. Pruebas de conciliación de magnitudes totalizadas en la aplicación durante varios períodos de tiempo frente a las disponibles, quizá también a través de utilización de herramientas de usuario, en otros sistemas con los que mantiene relación (sistema contable, almacenes, compras, etc.).

19.4.3. Planificación de la auditoría

La auditoría de una aplicación informática, como toda auditoría, debe ser objeto de una planificación cuidadosa. En este caso es de crucial importancia acertar con el momento más adecuado para su realización:

- Por una parte no conviene que coincida con el período de su implantación, especialmente crítico, en que los usuarios no dominan todavía la aplicación y están más agobiados con la tarea diaria. En el período próximo a la implantación, frecuentemente se detectan y solucionan pequeños fallos en la aplicación, situación que convendría esté superada antes de iniciar el proceso de auditoría.

- Por otra parte el retraso excesivo en el comienzo de la auditoría puede alargar el período de exposición a riesgos superiores que pueden y deben ser aminorados como resultado de ella.

En nuestra experiencia, se han manejado períodos de entre 4 y 8 meses desde el inicio de la implantación en función de la magnitud de la aplicación.

- También hay que establecer el ámbito de actuación: tratándose de organizaciones implantadas en amplias zonas territoriales, será necesario delimitar el campo de actuación de la mayor parte de las pruebas a realizar a un reducido número de centros de trabajo. Sin embargo, se ampliará el ámbito, de manera que abarque la representación más extensa posible de usuarios y centros, en aquellas pruebas en que se considere factible, sin incurrir en un coste desproporcionado (encuestas, procesamiento de información, contactos telefónicos, etc.).

- Para la selección de ese limitado número de centros en los que llevar a cabo el trabajo de campo, conviene solicitar a la organización usuaria que los proponga, en base a razones por las que estime puedan aportar mayor valor al trabajo: su participación como pilotos en el desarrollo del sistema o en proyectos de innovación y mejora relacionados con el proceso, haber experimentado recientes cambios organizativos o en su personal directivo que puedan implicar riesgos adicionales, la existencia de indicadores de actividad que se desvíen significativamente de la media general, etc.

- Debe conseguirse cuanto antes, solicitándolo ya en las primeras tomas de contacto, las autorizaciones necesarias para que el personal de auditoría, que está previsto participe en el trabajo, pueda acceder a la aplicación y a las herramientas de usuario. Se solicitará un perfil de auditor –si específicamente se hubiese considerado– o, en otro caso, aquel que ofrezca las mayores posibilidades de sólo consulta: permitirá dedicar a su conocimiento, y a preparar pruebas que puedan precisar su uso, esos tiempos de parada que suelen producirse en el desarrollo de otros trabajos que vayan a ejecutarse durante los meses anteriores al inicio del trabajo de campo de nuestra auditoría de aplicación.

19.4.4. Trabajo de campo, informe e implantación de mejoras

En principio las etapas de realización del trabajo de campo, de redacción del informe y de consenso del plan de implantación de mejoras, no ofrecen peculiaridades de relevancia respecto a otros trabajos de auditoría. Es por eso que no vamos a hacer

más referencia a ellas que algún comentario que la experiencia nos sugiere de validez para cualquier auditoría.

- La etapa de realización del trabajo de campo consiste en la ejecución del programa de trabajo establecido. Evidentemente, los resultados que se van obteniendo pueden llevar a ajustar el programa en función de dichos resultados, que pueden aconsejar ampliar la profundidad de algunas pruebas, acometer otras no previstas y concluir alguna antes de su final.

  - Una recomendación de cara a esta etapa es la de plantearse la mínima utilización de "papeles de trabajo", en el sentido literal, físico, potenciando la utilización de PCs portátiles como soporte de la información de las muestras con las que se vaya a trabajar y para la recogida de información y resultados de las diferentes pruebas: no es sólo cuestión de imagen, sino de productividad.

- Respecto a la etapa de redacción del informe de la auditoría, que recogerá las características del trabajo realizado y sus conclusiones y recomendaciones o propuestas de mejora, quiero recoger la inquietud, que compartimos los integrantes de nuestra dirección de Auditoría, por el tiempo que nos está requiriendo: lo consideramos excesivo, tanto en horas de dedicación como en avance del calendario. Son de aplaudir iniciativas como la propuesta en el artículo "The single page audit report", de Francis X. Bossle y Alfred R. Michenzi, publicado en la revista *Internal auditor* de abril de 1997, que por nuestra parte estamos dispuestos a experimentar.

- En cuanto a la etapa de implantación de las mejoras identificadas en la auditoría, simplemente quisiera lanzar un reto: la situación óptima a alcanzar es conseguir que la organización auditada asuma las propuestas de actuación para implantar las recomendaciones como objetivos de la organización, iniciativa con la que gratamente nos hemos visto sorprendidos en un reciente trabajo en nuestra empresa; ésta es la mejor señal de valoración positiva por parte de una organización a un trabajo de auditoría.

19.5. CONCLUSIONES

La **creciente importancia asignada a los sistemas de información** como ayuda inestimable e imprescindible en el desarrollo de los procesos de negocio, aportando no ya información, sino conocimiento –se está demandando– que apoye la correcta toma de decisiones *atribuye esa misma importancia a la auditoría de las aplicaciones informáticas*, garantes del correcto cumplimiento de la función encomendada a las mismas. Efectivamente, si la base de la toma de decisiones no es segura, fiable y confidencial los resultados pueden ser exactamente los contrarios a los pretendidos.

Por otro lado **el enorme y continuo avance tecnológico en este terreno y la apertura de los sistemas al exterior, exige un gran esfuerzo de formación a los auditores informáticos,** que debe ser cuidadosamente planificado, para poder seguir ofreciendo las garantías mencionadas en un **entorno cada vez más amenazado por nuevos riesgos,** *entrañados en esas mismas tecnologías.* Téngase en cuenta que las amenazas son de tal calibre, que pueden llegar al extremo de poner en peligro la supervivencia de aquellas empresas que fracasen en el empeño de tener bajo control el conjunto de la función informática que da soporte a sus sistemas de información.

19.6. LECTURAS RECOMENDADAS

Manuales de Auditoría informática de las empresas de Auditoría y Consultoría.

Metodología de Auditoría "AUDINFOR", del Instituto de Auditores Internos de España (incluye programa informática).

Handbook of EDP Auditing, de Stanley D. Halper, Glenn C. Davis, P. Jarlath O'Neil-Dunne y Pamela R. Pfau (COOPERS & LYBRAND).

Systems auditability & control, compilado por: The Institute of Intemal Auditors, Inc. Researched by: Stanford Research Institute.

19.7. CUESTIONES DE REPASO

1. ¿Qué fines persigue una aplicación informática?

2. Enumere las principales amenazas que pueden impedir a las aplicaciones informáticas cumplir sus objetivos.

3. ¿Qué es una "pista de auditoría"?

4. Explique en qué ocasiones utilizaría la técnica de encuesta frente a la de entrevista.

5. ¿Cuándo se deben llevar a cabo pruebas de conformidad? ¿Y pruebas substantivas?

6. Valore la importancia del manual de usuario para la auditoría de aplicaciones.

7. ¿Qué aspectos se deben considerar en la preparación del plan de trabajo detallado?

8. Proponga técnicas para medir el nivel de satisfacción del usuario con el modo de operar de las aplicaciones.

9. ¿Cómo verificaría el grado de fiabilidad de la información tratada por una aplicación?

10. ¿Cree conveniente que el auditor tenga autorización para actualizar datos de las aplicaciones que está auditando?

CAPÍTULO 20

AUDITORÍA INFORMÁTICA DE EIS/DSS Y APLICACIONES DE SIMULACIÓN

Manuel Palao García-Suelto

Este capítulo versa sobre la Auditoría Informática (AI) de los *"Executive Information Systems/Decision Support Systems"*[1], y las Aplicaciones de Simulación.

Aunque se trata de aplicaciones informáticas cuantitativamente minoritarias, su uso creciente, su importancia relativa y otras características las hacen particularmente interesantes para el auditor informático.

20.1. PROPÓSITO Y ENFOQUE

El objetivo de este capítulo es presentar este tipo de paquetes y aplicaciones señalando sus características diferenciales respecto de la mayoría de las aplicaciones informáticas de gestión, y realizar unas reflexiones y recomendaciones de Auditoría Informática (AI) específicas para esas características diferenciales.

Por razones de deferencia hacia el lector y del espacio disponible, se ha optado por un enfoque genérico (sin abundar en técnicas o paquetes comerciales concretos, por ejemplo) y por excepción (sin cubrir en detalle temas y técnicas más generales ya cubiertos en otros capítulos).

En todos los casos, supondremos que se trata de implantaciones de paquetes y no de desarrollos a medida (que difícilmente estarían justificados).

---

[1] *"Executive Information Systems"*, Sistemas de Información a la Dirección; en adelante SID[EISI].
"Decision Support Systems", Sistemas de Ayuda a la Decisión; en adelante SAD[DSS].

20.2. DESARROLLO DE LAS DEFINICIONES OPERATIVAS DE LOS CONCEPTOS CLAVE

Los tres conceptos introducidos al principio del capítulo exigen ciertas precisiones para poner en perspectiva el planteamiento de este capítulo.

20.2.1. Auditoría Informática

Sin perjuicio del más amplio y detallado planteamiento que sobre AI se hace en la Parte I de este libro, deseo destacar aquí dos características importantes de la misma: i) la amplitud y variabilidad del concepto, misión, objetivos detallados y formas organizativas de la AI; y ii) su nula o baja regulación *oficial*.

20.2.1.1. Amplitud y variabilidad del concepto de AI

Si se acepta como definición operativo *amplia* de Auditoría Informática:

a) Una actividad profesional de investigación, evaluación, dictamen y recomendaciones...
b) centrada en la informática como actividad o fin en sí misma...
c) como instrumento al servicio de otras funciones más o menos *dependientes* de ella...
d) o en ambos aspectos...
e) con el fin de enjuiciar si ayudar (auditores... consultores) a que...
f) la organización y su funcionamiento sean *conformes* (Control Interno) con lo dispuesto... (estructuras políticas, procedimientos...
g) por quien tiene poder legítimo para disponerlo (los "dueños" [interesados o *stakeholders*]: Consejo, Presidente Director General, Administración Pública...

quedará manifiesta la amplitud y variabilidad señalada.

20.2.1.2. Nula o baja regulación oficial de la AI

La variabilidad de concepciones sobre lo que es la AI, su relativa juventud, una insuficiente apreciación de su importancia y otros intereses en juego han limitado o frenado dicha regulación (diversa, según países y sectores –estos últimos, tratados en la Parte III de este libro–).

Ante esa falta de regulación, las asociaciones profesionales, y en este caso –de modo destacado– ISACA (Information Systems Audit and Control Association) han propuesto normas y códigos de buena práctica de uso voluntario, entre los que cabe destacar COBIT. A este conjunto de documentos (aún en evolución cuando escribo esto) me remitiré, más adelante, como norma de aplicación.

20.2.2. SID[*EIS*] / SAD[*DSS*]

Los Sistemas de Información a la Dirección –SID[*EIS*]– y los Sistemas de Ayuda a la Decisión –SAD[*DSS*]- han venido suponiendo en la historia de la Informática de Gestión un "Santo Grial" o "manto de Penélope": un anhelo aún no suficientemente realizado.

Los SID[*EIS*] y los SAD[*DSS*] han sido, casi desde que se acuñaron los términos, compañeros de viaje, aunque su tecnología, grado de evolución y nivel de uso no sean parejos.

20.2.2.1. Antecedentes de los SID[EISI

Las prestaciones típicas de la Informática de Gestión a lo largo de sus diversos estadios evolutivos: Informatización Administrativa (Nóminas y Contabilidad) en la década de los sesenta; Sistemas de Información en los setenta, etc., no han podido o no han sabido[2] aportar al Directivo la información adecuada (oportunidad, actualidad, nivel de agregación, etc.) que requería.

Ya en la década de los setenta comenzó[3] la moda del MIS (*"Management Information System"*, Sistema de Información de Gestión), que aún da nombre a más de un departamento informático. Dicha moda supuso buenas aportaciones teóricas y prácticas, pero muchas más operaciones de oportunismo en mercadotecnia[4] a su impacto en la información de dirección fue limitado.

---

[2] Una famosa encuesta de *Fortune* sobre sus mayores 500 empresas, señalaba, como principales problemas (y causas): i) un exceso de información irrelevante; ii) un estilo ininteligible; iii) información poco flexible; iv) incoherencias; v) falta de perspectiva histórica; vi) excesiva dependencia de los informáticos; y vii) desbordamiento de los informáticos.

[3] Algún lector erudito o viejo recordará el impacto que tuvo el libro BLUM69: *Management Information Systems*.

[4] Recuérdese el "IMS" de IBM.

20.2.2.2. Aparición de los SID[*EIS*]

A mediados de los años ochenta comenzaron a proliferar paquetes, aplicaciones y textos de *SID[EIS]*, con planteamientos variados, muchos de los cuales no han quedado retenidos en las actuales tendencias. Entre esos planteamientos, uno –cuyas trazas permanecen– es el de bajar de rango al MIS, que devendría una herramienta para mandos medios, dejando espacio por arriba para el más noble SID[*EIS*][5].

20.2.2.3. Los actuales SID[*EIS*]

En los últimos años, los SID[*EIS*] parecen haberse estabilizado en su enfoque y funcionalidades, como esquematiza el cuadro siguiente, y que se resume en: gran accesibilidad y fácil uso.

Esta facilidad de uso ha conducido a una *utilización alternativa* de los SID[*EIS*]: su utilización como un sistema general de información "para todos".[6]

*Tabla 20.1. Características usuales de los actuales SID[*EIS*]*

Interfaz Gráfica	Iconos, intuitivo, (táctil, menús dinámicos con cambios interactivos, hipertexto, hipermedio, no procedimental, personalizable.
Consultas	"Query" sencillo, *"data driven"*.
Formatos de presentación	Por "jerarquías anidadas", *"drill-down"*. Navegabilidad. Intranet. Internet.
Bancos de Datos	Bases de Datos Corporativas. Creciente tendencia a "atacar" directamente a la BD Corporativa (por ejemplo, paradigma OLAP) en lugar de hacer réplicas o extractos "locales". Información externa. Información cualitativa.[7]
Estructura de datos	Tuplas n-dimensionales (paradigma OLAP; ROLAP).
Vistas	Predefinidas y personalizables.
Ámbito	Información histórica y de contexto.
Detección de desviaciones	Semáforos.
Entorno ofimático	Fax, e-mail, teléfono, teleconferencia, etc.
Herramientas mínimas	Calculadora. Estadística descriptiva, gráfica e interactiva.
Herramientas usuales	SAD [*DSS*].
Método de desarrollo	Usualmente, prototipos evolutivos.
Programación	Gráfica interactiva, por menús, generación automática de código de alto nivel (estructurado) "propietario", editable.

[5] JOHN90, pp. 380-381.

[6] Se ha acuñado el juego de palabras EIS = *Everybody's Information System* = Sistema de Información para Todos. Ver Caso "CIGNA Corporation" en CURT95a, p. 25.

[7] "Los sistemas de información, generalmente, sólo usan datos cuantitativos, creados internamente en la estructura de control de la empresa, específicamente para el uso por ese sistema." CURT95a, p. 25.

Ejemplos de paquetes con estas funcionalidades pueden ser: HOLOS, COMMANDER, PILOT, DSS de MicroSrategy.

20.2.2.4. Antecedentes de los SAD [*DSS*]

La decisión es la tarea por antonomasia de la persona[8] y –en un contexto empresarial moderno– del ejecutivo.

Los sistemas de ayuda a la decisión son tan antiguos como la Humanidad[9]; los racionales y eficientes, bastante más modernos (y aún poco aplicados) [10].

En todo caso, los ejecutivos toman decisiones continuamente[11] de forma poco estructurada. A mí me parecen particularmente interesantes dos aspectos: la baja trazabilidad (a los datos, modelos, razones y documentos), y la baja/nula imputabilidad (exigencia de responsabilidad por la decisión concreta) directa.

20.2.2.5. Aparición de los SAD[*DSS*]

Los SAD[*DSS*] son, también, tan antiguos como la Informática.

20.2.2.6. Los actuales SAD[*DSS*]

Los actuales SAD[*DSS*] comparten una serie de características que se resumen en la siguiente tabla.

---

[8] En cuanto "ser libre" que se enfrenta a opciones.

[9] La Prospectiva a-científica, la astrología, los oráculos, la quiromancia, y sus demás numerosísimas formas (muchas de las cuales han llegado a nuestros días), se remontan a 40.000 años a. C (Britannica, 15 ed. IV: "fortune-telling"). En ningún caso se ha probado su valor predictivo o de ayuda a la decisión racional, y en casi todos han dejado evidencias o, al menos, un "tufillo" inequívoco de servir a intereses de sus administradores.

[10] En las últimas décadas se ha desarrollado un formidable –aunque, en general, inconcluyente y excesivamente teórico– cuerpo de conocimientos psicológicos, sociales y económicos sobre la "toma de decisiones". La "teoría de la decisión" (en Estadística) persigue la solución óptima a partir de una serie de estados iniciales, unos estados finales posibles y un conjunto de experimentos disponibles. El "problema de la decisión" (en Matemáticas) busca un algoritmo o recursividad que dé una respuesta definitiva. (Britannica, 15 ed., III, pp. 424, ss).

[11] "...no estructuradas, multi-dimensionales, *ad hoc*, e impredecibles." CURT95a, p. 25.

Tabla 20.2. Características de los actuales SAD[DSS]

Herramientas	Calculadora Estadística descriptiva gráfica interactiva Estadística avanzada
Series Temporales	Análisis tendencias. Búsqueda automática del mejor ajuste
Modelos	Generales, Sectoriales, "Propietarios"
Paramétricos	Ajustes automáticos
No Procedimentales	Lenguajes de 4ª + Generación
"What if"	Análisis sensibilidad
"Goal Seeking"	Búsqueda de objetivos (normalmente como exploración por pasos incrementales ("step") en un intervalo).
Usualmente, una "opción" de un SID[EISI]	
Conectividad	Soporte ofimático ("decisiones inmediatas")

20.2.3. Aplicaciones de Simulación

Desde los inicios de la Informática, ésta se ha usado en variadas aplicaciones de simulación.

20.2.3.1. Aplicaciones de Simulación

La irrupción de la Investigación Operativa en la gestión en los años cincuenta dio lugar en los sesenta a una irrupción (limitada al reducido ámbito de las empresas suficientemente "culturizadas") de aplicaciones y paquetes de simulación[12], fundamentalmente de teoría de colas.

20.2.3.2. Aplicaciones de Gestión y Aplicaciones Técnicas

Aquí me ceñiré a las aplicaciones "de gestión" para ayuda a la toma de decisiones DAS[DSS], aunque es evidente que la frontera está desdibujada, pues –salvo en casos de ciencia pura– las simulaciones "técnicas" sirven o pueden servir para toma de decisiones "de gestión", en muchos casos de gran transcendencia económica.

Las aplicaciones "de gestión" –a su vez– sirven a dos grandes propósitos: i) la planificación o diseño; y ii) la optimización o reingeniería.

[12] GPSS, *General Purpose Simulation System*, todavía existente, es uno de ellos.

En el primer caso, se trata de diseñar o planificar una realidad aún inexistente (es el caso de inversiones en infraestructura o en planta). En este caso, los grados de libertad al desarrollar el modelo son máximos (se pueden cambiar la "estructura" y sus "reglas"); los riesgos de error asociados, también, al no existir posibilidad de contrastación empírica directa (comparar el funcionamiento del modelo con la realidad que modeliza).

En el segundo caso, la infraestructura ya existe, se trata de mejorar –más o menos radicalmente– su funcionamiento. En este caso, los grados de libertad –y los riesgos asociados– son menores: la "estructura" es inamovible[13]; se pueden explorar reglas alternativas; caben ciertos contrastes empíricos.

20.2.3.3. Técnicas de modelización y simulación por computador

Hay una gran variedad de técnicas de simulación combinables con la variedad de lenguajes en que se pueden implementar.

Las aplicaciones de simulación se programan, todavía más frecuentemente de lo deseable, en FORTRAN o en BASIC, con una introducción progresiva de lenguajes más modernos.

Entre los paquetes, aparte de una pléyade de paquetes para fines específicos -desde gestión de tesorería a distribución en planta de grandes superficies, pasando, por ejemplo, por optimizadores del proceso de producción de cerveza-, hay también una gran variedad de paquetes de propósito general (horizontales, no específicos de una función o sector); entre éstos, por citar dos[14] tipos importantes, están los de simulación estática y los de simulación dinámica; y los deterministas y los estocásticos. La tendencia (no justificable en este espacio) es hacia los dinámicos, estocásticos e interactivos, y con una excelente interfaz gráfica (GUI). Entre éstos se pueden citar: Arena, Taylor II, y WITNESS[15]. Todos ellos se caracterizan (en mayor o menor grado) por una orientación a objetos, una fácil programación gráfica, por menús, y por código de alto nivel (generado automáticamente). Su potencia, flexibilidad y facilidad de uso varían, al igual que sus facilidades de "documentación interna".

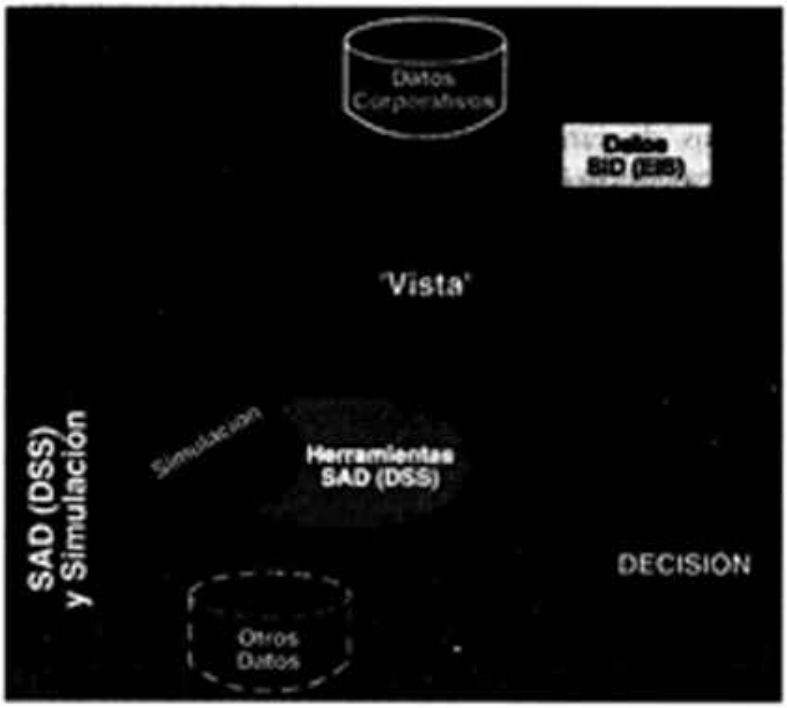
Los SID y los SAE se presentan frecuentemente juntos, como se ha dicho, por razones funcionales y comerciales, aunque –estrictamente– pueden tratarse de modo independiente. En la figura de la página siguiente, se muestran conjuntamente.

---

[13] A medio o largo plazo, todo es variable. En el límite, se estaría en el caso primero.

[14] PI+C96.

[15] Declaración de intereses: al escribir estas líneas, tengo una participación en MODELCO The Model Company, S.L., distribuidora exclusiva de WITNESS en España, en diversos sectores, entre ellos: Distribución, Administración, Logística, Servicios.



A partir de un Banco de Datos Corporativo [1] se obtienen directamente (o indirectamente [2], mediante una Base de Datos "local") "vistas" [3]. Ambos enfoques tienen ventajas e inconvenientes: el ataque directo a la Base de Datos Corporativa tiene la ventaja del acceso a la "totalidad actualizada" y el inconveniente de la mayor concurrencia, tiempo de respuesta y complejidad (cuando, de hecho, el nivel desagregado rara vez interesa al ejecutivo); el uso de una base de datos privada o local para el SID reduce y resume la información y plantea el problema de los criterios y filtros de extracción y el del ciclo de refresco (que, en la mayoría de los sectores, no es crítico). La tendencia es el ataque directo a la Base de Datos Corporativa.

Las "vistas" [3] son la frontera entre los SID y los SAE: dependen del tipo de herramientas que se les apliquen: si no hay ninguna o son sencillas, nos quedamos en el SID; si son más complejas, pasamos al SAD [4]. Si se aplican paquetes de simulación [5] que rebasan las herramientas propias del SAD, estamos en una situación de SAD, pero usando otras herramientas y –eventualmente– otras fuentes de datos [6].

20.3. SINGULARIDADES DE LA AI DE LOS SID[*EIS*], SAD [*DSS*] Y SIMULACIÓN

Sobre AI de los SID[*EIS*] se encuentra una cierta cantidad de documentación; no así sobre SAD *[DSS]* y Simulación. Sin embargo, parece que debería preocupar más este último grupo de aplicaciones, debido –sobre todo– a la "materialidad" o importancia relativa de las decisiones que entren frecuentemente en juego.

20.3.1. AI de los SID[*EIS*]

Por lo que respecta a la AI de los SID[*EIS*], las tablas 20.3 y 20.4 resumen los principales riesgos de *control general y de aplicación*[16].

Tabla 20.3. Riesgos de Control General

Área	Riesgo
Datos	Se puede acceder a datos y/o manipularlos vía el SGBD (tanto más si hay 2 escalones: BD Corporativa y BD local) u otras utilidades.
	Probablemente hay datos en PCs y laptops: entornos poco seguros.
	Puede tratarse de información muy sensible, sobre todo si lleva asociados informes, memorandos y mensajes.
	Las facilidades de extracción de información facilitan el robo.
	Los procedimientos normales de control de telecomunicaciones no son aplicables.
Logical[17]	La arquitectura de sistema abierto tiene más debilidades de control.
	El Desarrollo Rápido puede suponer fallos de análisis o diseño.
	La gestión y control de accesos es compleja.
	La programación de usuario final es difícil de controlar.
Material	Los equipos y datos distribuidos dificultan la gestión de copias de seguridad.
	Los planes de contingencia pueden no cubrir o no cubrir suficientemente los PCs.
Personal y procedimientos	Los directivos pueden resistirse en la práctica a procedimientos de seguridad y control.
	El control sobre datos cualitativos es más difícil de implementar.
	Los propietarios de datos pueden decidir comunicarlos sin que se hayan revisado suficientemente.
	A efectos de AI, los auditores deben tener una alta cualificación; el uso de herramientas CAAT[18] será difícil; todo ello encarecerá la auditoría.

[16] Ampliamente basadas en CURT95b, pp. 30-31.

[17] *Software*, "Soporte Lógico".

[18] *CAAT, Computer-Assisted Audit Tool (or Technique)*, Herramienta (o Técnica) de Auditoría Asistida por Computador.

Tabla 20.4. Riesgos de Control de Aplicación

Área	Riesgo
Entradas	Dependencia de fuentes muy dispersas.
	Carencia de controles normalizados sobre fuentes externas.
	Dificultad de controlar datos cualitativos.
	Presión para introducción de datos urgente, antes de su revisión.
	Acceso no autorizado gracias a la interfaz fácil de usar.
	Gestión de accesos compleja.
Procesos	Rutinas de proceso complejas.
	En el caso de herramientas estadísticas y de simulación, el algoritmo, sus limitaciones, su aplicabilidad y su documentación pueden ser inadecuados o insuficientes.
	La modificación continua del logical puede inhibir controles de mantenimiento y gestión de la configuración.
	Carencia de procesos estructurados de desarrollo.
Salidas	Se pueden enviar salidas vía e-mail a destinatarios no autorizados.
	La exactitud de las salidas gráficas es más difícil de verificar.

Tabla 20.5. Consideraciones sobre la Auditoría de SID[EIS][19]

Controles de Desarrollo	El liderazgo y la participación comprometida de la Alta Dirección son cruciales. El SID[*EIS*] puentea a los mandos medios, que serán hostiles.
	El directivo responsable del proyecto debe tener el nivel, el poder, el tiempo y el propósito de que el sistema se adapte a las necesidades de la organización y esté claramente enlazado con sus *objetivos de negocio*.
	El AI debe participar *desde el estudio de viabilidad*.
	El SID[*EIS*] está destinado a la toma (asistida por SAD[*DSS*], o no) de *decisiones estratégicas*. Esto muestra una situación de altísimo riesgo para el AI. Principales factores críticos de éxito: gestión de problemas de datos, gestión de resistencia organizativa, gestión del ámbito y la evolución.
Datos	El ámbito de análisis de la AI no debe limitarse al SID[*EIS*], sino que debe abarcar la totalidad de los Sistemas de Información que directa o indirectamente interactúen con él o le aporten datos.

[19] Extractado de CUR+95, y adaptado.

Tabla 20.5. Consideraciones sobre la Auditoría de SID[EISI] (Continuación)

	La auditoría de un SID[*EIS*] debería comenzar antes de que los datos lleguen a estar en el mismo.
	El aumento de riesgo (por el riesgo estratégico del SID[*EIS*] debe llevar a revisar los objetivos, controles, tamaños de muestra, etc. de las aplicaciones de origen.
	Particular atención debe prestarse a la revisión de los procedimientos de control interno de entradas y procesos; documentación de programas, listados de fuentes, comunicaciones y seguridad física.
Telecomunicaciones	El entorno puede ser internacional, con diversas redes LAN, WAN, Intra e Internet. La seguridad del entorno de comunicaciones debe ser evaluada.
Interfaz de Usuario	La facilidad y sencillez de uso son críticas. El AI debe evaluar: la calidad de la interfaz de usuario, la navegabilidad, la facilidad de informes a medida, la flexibilidad y calidad de los gráficos, la facilidad de uso de las herramientas de análisis, y la facilidad de acceder a datos externos, integrar datos en entornos ofimáticos y producir salidas por fax y e-mail.
	El AI debe asegurarse de que –desde el inicio– (para minimizar los cambios posteriores) el sistema satisface en contenidos y procedimientos las necesidades de los ejecutivos usuarios.
Costes de Desarrollo	Debe diseñarse el sistema más simple posible que satisfaga en contenidos y procedimientos las necesidades *reales* de los ejecutivos usuarios. El método de desarrollo será normalmente por *prototipos evolutivos*, cuyo control de costes puede ser más difícil. La justificación del gasto es intangible.
Seguridad	El mayor riesgo es el de filtración de información estratégica.
	La posibilidad de errores o de manipulaciones puede tener consecuencias muy graves.
	Deben extremarse los controles de: autentificación de accesos, autorización de accesos a información sensible, registros de accesos y telecomunicaciones, registros de modificaciones, cifra[20] seguridad física (manipulación, robo) de equipos, evitación de copias en disquete, protección antivirus, protección física y lógica de las comunicaciones, seguridad del sistema operativo, de la red y del gestor de bases de datos.
Varios (de la máxima importancia)	Asegurar que no se falla en la identificación de información relevante.
	Asegurar que no se falla en la interpretación del significado y valor de esa información.
	Asegurar que no se falla en la comunicación de información a otros decisores clave.

La Tabla 20.6 propone una selección[21] de objetivos de control extractados de COBIT 96. Se centra más en "controles generales" que en "controles de aplicación". Pretende servir de complemento a las presentadas más arriba.

[20] "Encriptación".

[21] Esta selección es del autor del capítulo, NO de COBIT. La traducción al castellano de los objetivos de control NO ha sido homologada.

Tabla 20.6. Principales Objetivos de Control (COBIT 96) a considerar en AI de SAD [DSS] y Simulación

Objetivo de Control de Alto Nivel (1)		Objetivo de Control		Comentario
P09	Evaluar Riesgos	§ 9.2	"La calidad de la evaluación de riesgos debe asegurarse con un método estructurado y con asesores sobre riesgos que estén cualificados."	Arduo problema.
		§ 9.6	"El enfoque de la evaluación de riesgos debe asegurar la aceptación formal del riesgo residual, según la identificación y medida del riesgo, la política organizativa, la incertidumbre incorporada al propio enfoque de evaluación del riesgo, y el coste-eficacia de implantar salvaguardas y control. El riesgo residual debe compensarse con una adecuada cobertura de seguros."	
PO10	Gestionar Proyectos	§ 11.10	Relaciones con el subcontratista.	
		§ 11.11	Normas de documentación de programas.	
PO11	Gestionar la Calidad			Ver comentario a DS2.
AI1	Identificar soluciones			
AI2	Adquirir y Mantener Logical de Aplicación	§ 2.11 Controlabilidad	Incluyendo "controles de aplicaciones que garanticen la exactitud, complitud, oportunidad y autorización de entradas y salidas. Debiera hacerse una evaluación de sensibilidad..." "... Integrar en el diseño, tan precozmente como se pueda, los conceptos de seguridad."	Una parte substancial de este tipo de aplicaciones son de desarrollo de prototipos y de "informática de usuario final", donde es difícil aplicar los objetivos de control clásicos e incluso dudoso si debe hacerse.[22]

[22] ¿Debe la Informática de Usuario Final considerarse (a efectos de AI), o debe más bien entenderse como ejercicio discrecional del profesional o ejecutivo, auditable por otras vías? Las herramientas de usuario final son excluibles –en mi opinión– de la auditoría informática, salvo en los aspectos de homologación de los productos, formación y concienciación de usuarios, servicio de incidencias (*hotline*), copias de seguridad, control de licencias y actualización de versiones.

Objetivo de Control de Alto Nivel		Objetivo de Control		Comentarios
DS3	Gestión del Funcionamiento y Capacidad	§ 3.4	Modelización del funcionamiento y capacidad de los servicios de información	Ésta es la única cita directa a modelización – simulación que he identificado en COBIT.
DS7	Formar y Entrenar a los Usuarios			Concienciación en las peculiaridades –en cuanto a riesgos– de estas aplicaciones.
DS11	Gestión de Datos	§ 11.4	Pistas o Trazas de Auditoría	Asegurar que todo documento impreso o exportado lleve identificación de autor, "vista", sesión, versión, y –por defecto– indicación de "Borrador".
		§ 11.15	Revisión de Salidas y Gestión de errores	
DS2	Gestión de Servicios por Terceros			Los SAD y los modelos de Simulación son frecuentemente subcontratados a empresas especializadas, sobre *las cuales* y cuyos contratos debe ejercerse vigilancia. Desgraciadamente, con COBIT ha perdido (respecto de anteriores versiones de los *Control Objectives*) la visión de auditoría o certificación de subcontratistas
M2	Obtención de Garantías Independientes			

20.3.2. AI de los SAD [*DSS*] y Simulación

La principal singularidad de este tipo de aplicaciones es que se trata de "aplicaciones" muy características de "usuario final"[23] o de subcontratación de consultaría especializada. Cualquier uso de herramientas estadísticas o de simulación por personas sin una considerable especialización es probablemente temerario[24].

Las condiciones en que se desarrollan los "grandes modelos" (los que sustentan las grandes decisiones), son, con frecuencia, el contrapunto de lo deseable desde un punto de vista de AI: encargados por altos directivos que se enfrentan a unas disyuntivas, que suponen un caso singular y puntual, bajo presión política o económica, con premura y escasez de tiempo, con datos a menudo escasos y poco validados, con una comprensión limitada de los puntos fuertes y débiles y de los condicionantes de la modelización, aceptando la modelización como solución, pero no pudiendo conceder tiempo o prestar atención a análisis de sensibilidad y a "replicaciones" [25].

Las solicitaciones al AI llegan en este caso al límite. Los enfoques y técnicas aplicables deben ingerirse de lo anteriormente discutido (para la AI en general, y para los SAD [*DSS*] más concretamente). Pueden explotarse enfoques como el del doble cálculo independiente que se usa en ingenierías nucleares y otras, evaluaciones indirectas basadas en la *documentación y trazabilidad* (generalmente pobres, por las prisas) de los modelos y experimentos, y –finalmente– en "controles generales" (que son, relativamente, los más débiles; pero, en última instancia los más sólidos): formación y concienciación del usuario, controles de subcontratación, etc.

Según Mike O. Villegas, de Arthur Andersen, en su modelo[26] de 7 capas [p. 24] de Gestión de Riesgos, los mayores riesgos están en las capas de Aplicación y de Proceso [p. 25], que son las específicas de los "controles de aplicación", esto es –según mi interpretación, y usando terminología clásica– en los "controles específicos" y no en los "generales".

En todo caso, la mejor estrategia de AI es aplicar consistentemente COBIT96, aceptando el hecho de que algunos entornos tecnológicos especiales pueden requerir una cobertura independiente de objetivos de control" [27].

---

[23] Que, en estos casos, no es normalmente un directivo, sino una persona o un equipo de su gabinete técnico.

[24] Piénsese, por ejemplo, en una herramienta DSS tan relativamente simple y banalizada como Excel 97 de Microsoft. Moléstese el lector no especialista en estadística en consultar el menú: Herramientas-(Complementos)-Análisis de Datos-Análisis de Fourier; o –en Ayuda– "estadística, publicaciones técnicas".

[25] "Replicaciones": repetición de experimentos en modelos estocásticos (PI+C96, p. 98).

[26] DHAL96.

[27] COBIT96, *Executive Overview*, p. 17.

No debe desdeñarse el recurso a grandes indicadores y cuadres "externos", aplicado por personas con experiencia; ni el uso de *systems-walk-thrus*.

Puede también desempeñar aquí un importante papel el CSA Control SelfAssessment[28] –Autoevaluación del Control– método aún insuficientemente normalizado, con un enfoque de "gestión de salud primaria y preventiva", "... coherente con los conceptos de Calidad Total" [p. 30], "suplemento y no substituto" [p. 4] de la auditoría convencional, cada vez más popular desde "mediados de la década de los ochenta" [p. 20], por el que "el personal, a todos los niveles, en todas las funciones, lo constituyen los Analistas Informadores de Control Primarios" [p. 32].

20.4. CONCLUSIONES

La AI de SID[*EIS*] y SAD[*DSS*] y Sistemas de Simulación entraña dificultades límite (sobre todo, en el caso de los últimos): la "importancia relativa" puede ser enorme, agravada por la baja estructuración/documentación de procedimientos. Los procedimientos clásicos y las normas disponibles (COBIT96) son insuficientes, pero el tema está ahí, y cada vez será más frecuente. El AI debe recomendar al máximo controles generales y controles de aplicación (de las que alimentan de datos a estos sistemas), extremar el uso de técnicas indirectas (indicadores externos, *systems-walkthrus*), y recurrir a técnicas (CSA) alineadas con la Calidad Total.

20.5. LECTURAS RECOMENDADAS

COBIT96. ISACA. *Control Objectives for Information and Related Technology.* ISACA. Illinois, EE.UU. 1996.

CUR+95. Curl, Steven y Gallegos, Frederick. *Audit Considerations for EIS.* IS Audit Control Journal. Illinois, EE.UU. Vol. II, 1995, pp. 36 y ss.

20.6. CUESTIONES DE REPASO

1. Definición operativa amplia de Auditoría Informática.
2. Resuma la evolución de los SID.
3. Principales características de los SID actuales.

[28] CSA_97

4. ¿Qué diferencias destacaría entre un SID y un SAD?

5. Riesgos de control general de los SID.

6. ¿Cuáles son los principales medios de control de aplicación de los SID?

7. Objetivos de control de la auditoría informática de las aplicaciones de simulación.

8. ¿Qué es la autoevaluación del control?

9. ¿Por qué resulta tan importante la auditoría de los SAD, SID y de las aplicaciones de simulación?

10. Elabore listas de control para auditar algún sistema que conozca para el desarrollo de aplicaciones de simulación.

CAPÍTULO 21

AUDITORÍA JURÍDICA DE ENTORNOS INFORMÁTICOS

Josep Jover i Padró

21.1. INTRODUCCIÓN

La **Auditoría Jurídica** forma parte fundamental de la **Auditoría Informática.** Su **objeto** es **comprobar** que la utilización de la Informática se ajusta a la legislación vigente. A sólo título de ejemplo, citaremos normativa como la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LOPD)[1] y la Ley de Propiedad Intelectual[2]... que, entre otras[3], está presente en tal comprobación. Superar el test de la legalidad implica la existencia adecuada a Derecho de las bases de datos, de los programas y, en definitiva, de la estructura informática de la organización que se somete a examen.

La Auditoría Jurídica es esencialmente importante para evitar posibles reclamaciones de cualquier clase contra el sujeto a auditar. Por ello, el trabajo del auditor es la **medida preventiva** idónea contra sanciones en el orden administrativo o

[1] Ley Orgánica 15/99, de Protección de Datos de Carácter Personal.

[2] Ley 16/93 de incorporación de la Directiva 91/250/CEE, de 14 de mayo de 1991, sobre la protección jurídica de los programas de computador (BOE de 24 de diciembre de 1993).

[3] Entre estas otras, además de las específicamente referidas a la materia, existen otras que a pesar de estar dedicadas a otras materias, abordan el tema desde alguno de sus aspectos. Así, la Ley de Protección Jurídica y Modificación del Código Civil y de la Ley de Enjuiciamiento Civil (LO de 15 de enero de 1996 núm. 1/1996, BOE 17 de enero de 1996).

incluso *penal, así como indemnizaciones*[4] *en el orden civil por daños y perjuicios a los afectados, y ello lo referimos tanto a las Administraciones Públicas como a las empresas privadas.*

Con el examen jurídico-técnico se pretende conseguir una ***gestión más eficaz*** *de dichas bases de datos y programas. Uno de los primeros objetivos para cualquier organización, en esta área, es evitar costes económicos en forma de sanciones o indemnizaciones por negligencias que se podrían haber prevenido de fácil modo y, en combinación con las otras facetas de la Auditoría Informática, lograr el descubrimiento de irregularidades en el contenido o en el uso de los programas o de la información tratada. Estas irregularidades afectan no sólo al normal funcionamiento de las empresas auditadas, sino especialmente a las "fugas" de esa información. Todo ello influye, no cabe duda, en la Cuenta de Pérdidas y Ganancias.*

Adentrándonos en el campo del Derecho Penal, y siguiendo a Emilio del Peso[5]*, cabe señalar que la auditoría informática, en sus diferentes modalidades, puede servir para prevenir el llamado delito informático, detecta rápidamente el acto delictivo en caso de que se produzca y facilita la prueba del mismo, en su caso. Las revisiones en que consisten las auditorías informáticas, ya sean periódicas o continuas, causan beneficiosos efectos de cara a la prevención de una posible actuación delictiva. El simple conocimiento, por parte del personal de una empresa, de que existe este tipo de auditoría evita ya, muchas veces, la comisión del delito ante la posibilidad de ser fácilmente descubierto. Cuando existe la auditoría continua, el empleo de las técnicas auditoras informáticas permite, en gran número de casos, descubrir los fraudes cometidos y facilitar la prueba del delito cometido con la ventaja de la inmediatividad. Como consecuencia de todo ello, podemos llegar a la conclusión de que la auditoría informática, y dentro de la misma, la estrictamente jurídica, cumple una* ***función de tipo preventivo*** *imprescindible en relación con el* ***delito informático.***

En base a los aspectos reseñados sucintamente hasta ahora, podemos ofrecer una primera ***definición de la auditoría jurídica dentro de la auditoría informática.*** *Aquélla es la revisión independiente del uso del material, de la información y de sus manipuladores desde la perspectiva de la normativa legal (civil, penal, laboral...),*

---

[4] En relación con esa indemnización por daños y perjuicios, en concepto de responsabilidad por la información manipulada, la LORTAD le abrió definitivamente la puerta, si bien ésta ya aparecía entreabierta en base al artículo 1902 del Código Civil, los artículos en materia de responsabilidad contractual del mismo Código, la Ley Orgánica 1/1982 de 5 de mayo de Protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen y, la responsabilidad de las Administraciones Públicas regulada en la Ley 30/92, en su caso.

[5] *DEL PESO NAVARRO, E. La auditoría informática como medio de prevención frente al delito informático.* III Encuentro sobre la Informática en las facultades de Derecho (mayo 1989) Universidad Pontificia Comillas. Madrid. Editado por la Sección de Publicaciones de la Facultad de Derecho de la Universidad Complutense de Madrid.

efectuada por un ***jurista experto independiente***[6] con la finalidad de emitir un dictamen sobre su adecuación a la legalidad vigente, y con ello conseguir evitar inseguridades, pérdidas o costes innecesarios para la empresa o Administración a la que somete a auditoría jurídica, siendo el cliente auditado en último término el que decide la aplicación de las eventuales medidas correctoras que se estimen oportunas.

La auditoría jurídica comprende cuatro grandes áreas: A) la auditoría del entorno informático, B) la auditoría de las personas que manipulan la información, C) la auditoría de la información, D) la auditoría de los archivos, incluyendo dentro de ésta una auditoría propia, la auditoría de objetivos. Pretende esta última averiguar la correspondencia entre el uso que se le da al archivo y aquellas motivaciones por las cuales se creó, así como la constitucionalidad de la finalidad última del archivo. La auditoría de objetivos va más allá de la del principio de legalidad: es una auditoría de Derechos Humanos de Tercera Generación. Se examina no tanto la legalidad como el espíritu del archivo, con la pretensión de que éste respete y garantice tales derechos. Sin plantear en estas líneas un análisis exhaustivo de la materia, se pretende ofrecer una noción general sobre la tarea del auditor jurídico mediante un examen de cada una de las cuatro áreas reseñadas y de sus consecuencias.

21.2. AUDITORÍA DEL ENTORNO

Definimos como entorno a los programas y soporte físico que sirven de receptáculo a la información y los datos objeto último de la auditoría jurídica. Concretamente, la auditoría jurídica del Entorno se divide en tres partes.

a) Auditoría de los elementos del Hardware

La primera consiste tanto en la comprobación de elementos del HARDWARE como de los contratos que los soportan. Es preciso el examen de los contratos en virtud de los cuales se utiliza dicho material (sea con transmisión de la propiedad o no), así como de sus contratos de mantenimiento. Sólo a modo de ejemplo cabe destacar como más importantes los de compraventa, alquiler, *leasing*, *renting*, reposición y mantenimiento de dicho hardware.

---

[6] Esto es aún más necesario en aquellas empresas que manipulan archivos con datos personales y cuyo responsable es el personal de la propia empresa, o bien en aquellas que poseen datos de morosidad. Según José Mª González Zubieta cabe poner en duda que sea el auditor interno quien haga la auditoría en estos casos, ya que puede verse coaccionado en su independencia profesional sujeta en este caso a la disciplina laboral, al ser la propia empresa el responsable del archivo, y además al no cumplirse uno de los principios fundamentales de la práctica profesional de la auditoría cual es la segregación de funciones para garantizar la independencia y objetividad del dictamen. Es por ello necesario que las auditorías jurídicas sean realizadas por un jurista experto, externo a la organización a auditar y como consecuencia de ello, verdaderamente independiente.

b) Auditoría de los elementos del Software

La segunda parte está dedicada a los elementos del SOFTWARE e incluye, entre otros, el control de las licencias de uso personalizadas, licencias de uso no personalizadas, licencia de uso de código fuente, desarrollo de software y mantenimiento de los programas.

c) Contratos de "paquetes gestionados"

La tercera correspondería a los contratos que entienden la informática y su gestión como un entorno completo donde la organización cede a un tercero la totalidad o parte de su gestión desligándose de las decisiones propias de los departamentos técnicos. *Outsourcing*, elaboración de trabajos auxiliares, contratos de entrada de datos, subcontratación de la gestión de sectores de una empresa o de un grupo de ellas, constituyen ejemplos de dichos contratos.

En lo que hace referencia a este ámbito, de la revisión de la contratación comentada, es importante que la redacción de los clausulados contractuales sea clara y precisa. Así, por ejemplo, en materia de origen de la titularidad de los programas, el auditor debe constatar y en caso de defecto, recomendar especialmente, que en los contratos con programadores asalariados (contratos laborales) o con programadores por encargo (contrato de obra o de servicio) se determine quién adquiere la propiedad de los mismos (a pesar de que en los primeros desempeña la presunción legal de la Ley de Propiedad Intelectual de transmisión al empresario para el ejercicio de su actividad habitual) para la más diáfana determinación de la titularidad, independientemente de la autoría, y con ello evitar posibles dudas y reclamaciones al respecto. Del mismo modo se debe proceder en temas de obras colectivas y obras en colaboración. También se constatará por parte del auditor la existencia de pruebas documentadas de esa titularidad como, por ejemplo, el depósito notarial o *escrow*, el registro de la Propiedad Intelectual, y en su defecto, aconsejará el uso de dichos mecanismos de registro.

Se trata, en definitiva, del análisis de contratos, desde la perspectiva del Derecho Civil y particularmente del Derecho de la Propiedad Intelectual e Industrial. Aspectos como titularidad de los derechos de explotación, autoría, patentes, marcas... están presentes en tal revisión.

En lo que hace referencia a derechos de autor, cabe destacar por su importancia la polémica en la regulación de los programas de computador. Una de las novedades que incorporó la Ley de 1987 fue, precisamente, la regulación de la protección de los programas de computador en el seno del derecho de autor (arts. 95-100 LPI).

El legislador español apostando por la protección jurídica de los programas de computador en este marco, se incardinó en la tendencia existente en la mayor parte de Estados de la Comunidad Europea. De igual manera ha actuado la misma Comunidad que, ya desde la Directiva del Consejo 91/250/CEE[7], ha organizado la protección jurídica de los programas de computador en el Derecho de Autor, en concreto como obra literaria, en el sentido recogido en el Convenio de Berna[8] y como señala MASSAGUER, "renunciando a la idea de establecer un sistema de protección *sui generis*, siquiera dentro del Derecho de autor, no obstante el establecimiento de una regulación particular"[9]. Un sector de la doctrina especializada opina que la decisión de optar por regular esta materia en el campo de la propiedad intelectual es lógica si se atiende a las características de los programas de computador. Así, por ejemplo, OROZCO PARDO[10] siguiendo a GALÁN CORONA señala como principales razones para dicha opción "las ventajas que confiere la protección del derecho de autor ya que no se requiere novedad ni actividad inventiva, sino solamente originalidad, ni tampoco es preciso registro conforme a la Convención de Berna. Todo ello conlleva, gracias al juego de los convenios internacionales, una protección sobre la materia inmediata, geográficamente generalizada y desde el análisis económico del derecho, barata".

Razones de carácter práctico que vienen avaladas por el aumento de la piratería informática de consecuencias negativas tanto para los propios autores como para la comunidad. No obstante, siguen existiendo casos en los que un programa va ligado a un proceso industrial, en cuyo caso se le brinda una protección complementaria, así en el art. 96.3 LPI antigua.

El Derecho de Autor no es el único sistema de protección jurídica a que pueden acceder los programas de computador, que también pueden ser tutelados mediante la aplicación de las disposiciones sobre patentes, marcas, competencia desleal, secretos empresariales, topografías de productos semiconductores o contratos según el art. 9.1 de la Directiva mencionada, protegiendo de modo concurrente con la tutela del derecho de autor el objeto protegido. La generosidad de la relación de sistemas de protección jurídica adicional ofrecidos a los programas de computador de la Directiva 91/259/CEE contrasta con la parquedad de la LPI de 1987, limitada a los programas de computador "que formen parte de una patente o un modelo de utilidad", por ello, era deseable, como señalaba MASSAGUER[11], de cara a mantener un criterio claro de protección, o la supresión del art. 96.3 LPI, ya que el principio de interpretación

[7] Directiva del Consejo (91/250/CEE) de 14 de mayo de 1991, relativa a la protección Jurídica de los Programas de Computador, DOCE, núm. L 122/42, 17 de mayo de 1991.

[8] Convenio de Berna, de 9 de septiembre de 1986, para la protección de Obras Literarias y Artísticas, vigente en España en la redacción del Acta de París de 24 de julio de 1971, ratificada mediante instrumento de 2 de julio de 1973, BOE, núms. 81 y 260, de 4 de abril de 1974 y 30 de octubre de 1974.

[9] En este sentido, MASSAGUER, J., "La adaptación de la Ley de Propiedad Intelectual a la Directiva CEE relativa a la protección jurídica de los programas de computador", en *Revista de Derecho Mercantil*, nº 199-200.

[10] Orozco Pardo, G. "Informática y propiedad intelectual", *Actualidad Informática Aranzadi*, nº 19, abril de 1996.

[11] En este sentido, MASSAGUER, J. *op. cit.*

conforme vigente en la Comunidad aseguraba la acumulación de protección jurídica, o la modificación del citado precepto, sustituyendo su tenor por el del primer inciso del art. 9.1 de la Directiva [12]. La Ley 16/93 de incorporación de la Directiva 91/250/CEE ha resuelto en su Disposición Adicional única "Salvaguardia de aplicación de otras disposiciones legales" en el sentido de tolerar dicha protección adicional pero sin especificar si los programas de computador han de formar parte de una patente o modelo de utilidad. El Texto Refundido de Propiedad Intelectual de 1996[13] no ha resuelto, sin embargo, ese problema de manera diferente al anterior texto legal de propiedad intelectual, desaprovechando, creemos, una oportunidad de mejora legislativa. Recordemos que su artículo 96.3.2 establece que cuando los programas de computador formen parte de una patente o modelo de utilidad gozarán además de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial, confirmando de ese modo la redacción anterior.

21.3. AUDITORÍA DE LAS PERSONAS

No es posible hablar de máquinas y programas sin hacer referencia a quien los usa. Por ello la auditoría jurídica dedica una de sus áreas al sujeto activo del tratamiento informático. La auditoría jurídica de las personas abarca cinco aspectos que el Jurista encargado de la misma debe examinar:

a) Quiénes tienen acceso a la información

Debido a la naturaleza de la información almacenada y manipulada, sea de carácter personal, que afecta al derecho a la intimidad de las personas, o simplemente, datos de interés para la competencia, el acceso a los mismos ha de restringirse atendiendo a la "sensibilidad" de la información.

Como eje vertebrador de esta protección, especialmente en lo que hace referencia a los datos, se crea por la Ley Orgánica de 1992 la figura del responsable del archivo. Éste debe velar por la seguridad de los datos y por ello, adoptar medidas de índole técnica y organizativas necesarias que eviten su alteración, pérdida, tratamiento o el aspecto al que hacemos referencia en este apartado, el *acceso no autorizado*. Para ello deben valorarse el estado de la tecnología, la naturaleza de la información almacenada y los riesgos a que está expuesta, ya provengan de la acción humana o del medio físico o natural.

Reglamentariamente, dentro de las empresas, han de establecerse los requisitos y condiciones que deban reunir las personas que intervengan en la manipulación de los

[12] En este sentido, MASSAGUER, J. *op. cit.*

[13] Real Decreto Legislativo de 12 de abril de 1996, núm. 1/1996 por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual (RCL 1987/2440), regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia. BOE de 22 de abril de 1996, nº 97.

archivos a los que se refiere el artículo 7 de la LOPD (datos especialmente protegidos) en primer lugar, y a las informaciones que son de importancia para la propia empresa o para terceros, en segundo lugar.

Por lo tanto, sólo deberían acceder a los datos "sensibles" aquellas personas que sean autorizadas, actuando la figura del responsable del archivo como garante de la protección de los mismos. Frente a terceros, o incluso en el ejercicio del derecho de acceso por parte de los afectados, el Responsable del Archivo es quien, en algunos supuestos, también limita temporal y parcialmente la obtención de información[14]. Con ello se evita el acceso indiscriminado a los datos de la propia organización.

b) Adecuación de aquéllos al cargo que ostentan

Es necesario, además, que aquellos miembros que tienen el acceso permitido a un cierto nivel de información dentro de la organización, lo tengan de forma adecuada con la responsabilidad y el cargo que ostentan. Deben evitarse accesos no necesarios para el normal desarrollo de las tareas que el trabajador o funcionario tiene encomendadas.

La empresa u organismo no puede arriesgarse a que cualquier usuario, desde cualquier punto del sistema, pueda "vaciar" el mejor tesoro de la organización: su información.

c) Conocimiento de la normativa y de que se debe mantener una actitud ética delante del archivo

Aquel que tiene acceso a un nivel de la información debe conocer las obligaciones y derechos que le asisten. En virtud de su vinculación con la organización, debe mantener una actitud ética ante la información a su disposición y no revelar los datos que conozca en el ejercicio de su cargo o en el desarrollo de su tarea si ello no es necesario para la ejecución de la misma. Si un trabajador de la empresa, vulnerando sus obligaciones, rompe este deber de secreto, rompe también la buena fe contractual, siendo ello motivo de despido disciplinario[15].

---

[14] Así, la LOPD establece que el derecho de acceso sólo podrá ser ejercido en intervalos superiores a doce meses, salvo que el afectado acredite un interés legítimo, en cuyo caso podrá ejercitarse antes. (Art. 15 de la LOPD y arts. 12 y 13 del RD 1332/94.)

[15] En este sentido también cabe recordar el artículo 20.1 y 2 o el artículo 21 del Estatuto de los Trabajadores: "Artículo 20. Dirección y control de la actividad laboral. 1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien éste delegue. 2. En cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquél en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe (...) Artículo 21. Pacto de no concurrencia y de permanencia en la empresa. 1. No podrá efectuarse la prestación laboral de un trabajador para diversos empresarios cuando se estime concurrencia desleal (...)."

En lo que hace referencia a los archivos, el artículo 10 de la LOPD recoge también este deber de secreto, si bien este precepto tiene un objeto diferente al que prevé la legislación laboral. Aquél pretende garantizar los intereses del empresario y éste cumple, como el resto del articulado en que se integra, una función de defensa del derecho a la intimidad. El artículo 10 de la LOPD establece que la obligación del deber de secreto afecta al responsable del archivo y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del archivo.

Asimismo, cabe recordar la existencia de una tipificación penal específica de conductas relacionadas con la vulneración del deber de secreto en relación con particulares, autoridades y funcionarios públicos.

Así el nuevo Código Penal incluye en el Capítulo IV de su Título XIX (artículos 413-418), referente a delitos contra la Administración Pública, tipifica con carácter general las conductas de infidelidad en la custodia de documentos y de la violación de secretos. Dichos delitos pueden ser cometidos por autoridad o funcionario público y, en el caso del artículo 418, por el particular que aprovechara para sí o para un tercero el secreto o la información privilegiada que obtuviere de un funcionario público o autoridad.

Los artículos 198 y 199 del mismo cuerpo legal inciden de nuevo en dicha materia, pero esta vez de modo más específicamente relacionado con el tema que nos ocupa. El primero se refiere a la autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo 197[16] (revelación

[16] Artículo 197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en archivos o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizara la conducta descrita en el párrafo anterior.

4. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los archivos, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

de secretos frecuentemente referidos a información obtenida por medios informáticos, electrónicos o telemáticos) y, el segundo, referido a aquel que revelare secretos ajenos de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, o al profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona.

Estos delitos los pueden cometer todos aquellos que revelen información o datos de carácter personal contenidos en los bancos de memoria de la organización a la que sirven o en archivos de tratamiento automatizado a los cuales tengan acceso o conocimiento por razón de su relación funcionarial, laboral o de simple arrendamiento de servicios.

La pena para las conductas tipificadas en el artículo 198 del Código Penal es la prevista en el artículo 197 (oscilan entre penas de 1 a 3 años de prisión y 12 a 24 meses de multa y cuatro a siete años de prisión más la misma multa, según las diversas conductas tipificadas en el artículo 197), más la inhabilitación absoluta por tiempo de seis a doce años por tratarse de un delito especial, esto es, aquel que sólo puede ser cometido por determinados sujetos, en este caso autoridad o funcionario público.

El artículo 199 tipifica específicamente las conductas de revelación por parte del trabajador o profesional de secretos de los que tenga conocimiento por razón de sus actividades laborales o de arrendamiento de servicios, se prevé para ellos una pena de prisión de uno a tres años y multa de seis a doce meses para el primero (trabajador) y, de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años para el segundo (profesional).

d) Reconocimiento en el contrato de la labor que cumplen y de la responsabilidad que ostentan

Es por todo lo anterior que en el contrato laboral que une a la organización con sus trabajadores ha de expresarse la garantía de la confidencialidad de las informaciones propias de la misma. Especialmente debe procederse a exigir la confidencialidad en el caso de manipulación de datos de carácter personal. Esa confidencialidad es realidad necesaria tanto en el caso de gestión como en el de mero acceso a las máquinas. Afecta a todos los empleados que puedan tener algún tipo de contacto con las máquinas, programas, instrucciones...

---

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Y ello porque existe una traslación de las responsabilidades de los encargados de la información a sus colaboradores, debiendo asumir cada uno de ellos su propia responsabilidad. Si bien la normativa laboral protege al trabajador y responsabiliza frente a terceros a quien le organiza la tarea, en el caso de que la actuación del trabajador pueda ser presuntamente delictiva, aunque fiel a la empresa, aquello no le excusa de las responsabilidades penales adquiridas en el acceso y tratamiento de la información. Es recomendable pues el conocimiento claro de las obligaciones y deberes que comporta el uso de información "sensible" de la organización y de los datos de carácter personal por parte de los trabajadores. Así se evitan, de paso, los "descuidos negligentes".

e) Que los contratos con los proveedores aseguren la confidencialidad del archivo y de la información

En el caso de que lo que se manipulen sean archivos, es aplicable a este ámbito el artículo 10 de la LOPD, todas las personas que intervengan en cualquier fase del tratamiento de la información están afectos a la obligación del deber de secreto, y por lo tanto también los proveedores en la medida en que intervienen en una fase del tratamiento o mantenimiento. Así, los contratos con los proveedores no pueden descuidar el principio inspirador de la legislación, esto es, la confidencialidad de la información y la salvaguarda del derecho a la intimidad. También les es aplicable el principio de buena fe contractual que ha de presidir las relaciones entre comerciantes[17].

21.4 AUDITORÍA DE LA INFORMACIÓN

Una vez visto el material y las personas que lo usan debemos ver el objeto lógico a auditar: la información. El auditor debe comprobar que, en relación con la misma, se cumplen los requisitos básicos del derecho en general y de los propios específicos en particular.

Así, en cuanto a los Principios relativos a la información, debido a la inexistencia de unos específicos[18], podemos establecer una analogía con los requisitos recogidos en el artículo 4 de la LOPD, en relación a la calidad de los datos, la necesidad de su

[17] Ello deriva del artículo 7.1 del Código Civil ("Los derechos deberán ejercitarse conforme a las exigencias de la buena fe") que inspira nuestro ordenamiento y que también encontramos a lo largo de la normativa mercantil por remisión y especialmente reforzada en su articulado por el agravante de exigir la diligencia de un ordenado comerciante.

[18] A pesar de que hay que tener en cuenta la existencia de principios informadores de legislación ligada, como, por ejemplo, la Ley de Protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

adecuación y pertinencia, y que no sean excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido.

La información no podrá usarse para **FINALIDADES INCOMPATIBLES** con aquellas para las que fue seleccionada, y deberá ser exacta y puesta al día. Si no es exacta o está incompleta debe ser cancelada o sustituida por la correcta, siendo cancelada cuando deje de ser necesaria, no pudiendo ser conservada (salvo en el caso en que se decida su mantenimiento por valores históricos o científicos) una vez que deje de ser útil para la función prevista, con excepción de la legislación prevista al efecto (Obligaciones Fiscales, Seguros...).

Se debe almacenar de forma tal que permita de una manera fácil el ejercicio del derecho de acceso de los afectados a la misma, comprobando también el auditor que ésta no se haya recogido por medios fraudulentos, desleales o ilícitos.

21.5. AUDITORÍA DE LOS ARCHIVOS

Quizá donde la Auditoría Jurídica sea más necesaria es en el terreno del tratamiento de los archivos. Analizamos a continuación distintos aspectos que pueden ser útiles para una mejor comprensión de la materia ante la que nos encontramos, para pasar seguidamente a un recorrido por los diferentes aspectos que el auditor debe examinar.

21.5.1. Niveles de protección de los archivos

La Ley Orgánica 5/92 de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD), señalaba como objetivo el limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, aplicándose tanto a los archivos públicos como privados que contuvieran datos de carácter personal.

21.5.1.1. Archivos excluidos de la aplicación de la lopd

Están incluidos en la ley todos los archivos que contengan información o datos personales salvo los que estén expresamente excluidos, sea efectuada dicha exclusión por la propia ley, sea efectuada por remisión de la misma a regulación específica del tipo de archivo de que se trate.

Como excepciones a la aplicación de la LOPD se reseñan en su art. 2.2.

21.5.1.2. Archivos con regulación específica

Determinadas materias se regirán por sus disposiciones propias. Así, existen regulaciones específicas en materia de régimen electoral, Ley Orgánica 5/85 de 19 de junio, Ley Orgánica 13/94 de 30 de marzo, que modifica la anterior; materias clasificadas (secreto oficial), de Ley 9/68 de 5 de abril y Ley 48/78 de 7 de octubre que modifica la anterior; Registro Civil, Ley de 8 de junio de 1957, Reglamento del Registro Civil, Decreto de 14 de noviembre de 1958; Registro Central de Penados y Rebeldes; los datos que sirvan exclusivamente para fines estadísticos amparados por la Ley 12/89 de 9 de mayo de la Función Estadística Pública; los informes personales a que se refiere el artículo 68 de la Ley 17189 de 19 de julio del régimen del personal militar profesional.

21.5.1.3. Grados de protección

Dentro de los archivos sometidos a la Ley y en relación con los datos en ellos contenidos, podemos hablar de diversos grados de protección. Se regulan en los arts. 7 y 8 de la LOPD tres tipos de protección, máxima, media y mínima. *La protección máxima* se otorga a datos referentes a ideología, religión o creencias y por la cual nadie podrá ser obligado a declarar sobre estos datos, salvo que el afectado consienta expresamente y por escrito; existe una obligación de advertir al interesado a su derecho a no prestar su consentimiento. *La protección media* se otorga a los datos que se refieran al origen racial, salud o vida sexual, y sólo podrán recabarse cuando por razones de interés general lo disponga una ley. *La protección mínima* se refiere a la obligación de toda persona o entidad que proceda a la creación de archivos automatizados de datos de carácter personal de notificarlo previamente a la Agencia de Protección de Datos. Dicha notificación deberá contener necesariamente el nombre del responsable del archivo, la finalidad del mismo, su ubicación, el tipo de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar. Deberán comunicarse a la Agencia de Protección de Datos también los cambios que se produzcan en la finalidad del archivo automatizado, en su responsable y en la dirección de su ubicación.

El Registro General de protección de datos inscribirá el archivo automatizado si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el archivo automatizado a todos los efectos.

21.5.2. Mecanismos de seguridad del archivo

En cuanto a la seguridad de los datos, el artículo 9 de la LORTAD establece que el responsable del archivo (figura creada por la LORTAD, que se analiza en el apartado siguiente) deberá adoptar medidas necesarias para mantener la seguridad de los datos y evitar la alteración, pérdida o acceso no autorizado a los mismos. El auditor debe verificar si estas medidas se han establecido, así como el método de implantación.

Además, y como ya hemos visto anteriormente, tanto el responsable del archivo como las demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del archivo, tienen la obligación del deber de secreto. El auditor deberá comprobar si el responsable, máxime encargado de la integridad y seguridad de los archivos, ha verificado las medidas oportunas y si procura por la seguridad
de aquéllos.

21.5.3. Formación de la figura del responsable del archivo

La figura del responsable del archivo es creada por la LORTAD, que la define en su artículo 3 como la persona física, jurídica de naturaleza pública o privada u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento citado.

El responsable del archivo actúa como cabeza visible de la seguridad de los archivos. A pesar de que la puesta en práctica de las medidas sea llevada a cabo por otras personas dentro de la organización, aquél se convierte en el máximo responsable, de manera que la toma de decisiones en ese campo sólo a él le corresponde, y no a otros miembros de la organización, aunque participen en el tratamiento automatizado de los datos.

El auditor debe comprobar la existencia de un responsable real del tratamiento automatizado de datos, dotado de la autoridad suficiente, de modo que éste pueda cumplir las funciones que le están encomendadas y así evitar (recordemos la función preventiva) las irregularidades de aquel tratamiento. Pero no debe controlar tan sólo la posibilidad efectiva de desenvolvimiento de sus tareas, sino que también debe verificar si ésta se lleva a cabo dentro de los límites correspondientes. Así, y a modo de ejemplo, el responsable tiene, entre otras:

a) La obligación de comunicar al afectado la cesión de datos.

b) La obligación de confidencialidad.

c) La obligación de hacer efectivo el derecho de acceso.

d) La obligación de hacer efectivo el derecho de bloqueo.

e) La obligación de hacer efectivo el derecho de cancelación.

f) La obligación de hacer efectivo el derecho de rectificación.

g) La obligación de hacer efectivo el derecho de supresión.

h) La obligación de informar del tratamiento de los datos, la obligación de informar en la recogida de los datos...

Existe un procedimiento administrativo de reclamación ante la Agencia de Protección de Datos por incumplimiento de aquellas obligaciones que, como hemos señalado anteriormente, puede finalizar en cuantiosas sanciones, por ello, el auditor jurídico debe verificar si el comportamiento del responsable se ajusta a aquellas obligaciones por el propio interés del auditado.

a) Requisitos de creación de archivos de titularidad pública y de titularidad privada

La LORTAD parte de la distinción titularidad privada/titularidad pública para el análisis de los archivos, previendo distintos requisitos para su creación, modificación y extinción. Otra tarea del auditor jurídico es la de verificar que se hayan cumplido los requisitos exigidos.

En cuanto a los **archivos de titularidad pública,** *la creación, modificación o supresión de los mismos sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.* Dichas disposiciones de creación o modificación deberán indicar: a) La finalidad del archivo y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del archivo automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal que, en su caso, se prevean. f) Los órganos de la Administración responsables del archivo automatizado. g) Los servicios o unidades ante los que pudieran ejercitarse los derechos de acceso, rectificación y cancelación. En las disposiciones que se dicten para la supresión de los archivos automatizados se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

En cuanto a los **archivos de titularidad privada** que contengan datos de carácter personal, podrán crearse cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que la LORTAD establece para la protección de las personas. *Toda persona o entidad que proceda a la creación de archivos automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos. La notificación deberá contener necesariamente el responsable del archivo, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.* Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del archivo automatizado, en su responsable y en la dirección de su ubicación. El Registro General de Protección de Datos inscribirá el archivo automatizado si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el archivo automatizado a todos los efectos.

a) Verificación del consentimiento

Seguidamente hacemos referencia al que la LORTAD denomina afectado[19], es decir, el titular de los datos que se tratan. Para que el tratamiento de datos, en cualquiera de sus fases, cumpla la legalidad vigente, se debe recabar siempre el consentimiento del afectado: ello se regula en el art. 6 de la LORTAD, siendo regla necesaria que el tratamiento automatizado, salvo algunas excepciones, requiera consentimiento del afectado. Ese consentimiento deberá manifestarse en dos momentos: en la recogida de la información y en la cesión, en su caso. Es tarea del auditor jurídico la comprobación de la existencia de dicho consentimiento y que el mismo se ha recabado atendiendo a los requisitos legales.

El consentimiento se podrá otorgar en cualesquiera de las formas admisibles en Derecho. Salvo para aquellos casos en que la Ley Orgánica prevea que el consentimiento haya de otorgarse expresamente, podrá otorgarse tácitamente o de modo presunto. Para que el consentimiento sea válido se requiere que los datos no se recaben por medios fraudulentos, desleales o ilícitos. El consentimiento dado puede ser revocado en cualquier momento, pero no se le podrán atribuir efectos retroactivos a la revocación. En el caso de datos especialmente protegidos, referidos a la ideología, religión o creencias, se deberá advertir explícitamente sobre el derecho del interesado

[19] Según el artículo 3 e) de la LORTAD el afectado es la persona física titular de los datos que sean objeto de tratamiento a que se refiere el apartado c) del mismo artículo. El apartado c) define el tratamiento de datos como las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

a no prestar su consentimiento. Asimismo, será requisito para la validez del consentimiento que de modo previo e inequívoco se advierta al interesado de la existencia de un archivo automatizado, de la finalidad del mismo, de los destinatarios de la información, del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del archivo. Cuando se utilicen cuestionarios u otros impresos para la recogida deben figurar las advertencias señaladas en los puntos anteriores.

En cuanto al consentimiento para la cesión, éste ha de ser previo, requiriéndose además que el cesionario sea determinado o determinable, en caso contrario el consentimiento será nulo. El que el concepto de cesionario sea determinado o determinable significa que serán nulas las cesiones o autorizaciones excesivamente amplias en la que se deje en manos del cedente la decisión de ceder los datos a una u otra persona y el afectado no pueda saber en último término, mediante reglas sencillas de identificación, quién dispone de sus datos personales. También será nulo el consentimiento cuando no conste la finalidad de la cesión.

El auditor debe comprobar la plasmación efectiva de estos requisitos teniendo en cuenta también que se prevén una serie de excepciones al consentimiento del afectado[20].

El afectado es el verdadero propietario de sus datos personales, de la información que desprende y, por tanto, es sólo él quien debe consentir su uso (en caso de menores de edad el consentimiento sería el del tutor). Por ello, hay que establecer los controles necesarios para garantizar que el afectado ejerza su derecho de consentir el uso y cesión de sus datos, ya sea tácito o expreso en el caso de datos de salud y los

[20] La LORTAD establece concretamente cuando una ley dispone otra cosa, cuando se recogen en fuentes accesibles al público, siempre que los datos provengan de archivos de titularidad privada que se recojan para el ejercicio de las funciones propias de las Administraciones Públicas, que se refieran a personas vinculadas por una relación negocial, laboral, administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato, que la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas, cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19 de la LORTAD, cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un archivo automatizado, o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

especialmente protegidos, garantizando que se cancelen cuando dejen de ser necesarios[21].

Debe evitarse con ello que se siga con la negativa práctica habitual en la que no se pide el consentimiento ni para el uso, ni para la cesión, o no se clarifica suficiente ni uno ni otro en la toma de datos (no se cumple con el derecho a la información en la recogida de datos). También es frecuente encontrarse que en el derecho de acceso, rectificación y cancelación se esté negando parte de la información que se tiene de un afectado, de manera sistemática y consciente, debido al origen irregular por cesiones ilícitas que comportarían borrarlas para regularizar añadiéndose a los costes de recogida y de regularización[22]. Pero dichos costes son mínimos si se comparan con las sanciones e indemnizaciones que hemos mencionado en la introducción de este trabajo.

El auditor debe señalar aquellos defectos que aprecie en el otorgamiento del consentimiento por parte del afectado a la empresa privada o Administración Pública auditada; aquellas irregularidades jurídicas que, precisamente por ser dicho auditor independiente, puede ayudar a subsanar al mismo tiempo que se evitan de cara al futuro, colaborando con su consejo, a la creación de una mentalidad respetuosa con la intimidad del ciudadano dentro de la estructura que audita.

c) Mecanismos de defensa de los incluidos en el archivo

El afectado tiene unos derechos por ley, reconocidos en la LORTAD, en relación con la inclusión de sus datos en un archivo. Estos derechos tienen carácter personalísimo, por lo que sólo pueden ejercerse por parte del mismo o su representante legal. Los derechos son los siguientes: derecho de impugnación, derecho a la información en la recogida de datos, derecho de acceso, derecho de rectificación y derecho de cancelación. El auditor debe comprobar que estos derechos se respetan

[21] En materia de prestación de servicios de información sobre solvencia patrimonial y crédito existe la obligación de comunicar la inclusión en estos archivos que se extiende tanto a los supuestos de información sobre solvencia patrimonial y crédito, como a la información relativa al cumplimiento o incumplimiento de obligaciones dinerarias, con independencia del origen de los datos. La notificación de la inclusión de datos personales en el archivo se efectuará en el plazo máximo de 30 días, informando al afectado de su derecho a recabar información sobre los datos recogidos en el archivo. La inscripción en el archivo común de la obligación incumplida se efectuará, bien en un solo asiento si fuese de vencimiento único, bien en tantos asientos como vencimientos periódicos incumplidos existan, señalando la fecha de cada uno de ellos, en este caso. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores. El responsable del archivo deberá adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y la fecha de entrega o intento de entrega de la misma. La notificación se dirigirá a la última dirección conocida del afectado a través de un medio fiable e independiente del responsable del archivo.

[22] GONZÁLEZ ZUBIETA, J. M., "Control Informático y marco jurídico (II)", *SIC seguridad en informática y comunicaciones*, nº 23, febrero 1997, año VI.

verdaderamente y se cumplen efectivamente; en definitiva, si tienen un eficaz reflejo en la práctica, al procurarse por parte de la empresa o Administración Pública, a través del responsable, su cumplimiento.

El afectado puede impugnar **(derecho a la impugnación,** art. 12 de la LORTAD) los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad. Este derecho guarda evidentemente una estrecha relación con el derecho de acceso que analizamos más adelante.

El afectado debe haber sido informado en la recogida de datos **(derecho de información en la recogida de datos, artículo 5 de la LORTAD)** de modo previo e inequívoco de la existencia de un archivo automatizado, de la finalidad del mismo, de los destinatarios de la información, del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, de la identidad y dirección del responsable del archivo[23].

Cuando se utilicen cuestionarios u otros impresos para la recogida deben figurar las advertencias señaladas en los puntos anteriores. No será necesaria la información referida anteriormente si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

El auditor comprueba que dicha información sea debidamente suministrada, verbalmente o por escrito, en su caso, haciendo efectivo el derecho a la información, y que por lo tanto los datos obtenidos en ese ámbito junto con los otros requisitos legales exigidos, sean objeto de un tratamiento automatizado correcto.

En lo referente al **derecho de acceso** (art. 14 de la LORTAD, arts. 12 y 13 del RD 1332/94), consiste en la facultad o capacidad que se reconoce al afectado de

---

[23] Sobre los datos almacenados (artículo 13 de la LORTAD), el Registro General de Datos en la Agencia de Protección de Datos tiene asignada la misión de dar a conocer la existencia de los archivos automatizados de datos de carácter personal, para hacer posible el ejercicio de los derechos de acceso, rectificación y cancelación. Es un registro de consulta pública y gratuita. En el Registro General queda inscrita una descripción de los archivos automatizados que tienen la obligación legal de inscribir. Por tanto, se puede averiguar mediante consulta al Registro de información aspectos concretos de los archivos, tales como su finalidad, estructura, identidad del responsable del archivo, ubicación, cesiones previstas... pero la Agencia no dispone de datos personales de los afectados. La principal información que facilita la Agencia es la dirección de la oficina o dependencia del responsable del archivo ante la que se ejercen los derechos de acceso, rectificación y cancelación. Es el responsable del archivo el que dispone de los datos y el que puede rectificarlos o cancelarlos, o bien dar acceso al afectado sobre sus datos. La función de la Agencia es informar al afectado para que pueda ejercer los derechos que la Ley Orgánica le reconoce. Para el caso de que el responsable del archivo desatienda la solicitud del afectado está previsto, como hemos comentado anteriormente, el Procedimiento de Tutela de Derechos.

recabar información de sus datos de carácter personal incluidos y tratados en los archivos automatizados, en intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo. El acceso podrá consistir en la mera consulta de los archivos por medio de la visualización, o en la comunicación de los datos pertinentes por escrito, copia o telecopia, certificada o no por el responsable del archivo. La información deberá ser legible o inteligible cualquiera que sea el medio utilizado. El derecho se ejercerá mediante solicitud o petición dirigida al responsable del archivo, formulada mediante cualquier medio que garantice la identificación del afectado y en la que conste el archivo o archivos a consultar. El responsable del archivo resolverá la petición de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso se puede denegar en el caso de los archivos de titularidad privada sólo cuando la solicitud sea llevada a cabo por persona distinta al afectado o cuando se pida sin acreditar interés legítimo en un número de veces superior al establecido por la ley para un plazo de tiempo determinado.

En el caso de los archivos de titularidad pública, se puede denegar el acceso cuando se trate de archivos de las Fuerzas y Cuerpos de seguridad para fines policiales, que contengan datos de carácter personal, cuando el ejercicio del derecho de acceso pudiera ser una amenaza contra la defensa del Estado, la seguridad Pública, la protección de derechos y libertades de terceros, o las necesidades de las investigaciones que se estén realizando por parte de los Cuerpos y Fuerzas de Seguridad. En el caso de los archivos del Ministerio de Economía y Hacienda podrá denegarse cuando se obstaculicen actuaciones administrativas para asegurar el cumplimiento de las obligaciones tributarias. En el caso de las Administraciones Públicas podrá denegarse también por razones de interés general o intereses de terceros más dignos de protección cuya existencia deberá llevarse a cabo mediante resolución motivada del órgano administrativo responsable del archivo. El afectado al que se deniegue estos derechos podrá ponerlo en conocimiento del director de la Agencia de Protección de Datos, que se asegurará de la procedencia o improcedencia de la deregación. Este derecho sólo podrá ser ejercido en intervalos superiores a doce meses, salvo que el afectado acredite un interés legítimo, en cuyo caso podrá ejercitarse antes.

La información que recibe el afectado comprenderá los datos de base del mismo y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos, facilitándose la irformación de modo perfectamente comprensible.

El derecho de rectificación y cancelación, regulado en el art. 15 de la LORTAD y art. 15 del RD 1332/94 se basa en el principio de la obligación de mantener la exactitud de los datos. Es la facultad o capacidad del afectado de instar al responsable del archivo a cumplir la obligación de mantener la exactitud de los mismos, rectificando o cancelando los datos de carácter personal cuando resulten incompletos e inexactos o bien sean inadecuados o excesivos, en su caso. En definitiva, es una

llamada a la existencia y uso por parte del responsable de mecanismos de actualización de los archivos. Su finalidad de evitar daños y perjuicios a los afectados por la tenencia de datos erróneos o inexactos.

Cuando los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del archivo deberá notificar la rectificación y cancelación efectuada al cesionario.

El derecho debe ejercerse mediante solicitud o petición dirigida al responsable del archivo mediante cualquier medio que garantice la identificación del afectado y en la que consten los datos que hay que cancelar o rectificar y el archivo o archivos donde se encuentran, haciéndose efectiva la rectificación por el responsable del archivo dentro de los cinco días siguientes al de la recepción de la solicitud. Si el titular considera que no procede acceder a lo solicitado se lo comunicará motivadamente en el plazo de cinco días. Si transcurrido el plazo de cinco días no contesta, podrá entenderse su petición desestimada. La denegación de la rectificación o cancelación opera en los casos previstos en los arts. 15.5, 21 y 22 de la LORTAD. El afectado al que se deniegue estos derechos podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos, que se asegurará de la procedencia o improcedencia de la denegación[24].

A modo de ejemplo se adjuntan en el Anexo I un grupo de formularios útiles para el ejercicio de los citados derechos y que sería conveniente que el responsable del archivo pudiera facilitar al interesado con la finalidad de garantizar la efectividad del ejercicio de los correspondientes derechos.

d) Tutela de los derechos

La LORTAD prevé mecanismos de tutela de los derechos de los afectados que, como hemos visto, pueden comportar sanciones o indemnizaciones cuantiosas para aquel que haya desatendido los reseñados derechos. A modo de síntesis recordemos las vías de las que goza el particular para hacer valer sus derechos:

[24] En el caso tanto de los archivos privados como de los archivos públicos existe un deber de conservación de los datos para el plazo que se establezca en cada caso por la legislación aplicable y, en todo caso, cuando su cancelación pudiese causar perjuicio al afectado o a terceros. Esta disposición es común a ambos tipos de archivos. Existen unas excepciones específicas previstas para los archivos públicos que podrán denegar, además, en otros casos como el de los archivos de las Fuerzas y Cuerpos de Seguridad para fines policiales que contengan datos de carácter personal, cuando su ejercicio pudiera ser una amenaza contra la defensa del Estado, la Seguridad Pública, la protección de derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando por parte de los Cuerpos y Fuerzas de Seguridad.

A) Reclamación en vía administrativa: Procedimiento de tutela de derechos. Procedimiento sancionador. Supone la búsqueda del respeto efectivo de los derechos reconocidos por la LORTAD y, en caso de que no se produzca, la sanción de las conductas irrespetuosas con los mismos[23].

B) Recursos ante los Tribunales: Recurso contencioso-administrativo contra las resoluciones del Director de la Agencia. Una vez finalizado el procedimiento administrativo ante la Agencia de Protección de Datos y recaída resolución del Director de la Agencia queda expedita la vía contencioso-administrativa.

C) Derecho de indemnización: Como hemos comentado anteriormente, la LORTAD abre definitivamente la puerta al derecho de indemnización. Así, las lesiones que el incumplimiento de los preceptos de esta Ley Orgánica puedan producir al afectado en sus bienes o derechos generan derecho de indemnización, bien de acuerdo con el procedimiento establecido de *responsabilidad* de las Administraciones Públicas, en el caso de los archivos de titularidad pública, o bien ante los Tribunales ordinarios para los archivos de titularidad privada.

La función del auditor es precisamente emitir un diagnóstico jurídico del sujeto auditado con la finalidad de que éste adopte las medidas correctoras oportunas y, con ello, evite que el afectado deba acudir a los citados procedimientos, concluidos normalmente con importantes sanciones.

21.6. CONCLUSIONES

Cada vez más lo contenido dentro de los computadores es el "activo real" de las empresas y Administraciones Públicas. Pero la incorporación de la informática en el hacer cotidiano de las mismas añade una nueva dimensión a controlar. A pesar de las notables ventas que ésta comporta, su uso también conlleva notables peligros que deben someterse a examen de no querer traducirse en elevados costes personales y económicos consecuencia de un estricto régimen sancionador. Con esta finalidad nace la auditoría jurídica dentro de la auditoría informática.

Con ella se pretende poner de manifiesto las irregularidades existentes para poder corregirlas y actuar *ex nunc* del modo legalmente indicado. La auditoría a la que se refiere este capítulo es un proceso controlado en todo momento por el sujeto auditado

[23] Las sanciones oscilan entre las 100.000 pesetas, mínimo previsto para las infracciones leves, y los 50.000.000 de pesetas, máximo previsto para las muy graves. Como ejemplo de las primeras señalamos el no proceder a la rectificación o cancelación de errores o inexactitudes o no cumplir las instrucciones del Director de la Agencia de Protección de Datos ni facilitar información. De las segundas, recordamos como ejemplo la recogida de datos de forma engañosa y fraudulenta o la cesión de datos fuera de los casos permitidos.

que es quien, en último término, decide si desea aplicar las medidas de adaptación a la legalidad que indicará el auditor.

La auditoría no es un procedimiento sancionador sino un procedimiento corrector que pretende evitar, precisamente, sanciones impuestas por parte de órganos administrativos y penales o indemnizaciones en el orden civil.

Es una búsqueda de mejora de la calidad del tratamiento informático a través del consejo independiente que los auditores ofrecen. Ello sin imponer en ningún momento decisiones sino ayudando a tomarlas correctamente.

Cada día son más los que han entendido esta función del auditor jurídico y someten su estructura informática a examen con la intención de adaptar el ámbito informático a los márgenes de la legalidad. Y ello no tan sólo como medida preventiva de costes económicos sino también como fruto de una incipiente concienciación social que propugna el respeto de los Derechos Humanos de Tercera Generación.

21.7. LECTURAS RECOMENDADAS

Davara Rodríguez, Miguel Ángel, *Derecho informático*, Aranzadi. Pamplona, 1993.

Peso Navarro, Emilio del y Ramos González, Miguel Ángel, *Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas*, Ediciones Díaz de Santos, Madrid, 1994.

21.8. CUESTIONES DE REPASO

1. ¿Cuál es la utilidad de la auditoría jurídica de entornos informáticos?
2. ¿Qué áreas comprende la auditoría jurídica?
3. ¿Qué se entiende por auditoría de objetivos?
4. ¿Qué debe verificar el auditor en materia de origen de la titularidad de los programas?
5. ¿Qué aspectos abarca la auditoría jurídica de las personas?
6. ¿Cómo pueden utilizarse los requisitos recogidos en el artículo 4 de la LORTAD a la hora de llevar a cabo la auditoría de la información?

7. ¿Qué archivos quedan excluidos de la aplicación de la LORTAD?

8. ¿De qué grados de protección se puede hablar en relación con los datos contenidos en archivos sometidos a la Ley?

9. ¿Cuáles son las obligaciones del responsable del tratamiento automatizado de datos?

10. ¿Qué legislación conoce sobre derechos de autor que afecte al software?

CAPÍTULO 22

AUDITORÍA INFORMÁTICA EN EL SECTOR BANCARIO

Pilar Amador Contra

22.1. CARACTERÍSTICAS GENERALES DE LA AUDITORÍA INFORMÁTICA EN LAS ENTIDADES FINANCIERAS

22.1.1. Necesidad y beneficios de la auditoría informática en la banca

La creación de la función de la auditoría informática en las organizaciones bancarias es relativamente reciente, hasta el punto de que aún actualmente en algunas entidades financieras se encuentra en proceso de definición o consolidación.

Sin embargo, su existencia aporta innumerables ventajas a las entidades que disponen de ella, ventajas que, si bien en ocasiones muestran elementos de coincidencia con las habidas en cualquier sector empresarial, en otros casos son específicamente propias y derivadas de las características particulares del negocio bancario.

El valor añadido que representa para una entidad financiera la existencia en su organización de una función de auditoría informática plenamente operativo abarca diversos aspectos.

Una de las tareas clásicas en cualquier actividad auditora es la relacionada con las funciones de control, por cuanto está dentro de su ámbito de actuación verificar la existencia de procedimientos y mecanismos de control suficientes y adecuados que, operando principalmente a nivel preventivo y detector, permitan asegurar

razonablemente el funcionamiento correcto de los sistemas informáticos, y lo que es más, evaluar la implicación de la inexistencia, la insuficiencia o la no adecuación de dichos procedimientos. En último extremo, es la bondad de las medidas de control implantadas la que permitirá al auditor en particular, y a la entidad en su conjunto en general, determinar el grado de confianza a depositar en el sistema informático.

A este respecto, la faceta en la que la participación de auditoría informática en el sector financiero es más valiosa la constituye, quizás, la revisión de las aplicaciones informáticas, con el objeto de asegurar que ellas cumplen con los criterios funcionales y operativos definidos por la entidad financiera. Esta actividad, que forma parte del ámbito de actuación habitual de la auditoría informática en todos los bancos que tienen como tal implantada la función, es de extrema importancia por cuanto comúnmente un error en la interpretación de un criterio, una especificación incompleta, una deficiencia en un algoritmo, suelen tener un impacto elevado, bien por el número de operaciones que resulten afectadas, bien por la repercusión económica del error.

Y no sólo ésos pueden ser los efectos de una mala definición o implantación de las especificaciones de diseño. Aun cuando es general el concepto de que los bancos contribuyen a la actividad económica de un país como empresas de servicios en el mercado financiero, no es tan común considerarlos como entidades suministradoras de servicios de información, si bien una importante cantidad de sus recursos e inversiones a esta actividad. Los sistemas de información de bancos y entidades financieras tienen, entre sus características particulares, la de constituir fuente de datos para múltiples agentes externos. El negocio bancario se caracteriza porque sus procesos, aun cuando no son excesivamente complejos si se comparan con los de otras actividades empresariales, están todos ellos muy interrelacionados, tanto dentro de la propia organización financiera como a nivel externo. Como consecuencia, los efectos de los posibles errores pueden tener repercusiones directas o indirectas en múltiples niveles, en un abanico de posibilidades que van desde el ámbito interno en exclusiva hasta, en el peor de los casos, afectar a la información proporcionada a terceros, principalmente, organismos públicos y, sobre todo, clientes.

A este respecto, es indudable la importancia actual que se le concede al cliente en el sector bancario, por cuanto la clientela es, a la vez, origen y destino de la propia actividad bancaria. Y desgraciadamente, es innegable también que entre los principales afectados por los errores en los sistemas informáticos de los bancos se encuentran, en ocasiones, los clientes. No es el objeto tratar aquí los aspectos asociados a las implicaciones que para un cliente puede tener un error, ni tampoco las que directamente o indirectamente, derivadas de las anteriores, puede tener para un banco, pero es claro que todos los errores tienen un coste, no siempre totalmente cuantificable. De ahí la importancia de la auditoría informática en cuanto que garantizadora del correcto funcionamiento de los sistemas, no sólo desde la perspectiva de la gestión de la propia empresa, sino también desde la óptica de los clientes.

Uno de los valores que de forma colateral, y debido al ámbito en el que actúa, suele aportar la auditoría informática en las entidades financieras es la detección de procesos obsoletos, ineficaces o redundantes, que no añaden valor a la actividad de negocio y, sin embargo, sí suponen un coste. En el transcurso de su trabajo, el auditor informático tiene la oportunidad de analizar los circuitos de información, los procesos operativos relacionados con los productos y tratamientos informáticos, la bondad y/o adecuación de los mismos en relación con el objetivo teóricamente perseguido, y en definitiva, proponer acciones de mejora que, sin menoscabo de la calidad real de los procesos, redunden en un mejor aprovechamiento de los recursos.

Con todo, la concienciación y el reconocimiento de la importancia de la auditoría informática ha venido de la mano de la entrada en vigor de la LORTAD y de las Instrucciones de la Agencia de Protección de Datos, en particular la que establece la obligatoriedad de realizar una auditoría informática periódica de las medidas de seguridad con que cuentan las instalaciones que procesan datos personales y patrimoniales.

22.1.2. Tipología de las actividades a auditar

No analizaremos aquí toda la casuística de posibles actividades a auditar en aquellas áreas que son comunes a cualquier otra actividad empresarial (auditorías de seguridad lógica, seguridad física, etc.) y, por tanto, no presentan particularidades especiales en el sector bancario.

En su lugar, nos centraremos en las actividades de auditoría en el marco de procesos y funciones en las que existen características de especial interés en el caso de una entidad financiera.

Distinguiremos en primer lugar, por su importancia en el conjunto de procesos informáticos de un banco, así como por las implicaciones de cualquier posible error, *las auditorías de aplicaciones informáticas que tratan y soportan productos bancarios* típicos: planes y fondos de pensiones, fondos de inversión, cuentas corrientes, de ahorro, de plazo y demás productos del pasivo tradicional, inversión crediticia (créditos, préstamos, descuento de efectos), etc. De las auditorías de este tipo se hablará en más detalle con posterioridad.

Estas aplicaciones tienen básicamente las siguientes características:

- Procesan y generan un gran volumen de datos relativos a contratos y operaciones.

- Los procesos de tratamiento de los datos son relativamente sencillos (aun cuando en algún caso puedan resultar conceptualmente complejos); sin

embargo, comparativamente suponen un gran consumo de recursos en el total de los procesos informáticos de un banco.

- Las operaciones y productos tratados por estas aplicaciones tienen normalmente un importante peso específico en el balance de la entidad.

- La disponibilidad de la información suele ser un factor crítico.

- La información generada tiene un elevado alcance, por cuanto se envía masivamente hacia destinos externos a la propia entidad financiera.

- En estas aplicaciones se produce un efecto amplificado del error: cualquier incidencia puede afectar a un número elevado de operaciones y tener una repercusión económica cifrada en millones de pesetas.

En segundo lugar podemos distinguir las *auditorías de medios de pago*: tarjetas de débito y crédito, transferencias de fondos, cheques personales, cheques de viaje, etc.

Entre las particularidades de estos sistemas destacan:

- Alto volumen de transacciones y de clientes.

- Existencia de regulaciones específicas para su tratamiento informático y operativo, consecuencia de los convenios suscritos con distintos organismos.

- Son áreas en las que los aspectos de control tienen gran relevancia, principalmente en materia de prevención de fraudes, así como en el cumplimiento de diversas normas emitidas por el Banco de España.

Otro de los ámbitos de actuación lo constituyen las *auditorías informáticas de actividades y productos de tesorería*: mercados de activos financieros, y de opciones y futuros, principalmente.

Destacan porque:

- Son áreas muy técnicas y especializadas desde el punto de vista bancario.

- El número de transacciones (operaciones) no es muy elevado pero sus importes sí son muy significativos.

- Las salidas de información hacia clientes son escasas (sobre todo si se las compara con las habidas en las aplicaciones de productos bancarios típicos) o nulas.

- Son sistemas en los que una deficiencia en los procesos y/o en los procedimientos de control puede provocar un quebranto económico de considerable magnitud.

Como colofón, señalaremos las *auditorías relacionadas con la información, en* las siguientes facetas:

- Auditorías de calidad de la información, en cuanto que verificación de la existencia de procedimientos que garanticen su exactitud, fiabilidad, oportunidad y utilidad, mediante el análisis de los mecanismos utilizados para su distribución, el intercambio de información entre diferentes departamentos de la entidad, el circuito que siguen los datos desde su creación y las subsiguientes transformaciones (agregaciones, clasificaciones) que experimentan hasta constituir el "producto" final.

- Auditorías de la protección de los datos personales. Entre ellas, destacaremos:

  - Auditoría de las medidas de seguridad de los archivos relativos al cumplimiento o incumplimiento de las obligaciones dinerarias de las personas físicas, de obligada realización a intervalos no mayores de dos años, según establece la Instrucción 1/1995 de la Agencia de Protección de Datos.

  - Auditoría de las medidas de protección de la información de carácter personal y patrimonial que, aun cuando no se pueda considerar amparada dentro de la Instrucción mencionada, sí está regulada por la LORTAD.

- Auditoría de los planes de recuperación de negocio o planes de contingencia. Es un área de especial importancia en la actividad auditora por cuanto actualmente las posibilidades de supervivencia de una entidad financiera en caso de un desastre en cualquiera de sus centros de proceso de datos dependen directamente de la existencia de un plan de recuperación de la actividad.

Por último, señalar que la transformación que está experimentando el sector bancario en los últimos años y, en particular, la instauración de nuevos canales de difusión (banca telefónica, banca virtual), amplían el ámbito de la función auditora más allá de las tareas tradicionales y, al mismo tiempo, exigen del auditor una permanente capacidad de aprendizaje para abordar con éxito los nuevos retos.

22.1.3. Objetivos de la auditoría y preparación del plan de trabajo

El alcance y el ámbito con el que se aborde la auditoría informática de una actividad específica es variable y dependiente de varios factores, entre otros:

- Los objetivos que se persigan con el trabajo y las razones que hayan motivado su realización. Probablemente, el contenido del plan de trabajo difiera en una auditoría de revisión general de un sistema de aquella otra en la que se pretende determinar el origen e aplicaciones de algunas incidencias detectadas en una actividad concreta.
- Los recursos de que se disponga para abordar la auditoría.
- El nivel de documentación del sistema a auditar, puesto que su inexistencia o insuficiencia puede conducir en la práctica a que aquél no sea auditable.

Como características particulares a tener en cuenta en la preparación del plan de trabajo de la auditoría, se destacan las siguientes:

- La conveniencia de que el auditor conozca con el suficiente detalle los procedimientos operativos internos de la entidad financiera relacionados con el área de negocio y/o el producto bancario soportado por la aplicación. El auditor, aun cuando el ámbito de su trabajo se circunscriba al sistema informático, debiera conocer los circuitos operativos y administrativos seguidos y asociados con los datos, desde su captura hasta la obtención de los subproductos finales derivados de ellos. Ello le permitirá evaluar el impacto de las debilidades y errores que pueda detectar en el funcionamiento del sistema, e incluso, poner de manifiesto situaciones en las que no exista la suficiente concordancia entre el sistema informático y el procedimiento operativo.
- La necesidad de contar con especificaciones funcionales documentadas de la actividad a auditar, así como disponer del suficiente conocimiento de la operativa bancaria tradicional asociada con el producto en cuestión. Es innegable que un auditor informático que trabaje para una entidad financiera, además de auditor e informático, deberá ser bancario.
- Como paso previo a la elaboración del plan de trabajo, es extremadamente útil la recopilación de toda la normativa y documentación que pueda existir relacionada con el objeto de la auditoría.

En particular, en el caso de las aplicaciones bancarias típicas en el sector bancario, se destacan como referencias de consulta las diversas circulares e instrucciones emitidas por el Banco de España, la Asociación Española de la Banca Privada (AEB), la Confederación Española de Cajas de Ahorro (CECA), etc.

En ciertas áreas específicas, existen otras fuentes de información que pueden ser también de interés para el auditor, entre las que citamos a título de ejemplo:

- Convenios firmados por la entidad financiera con organismos de las administraciones central o autonómicas para la financiación de ciertas actividades empresariales (préstamos).

- Convenios relacionados con los sistemas de truncamiento de cheques y pagarés, efectos, etc.

- Normas reguladores del Mercado de Anotaciones en Cuenta (valores, activos financieros), del Servicio telefónico del Mercado de Dinero, etc.

En ciertos trabajos específicos, el auditor puede necesitar tener un conocimiento general de la legislación vigente así como las Directivas Comunitarias. A modo de ejemplo, éste el caso de la normativa sobre prevención del blanqueo de capitales, propiedad intelectual, protección de datos personales...

- Ante situaciones que requieran unos conocimientos particularmente técnicos en aspectos bancarios o legales, el auditor debe actuar siempre planteando su consulta a los departamentos competentes. Esto es tanto más necesario cuanto menos documentadas se encuentren las especificaciones funcionales del sistema, o cuando el auditor no esté seguro de que aquéllas han sido dictadas por los órganos funcionalmente responsables de ello. A este respecto, y como premisa básica, el auditor informático no debería en ningún caso asumir de antemano como válidas las funcionalidades implantadas en los sistemas informáticos sin contrastar previamente su bondad con las fuentes de documentación y estamentos que correspondan.

22.2. AUDITORÍA INFORMÁTICA DE UNA APLICACIÓN BANCARIA TÍPICA

Este apartado está dedicado a la actividad auditora en un área que, tradicionalmente, ha sido el objeto principal de la auditoría informática en el sector financiero y, que aún hoy, continúa siendo su mayor consumidora de recursos.

No es el objetivo de este apartado el exponer detalladamente los procedimientos y programas de trabajo de la auditoría de las aplicaciones informáticas; por el contrario, se pretende mostrar algunas de las particularidades de las citadas auditorías cuando éstas tienen como marco el sector financiero, bien porque el elemento auditado sea en sí mismo específico del citado sector, bien porque, aun no siéndolo, existan consideraciones especiales que el auditor debe tener en cuenta.

Resulta imposible, en un libro de carácter general como éste, comentar con el suficiente detenimiento los puntos de control que el auditor debería revisar en el ámbito fijado para el trabajo. En su lugar, se ha considerado que podría ser más interesante para el lector conocer algunos aspectos prácticos de este tipo de auditorías, de manera que cualquier auditor con experiencia en otros sectores empresariales pueda, aplicando sus conocimientos y experiencia, iniciarse en la auditoría informática bancaria.

22.2.1. Criterios para la planificación anual de los trabajos

La realización de la planificación anual de la auditoría informática requiere, como paso previo, un conocimiento general del estado de los sistemas de información con que cuenta la entidad, así como de los objetivos estratégicos fijados por los órganos de decisión. Dentro del ámbito de las aplicaciones informáticas, en particular a la hora de proponer las tareas del plan de trabajo para el próximo período, el responsable del auditoría informática por lo común clasificará las posibles actividades en función de diversas pautas.

En primer lugar, están los factores clásicos, generalmente utilizados en la planificación de auditorías de aplicaciones en cualquier sector empresarial y entre los que podemos destacar:

- Antigüedad de la aplicación, aun cuando este dato tiene una doble valoración, ya que cuanto más antigua sea mayores problemas de obsolescencia, presentará probablemente con procesos poco eficientes o redundantes, especificaciones funcionales no cubiertas, etc.; pero al mismo tiempo, será presumiblemente más fiable, en cuanto a la calidad de la información procesada y generada, puesto que el sistema informático estará también más probado.

- Horas de mantenimiento invertidas anualmente, estableciendo una comparativa entre años, así como con las restantes aplicaciones.

- Factores cualitativos asociados a la posible obsolescencia (no siempre ligada a la antigüedad) de la aplicación, que el auditor podrá determinar analizando a aspectos como la forma y lugar en que se capturan los datos, la dimensión de los tratamientos manuales, la tipología de algunos de los controles que se realizan, la ausencia de datos básicos en relación con el producto o área cubierta por la aplicación, el volumen de recursos que requiere su adaptación al EURO y/o al año 2000, y, en general, aquellas características que a criterio del auditor se –consideren sintomáticas de posible obsolescencia–.

Pero, además, podemos distinguir un conjunto de aspectos típicamente bancarios a considerar en la planificación de la revisión de aplicaciones:

- Importancia económica de la función a la que se dedica la aplicación, esto es, su impacto en el balance del banco.

- Importancia de la actividad bancaria a que da soporte la aplicación en los planes de negocio y expansión de la entidad.

- La obtención de información a partir de la aplicación con destino a clientes y organismos públicos (Ministerio de Economía y Hacienda, Banco de España, diversos organismos adscritos a las autonomías).

- El volumen, la frecuencia y la importancia material de las incidencias y errores detectados mediante los mecanismos de control habituales; la existencia de posibles reclamaciones interpuestas por clientes ante diversos estamentos (la propia oficina bancaria o bien otros departamentos internos, el Defensor del Cliente o la Oficina de Reclamaciones del Banco de España).

- La existencia de descuadres entre los datos facilitados por la propia aplicación y los registrados en la contabilidad de la entidad.

Para finalizar este apartado, queremos hacer hincapié en dos aspectos que nos parecen, relevantes. De cara a abordar la planificación de trabajos, es particularmente importante que el auditor sea receptivo a las propuestas recibidas de cualquier estamento de la organización, puesto que son los propios usuarios de los servicios informáticos los que mejor suelen conocer –y en ocasiones padecer– los sistemas de información que utilizan.

Junto con ello, otro de los factores que consideramos crítico es la sensibilidad del auditor hacia el error, esto es, hacia aplicaciones, procesos y datos que estén dando muestras de errores, quizá no muy numerosos, ni muy importantes si se consideran de forma aislada, incluso pueden ser de tipología diversa y aparentemente no relacionados, pero con la característica común en todos los casos de que se producen de manera continua en el tiempo. Situaciones como la descrita suelen terminar poniendo de manifiesto tras la realización de la auditoría debilidades importantes en la aplicación, en una o más áreas: especificaciones funcionales poco definidas o mal implantadas, debilidades de control en los procesos, diseño defectuoso de la aplicación, mantenimiento deficiente de los programas informáticos, insuficiente documentación y conocimiento de la aplicación por parte del personal informático encargado del mantenimiento, etc.

22.2.2. Establecimiento del ámbito de la auditoría

La definición del ámbito de la revisión a realizar en el trabajo auditor, esto es, la determinación de las actividades y procesos que serán analizados, depende en primera

instancia del objetivo que pretenda cubrir el trabajo y de las razones que hayan aconsejado su realización.

Así, si la auditoría pretende obtener una visión de conjunto acerca del estado de una aplicación, al objeto de determinar si existen razonables garantías de que los tratamientos informáticos son correctos y la información generada tiene la calidad suficiente, el programa de trabajo probablemente se limitará al estudio de los procesos más relevantes de la aplicación. Podemos decir que, en la mayoría de las aplicaciones que soportan directamente productos bancarios, entre las actividades que casi siempre serán objeto de revisión se encuentran los procesos de liquidación, contabilización y periodificación contable.

Una vez seleccionados los procesos en los que se centrará la auditoría, y siempre y cuando los recursos disponibles así lo permitan, es aconsejable revisar dichos procesos desde un punto de vista integral, contemplando todas las facetas desde la generación del dato hasta la obtención de las diferentes salidas de información, puesto que ello le permitirá al auditor detectar debilidades que, de otra forma, pasarían inadvertidas.

Ahora bien, la aproximación al trabajo será necesariamente distinta si éste se deriva de la existencia de incidencias en algún proceso detectadas por los procedimientos de control habituales en la entidad. En este caso, el ámbito de la auditoría viene ya determinado por el objetivo del trabajo (averiguar las causas e implicaciones de las incidencias detectadas), y, si bien el punto de auditoría será también el estudio detallado del proceso en cuestión, los resultados parciales que se obtengan en el transcurso de la auditoría pueden obligar a redefinir en algún momento, el plan de trabajo.

La auditoría del proceso finalmente seleccionado abarcará las siguientes actividades de revisión:

- Procedimientos de recogida y entrada de datos que, en la mayoría de los casos, se realizarán mediante transacciones de teleproceso, para los que el auditor deberá asegurar la existencia y operatividad de los controles pertinentes. A este respecto, el trabajo de auditoría debería incorporar auténtico valor añadido, es decir, no limitarse a la revisión de los controles informativos típicos de entrada de datos (controles de mínimos y máximos, control de que el formato de los datos es el que corresponde, de fechas lógicas, etc.), sino que, por el contrario, debería centrarse en la revisión de la implantación informática de los controles operacionales definidos en la entidad.

  Por ejemplo, en un sistema organizativo en el que los tipos de interés de las operaciones necesitan ser autorizados por un estamento superior cuando aquéllos no están dentro de un rango de valores, el auditor debería comprobar

que el sistema informático no permite la formalización de la operación de estas características si no existe autorización electrónica para la misma.

O por citar otro caso, en cualquier transacción de alta y modificación de contratos de titulares de operaciones, se debería revisar el control de obligatoriedad de introducción de un DNI/NIF válido al objeto de cumplir con determinadas regulaciones existentes que obligan a la identificación de los clientes.

- Procedimientos de generación de la información de salida del proceso, básicamente la destinada a clientes (extractos de liquidación, comunicaciones de revisión de tipos de interés, etc.) y organismos externos: Hacienda, CIRBE, etc. El auditor, además de verificar que la información es fiable, correcta y completa, debería comprobar también que es conforme con las normas establecidas por los organismos receptores en cuanto a formato y periodicidad de envío y, en lo relativo a clientes, con lo estipulado por el Banco de España en sus circulares en materia de transparencia en las operaciones con la clientela.

A lo largo de toda la exposición se ha comentado la auditoría de procesos considerando que éstos forman parte de una aplicación. Sin embargo, en ocasiones una misma operación, servicio o producto bancario no es tratado en una única aplicación, sino que, por el contrario, es soportado por varias de ellas. Éste sería el caso de una organización en la que la contabilidad constituyera una aplicación propia e independiente del resto, alimentada a partir de los datos generados por el resto de aplicaciones. En un sistema como el descrito, una auditoría del proceso contable tendría una doble vertiente, puesto que se podría optar entre limitarse al propio proceso, asumiendo, por tanto, la bondad y exactitud de los datos recibidos de las aplicaciones que lo nutren, o bien, incluir la revisión de las interfases, esto es, verificar la concordancia entre los datos recibidos y los registrados en los otros sistemas.

22.2.3. Procedimientos de auditoría a emplear

El auditor, en el ejercicio de su actividad y al efecto de cumplir con el objetivo del trabajo, empleará diversos procedimientos y técnicas, entre los que destacaremos:

Análisis de los programas informáticos

Comprende la revisión de las funciones que realizan los programas por medio del estudio del cuaderno de carga y cualquier otra documentación que de ellos exista. Incluye también el análisis del propio código fuente de los programas, la realización de pruebas sobre ellos y la verificación de que cumplen con las especificaciones funcionales definidas.

El auditor deberá perseguir:

- Obtener un conocimiento detallado de la operativo del programa, que además le servirá posteriormente para comprender las aplicaciones de los tratamientos realizados por otros programas de la misma cadena.

- Detectar errores en la interpretación e implantación de las especificaciones Funcionales.

- Garantizar la existencia y operatividad de los controles adecuados.

Esta técnica es inabordable si los programas no están bien modulados o carecen de documentación, lo que ya de por sí es sintomático y pone de manifiesto una debilidad, porque apunta a que el mantenimiento del programa es complejo y susceptible de que se produzcan errores.

Dado que la revisión de programas es una tarea que consume muchos recursos, el auditor deberá seleccionar cuidadosamente los programas y rutinas objeto de revisión, centrándose exclusivamente en aquellos que sean críticos. Sin embargo, este procedimiento presenta la ventaja de que si el auditor es hábil y experimentado, le permite detectar la presencia de caballos de Troya y errores en la interpretación práctica de ciertas especificaciones funcionales.

Realización de controles de coherencia

Son quizá la mejor herramienta de trabajo del auditor, puesto que le facilitan descubrir de una manera muy eficiente ciertas anomalías en el funcionamiento de la aplicación. Se distinguen las siguientes variantes:

- Controles cruzados entre los datos existentes en archivos y bases de datos distintos obtenidos en un proceso común (si lo que se quiere probar es la bondad del proceso), o bien, en procesos distintos.

  Por ejemplo, si se desea comprobar que el saldo que presentan determinadas cuentas es correcto, se pueden utilizar los datos existentes en el archivo de movimientos de las cuentas, de manera que las imputaciones habidas, sumadas algebraicamente y teniendo en cuenta el signo (debe/haber) del apunte, conformarán un saldo que debería coincidir con el existente en el archivo de saldo de cuentas.

- Controles de coherencia sobre la propia base de datos para aquellos datos relacionados entre sí.

Por ejemplo, en una base de datos de préstamos en la que se guardan las informaciones relativas al plazo de la operación (meses comprendidos desde su formalización a su vencimiento), la periodicidad de la liquidación y el número de liquidaciones en la vida de la operación, uno de los posibles controles a realizar es comprobar que el producto de estos dos últimos datos (periodicidad y número de liquidaciones) no es superior al primero (plazo de la operación).

- Controles realizados utilizando programas independientes.

  Procedimiento clásico de auditoría informática, pero muy útil para detectar un mal funcionamiento en los sistemas, aun cuando en este caso el auditor debe garantizar que su programa (en especial si ha sido realizado por él) es adecuado al fin perseguido y proporciona resultados fiables.

  Esta técnica es principalmente de aplicación cuando se desea probar el correcto funcionamiento del programa de la entidad en fórmulas o algoritmos específicos.

  Por ejemplo, el auditor podría aplicar un procedimiento de este tipo en la base de datos anterior para determinar la bondad del dato del plazo de la operación generado por la propia aplicación, utilizando para ello un programa propio que procese las fechas de Normalización y de vencimiento.

22.2.4. Consideraciones a tener en cuenta durante la realización de la auditoría

- Realizar un seguimiento periódico del nivel de cumplimiento del plan de trabajo y evaluarlo a la luz de los hechos que se vayan poniendo de manifiesto en el transcurso de la auditoría. En ocasiones, puede ser interesante introducir modificaciones en el plan inicial y el auditor debería utilizar su lógica para decidir al respecto cuando:

  - Siendo los recursos muy limitados, haya encontrado un grado de cumplimiento razonablemente satisfactorio en ciertas actividades que no aconseje una revisión excesivamente detallada de ellas.

  - Se hayan detectado errores de relevancia en ciertas facetas que impliquen profundizar en el ámbito inicial previsto para ellas y suponga la imposibilidad de abordar algunos otros puntos del programa de trabajo.

- Si durante la auditoría se detectan errores, será necesario:

- Estudiar en detalle la repercusión e implicaciones del error, considerando todos los procesos afectados por él directa o indirectamente.

- Evaluar o, al menos, estimar el impacto económico del error, teniendo en cuenta el número de operaciones afectadas y el período de tiempo desde el que se vienen produciendo.

- Determinar las causas que han motivado el error y, en el supuesto de que éste lleve algún tiempo produciéndose, los fallos existentes en los procedimientos de control, que no permitieron su pronta detección.

- Proponer o recomendar las medidas a tomar para la resolución del error y realizar una estimación aproximada del coste asociado.

– En aquellos casos en que se detecte la inexistencia de los oportunos controles, o bien, aun cuando existan, no tengan operatividad, el auditor debería:

  - Realizar las pruebas y los controles de coherencia entre datos necesarios para determinar las consecuencias prácticas derivadas de la situación, fundamentalmente en materia de errores no detectados.

  - Recomendar los mecanismos de control que solventen la carencia existente.

– Cuando los usuarios de la aplicación hayan dejando sentir sus dudas acerca de un adecuado funcionamiento de la aplicación en algún aspecto concreto, el auditor debería obtener una relación documentada de las distintas incidencias existentes, para, a continuación, proceder a averiguar sus causas.

– Se debe tener presente que, lo que en ocasiones es percibido por el usuario como un mal funcionamiento informático, puede esconder, en realidad, una deficiencia más profunda de tipo operativo u organizativo. Al mismo tiempo, errores percibidos por los usuarios como hechos aislados pueden, en última instancia, ser sólo diferentes manifestaciones de una causa común que la auditoría debería poner de manifiesto.

22.3. AUDITORÍA INFORMÁTICA DE LA PROTECCIÓN DE DATOS PERSONALES

22.3.1. La importancia y el valor de la información en el sector bancario

Como una consecuencia lógica de las funciones que realiza, una entidad financiera dispone de diversa información acerca de la situación patrimonial y personal de cada uno de sus clientes.

Se puede realizar un ejercicio de abstracción pensando en qué datos posee un banco de su clientela. En primer lugar, sus datos personales (nombre, dirección, teléfono), pero muy probablemente dispondrá también de datos profesionales (actividad a la que se dedica, empresa para la que trabaja). Tendrá asimismo la información relativa a todos los productos contratados por el cliente con el banco: posición completa de sus cuentas (saldos e imputaciones realizadas por diversos conceptos), el valor tasado de su vivienda si en algún momento la entidad le ha concedido un préstamo para su adquisición, su nivel de endeudamiento, las inversiones que realiza y los productos en que las materializa, el importe de su nómina...

Pero además, ¿qué conocimiento indirecto se puede obtener a partir de algunas de estas informaciones? Entre otras cosas, se pueden conocer aspectos personales de su vida privada: sus gustos y aficiones, las asociaciones a las que pertenece, las tiendas en las que compra, los lugares que visita, el colegio donde cursan estudios sus hijos y un largo etcétera.

La sensibilidad de la información manejada por una entidad financiera es mayor si se tiene en cuenta la totalidad de sus clientes y productos, así como el nivel de agregación que ello representa. Piénsese en el valor añadido que tiene la información a medida que ésta va siendo más completa; por ejemplo, conocer la posición de todos los clientes de pasivo en todos los productos que tienen contratados es una información más valiosa, y por tanto más sensible, que disponer exclusivamente del saldo de las cuentas de un único-cliente.

Los principales riesgos a los que hace frente la gestión de la información son los siguientes:

- Difusión no autorizada, intencionada o no, hacia destinos improcedentes. A este respecto, es incuestionable el valor que la información bancaria de los clientes puede representar para empresas comerciales y otro tipo de organizaciones.

La confidencialidad es, en general, un tema de especial preocupación en cualquier entidad financiera, puesto que el negocio bancario tiene como una de sus características la de ser una actividad en la que, en mayor o menor grado, interviene la confianza depositada por el cliente en la entidad.

- Obtención de información errónea, por accidente o por manipulación indebida, que además, y como consecuencia de la normativa a la que está sometida la actividad bancaria, es cedida a terceros, con los consiguientes perjuicios que ello pueda ocasionar en última instancia a los clientes.

La combinación formada por el valor de la información y los riesgos a que está expuesta, han propiciado la aparición de diversas regulaciones para protegerla cuyo cumplimiento forma parte del ámbito de revisión de la auditoría informática.

Existen dos factores que, de manera especial, creemos deben ser tenidos en cuenta al abordar cualquier trabajo de auditoría relativo a la calidad (entendida ésta en su más amplio concepto) de la información. En primer lugar, está el hecho de que cada vez en mayor medida existe dentro de las organizaciones una elevada difusión interna de los datos que puede llegar a motivar que una misma información resida en más de una ubicación con medidas de seguridad que deberían ser homogéneas. En segundo lugar, el auditor debe ser consciente de la riqueza que presenta la información a medida que ésta va siendo agregada, comparada con otras fuentes de datos y estudiada evolutivamente.

La combinación de ambos factores (difusión y enriquecimiento de la información) puede conducir a un proceso en el que las organizaciones no lleguen a conocer exactamente el volumen de información de que disponen y, por tanto, no sean capaces de protegerla convenientemente frente a los riesgos expuestos.

No es excesivamente común encontrar organizaciones empresariales que tengan su información clasificada en niveles de seguridad, en función de la sensibilidad, confidencialidad y valor estratégico que aquélla posea. Sin embargo, la adopción de este tipo de prácticas, que surge en general de la necesidad de conocer, mejorar y controlar la distribución de la información existente, se hace más necesaria a medida que surgen regulaciones que obligan a garantizar la protección de los datos personales y financieros de los clientes.

22.3.2. Actividades de auditoría en relación con la protección de datos personales

El ámbito de actuación de la función auditora en este campo se centra en la verificación de la LORTAD y demás Instrucciones promulgadas por la Agencia de Protección de Datos.

22.3.2.1. Auditoría de cumplimiento de la Instrucción 1/1995

El artículo 9.1 de la LORTAD establece que *"el responsable de los datos deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural"*.

La Instrucción 1/1995, publicada en fecha 4/03/95, en su Capítulo 11 obliga a la realización de una auditoría periódica:

1. *Los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de las obligaciones dinerarias deberán acreditar la efectiva implantación de las medidas de seguridad exigidas por el artículo 9.1 de la Ley Orgánica dentro del año siguiente a la publicación de la presente Instrucción (...)*

2. *La implantación, idoneidad y eficacia de dichas medidas se acreditará mediante la realización de una auditoría, proporcionada a la naturaleza, volumen y características de los datos personales almacenados y tratados, y la remisión del informe final de la misma a la Agencia de Protección de Datos.*

5. *El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles destinados a garantizar la integridad y confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencias o insuficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basan los dictámenes alcanzados y recomendaciones propuestas.*

6. *Adicionalmente, los sistemas que almacenen o procesen información relativa al cumplimiento o incumplimiento de obligaciones dinerarias deberán someterse a una nueva auditoría tras la adopción de las medidas específicas que, en su caso, la Agencia determine, a resultas del informe inicial de*

auditoría. En todo caso, dichos sistemas deberán ser auditados periódicamente, a intervalos no mayores de dos años."

En el momento en que se promulgó esta Instrucción, se suscitaron diversas dudas acerca de su alcance. Así, se planteaba si su ámbito de aplicación se limitaba a los archivos de solvencia patrimonial o crédito formados por agregación de los archivos de las entidades acreedoras (los citados archivos agregados están tratados en el Capítulo 1 de la Instrucción) o si, por el contrario, amparaba también a los segundos. También se cuestionaba si, en el supuesto de que el ámbito de la Instrucción estuviera limitado al archivo agregado, llamado en ella "común", era de aplicación para los bancos y demás entidades financieras o estaba restringido a aquellas sociedades que, específicamente, prestan servicios de información sobre solvencia patrimonial y crédito, como puede ser el caso del ASNEF.

Finalmente, la opinión más generalizada, sustentada en algunas consultas efectuadas a la Agencia, fue que se deben considerar afectadas por dicha Instrucción y, por tanto, sujetas a la obligación de ser auditadas, las entidades financieras que posean copia de los archivos agregados, y en especial, del RAI (Registro de Aceptación de Impagados).

Por lo que respecta a la realización de la auditoría en sí, ésta debería verificar el cumplimiento de los controles en las siguientes áreas:

- Controles de procedimientos y normas operativas:
  - Verificación de la existencia de procedimientos documentados, de aplicación en toda la entidad, que establezcan las medidas a cumplir en cuanto al archivo y distribución de la información:
    - Etiquetado, transporte y destrucción de los soportes de datos (cintas, *cartridges*, disquetes).
    - Período de retención (archivo) de archivos y sus copias de seguridad; procedimiento de borrado de los datos a la finalización del período de retención.
    - Transmisiones de archivos.
  - Verificación de la existencia de normas de actuación a seguir por los empleados:
    - Políticas de concienciación en materia de seguridad que profundicen en la importancia de la confidencialidad de la información, los riesgos a los que se enfrenta y las posibles implicaciones derivadas de la materialización de esos riesgos.
    - Normas escritas que especifiquen el código de ética establecido por la entidad y de obligado cumplimiento por todos los empleados.

- Controles relacionados con la seguridad física:

  - Comprobación de la operatividad y adecuación a los fines a los que van destinadas de las medidas de control existentes en materia de acceso a las instalaciones y de acceso a los soportes de datos (tanto en las distintas instalaciones de proceso como en el lugar de almacenamiento secundario de respaldo).

  - Verificación de las medidas de seguridad en relación con el transporte físico de los soportes de datos, tanto entre las distintas instalaciones en que se procesa, como desde éstas al almacenamiento secundario y viceversa.

- Controles relativos a la seguridad lógica:

  - Verificación de que están implantados controles de acceso a los archivos y bases de datos, en los distintos entornos en que éstos residan, que eviten que aquéllos puedan ser indebidamente leídos, copiados o alterados.

  - Verificación de que la entidad tiene formalmente definido un registro de usuarios autorizados a acceder a cada uno de los archivos de datos en el que se especifique el modo de acceso (lectura, copia, etc.) que cada usuario tiene permitido. Comprobación del procedimiento establecido para la inclusión y baja en dicho registro.

  - Comprobación de que existe un registro de los intentos de acceso al sistema no autorizados, y para aquellos archivos más críticos, un registro de los accesos efectivamente producidos en el que se indique la fecha y hora, el tipo de operación realizada sobre los datos y el usuario que la inició.

- Controles de respaldo:

  - Verificación de los procedimientos de realización de copias de seguridad de datos y programas al objeto de determinar su adecuación y operatividad.

  - Revisión de los procedimientos establecidos en relación con el centro de backup y el plan de contingencia: comprobación de la realización de pruebas periódicas, análisis del resultado de éstas, etc.

22.3.2.2. Auditoría de cumplimiento de otros aspectos de la LORTAD

La LORTAD, y demás Instrucciones emitidas por la Agencia de Protección de Datos, incluye en su articulado varias normas y obligaciones legales, cuyo

cumplimiento debería ser verificado por la auditoría informática, de las cuales extractamos aquí las que consideramos más relevantes:

22.3.2.2.1. Calidad de los datos patrimoniales y financieros incluidos en archivos de morosos

La ya mencionada Instrucción 1/1995 establece:

"1. *La inclusión de los datos de carácter personal en los archivos relativos al cumplimiento o incumplimiento de obligaciones dinerarias, a los que se refiere el artículo 28 de la Ley Orgánica 5/1992, deberá efectuarse solamente cuando concurran los siguientes requisitos:*

a) Existencia previa de una deuda cierta, vencida y exigible, que haya resultado impagada.

b) Requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación.

2. *No podrán incluirse en los archivos de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores.*

3. *El acreedor o quién actúe por su cuenta e interés deberá asegurarse de que concurren todos los requisitos exigidos en el número 1 de esta norma en el momento de notificar los datos adversos al responsable del archivo común".*

Por tanto, la auditoría informática debería revisar los archivos de morosos y fallidos relativos a clientes de la propia entidad, esto es, cuando el banco es el acreedor, así, como los archivos generados con destino a ser incorporados en un archivo común de varias entidades (RAI, ASNEF, CIRBE), al objeto de verificar que la deuda registrada y comunicada es real.

22.3.2.2.2. Compra de archivos para prospección comercial

El artículo 30 de la LORTAD regula:

"*1. Sólo se utilizarán de forma automatizada datos de carácter personal en las encuestas de opinión, trabajos de prospección de mercados, investigación científica o médica y actividades análogas, si el afectado hubiera prestado libremente su consentimiento a tal efecto.*

2. *Los datos de carácter personal tratados automáticamente con ocasión de tales actividades no podrán ser utilizados con finalidad distinta ni cedidos de forma que puedan ser puestos en relación con una persona concreta."*

Ante la posible existencia de archivos con datos personales comprados al objeto de realizar prospecciones comerciales, el auditor debería verificar que:

- La entidad se ha asegurado de la legalidad de los datos que compra.

- El contrato recoge las cláusulas adecuadas que liberen de responsabilidad a la entidad financiera frente a posibles incumplimientos de la normativa legal por parte del vendedor.

22.3.2.2.3. Datos personales recabados para un seguro asociado a un préstamo

La Instrucción 2/1995 protege los datos personales recabados para la formalización de aquellos seguros de vida asociados con la concesión de un préstamo o crédito, de manera que el beneficiario del seguro es la propia entidad acreedora. Entre otras, establece las siguientes normas, cuyo cumplimiento entra dentro del ámbito de revisión de la auditoría informática de la entidad financiera:

"Norma segunda.- De la recogida de los datos

1. *La obtención de datos personales a efectos de la celebración de un contrato de seguro de vida, anejo a la concesión de un crédito hipotecario o personal, efectuada por las entidades de crédito a través de cuestionarios u otros impresos, deberá realizarse, en todo caso, mediante modelos separados para cada uno de los contratos a celebrar. En los formularios cuyo destinatario sean las entidades bancarias no podrán recabarse en ningún caso datos relativos a la salud del solicitante.*

2. *Cualquiera que sea el modo de llevarse a efecto la recogida de datos de salud necesarios para la celebración del seguro de vida deberá constar expresamente el compromiso de la entidad de crédito de que los datos obtenidos a tal fin solamente serán utilizados por la entidad aseguradora. Las entidades de crédito no podrán incluir los datos de salud en sus archivos informatizados o en aquellos en los que almacenen datos de forma convencional.*

Norma tercera.- Consentimiento del afectado y tratamiento de los datos

El afectado deberá manifestar su consentimiento por separado para cada uno de los contratos y para el tratamiento distinto de la información que ambos conllevan.

Las entidades de crédito solamente podrán tratar aquellos datos personales, no especialmente protegidos, que sean estrictamente necesarios para relacionar el contrato de préstamo con el contrato de seguro de vida celebrado como consecuencia de aquél o que estén justificados por la intervención de la entidad de crédito como agente o tomador del contrato de seguro."

Por tanto, el auditor debería verificar:

- La ausencia de referencias a datos sobre la salud del futuro prestatario en los formularios de recogida de datos del préstamo.
- La inexistencia de ningún tipo de archivo por parte de la entidad financiera, ni informática ni manual, en el que expresamente se recojan los datos de salud de los clientes.
- La existencia de la información adecuada en el clausurado del impreso utilizado para la recogida de los datos relativos al seguro, al respecto de:
  - El compromiso del banco de que los datos que proporcione el cliente serán exclusivamente cedidos a la entidad aseguradora.
  - Nombre y dirección del destinatario de la información (entidad aseguradora).
  - El derecho del afectado a la consulta, rectificación y cancelación de los datos existentes acerca de él, en cumplimiento de lo establecido en la LORTAD.

22.4. CUESTIONES DE REPASO

1. ¿En qué faceta resulta más valiosa la participación de la auditoría informática en el sector financiero?
2. ¿Qué características tienen las aplicaciones informáticas que soportan productos bancarios?
3. ¿En qué se diferencian las auditorías de medios de pago de las auditorías de productos de tesorería?
4. ¿Qué conocimientos necesita un auditor informático para poder llevar a cabo una auditoría en el sector bancario?
5. Comente cómo afecta la LORTAD a las aplicaciones bancarias.

6. ¿Qué aplicaciones cree que tiene el problema del EURO en la auditoría informática de entidades financieras?

7. Comente aspectos a tener en cuenta respecto a los "archivos de morosos".

8. ¿Qué restricciones existen respecto a los datos recabados para un seguro asociado a un préstamo?

9. Diseñe una planificación anual de trabajos para auditoría informática de una pequeña entidad bancaria.

10. ¿Qué consideraciones de las expuestas en el capítulo podrían aplicarse a la auditoría de empresas de seguros? ¿Y de asistencia sanitaria?

CAPÍTULO 23

AUDITORÍA INFORMÁTICA EN EL SECTOR AÉREO

Aurelio Hermoso Baños

23.1. INTRODUCCIÓN

Por hacer un poco de historia podríamos decir que en el mundo informático del sector aéreo los aspectos jurídicos no han tenido un gran impacto en el desarrollo dado que apenas existían y este sector estaba monopolizado por las empresas fabricantes de hardware y los productos y aplicaciones software en las que se basaba el tratamiento de los datos y en las facilidades que ofrecía el sistema operativo de sus máquinas.

Los aspectos sobre los que se realizaban trabajos de auditoría eran los clásicos de materia económica y financiera sobre los cuales, aparte del modo operativo, había que cumplir requisitos obligados que estaban reglamentados por los organismos oficiales del país. No obstante, dentro del sector había que cumplir la legislación internacional correspondiente.

Cuando el mundo de la auditoría se dio cuenta de que los datos eran manejados por sistemas informáticos, nació la auditoría informática, la cual iba más dirigida a la organización del centro proceso de datos y a la custodia de los datos en dispositivos magnéticos cumpliendo con la legislación de guardar la información al menos cinco años.

La expansión del mundo informático debido al avance de la tecnología motivó que determinados datos se procesaran en lugares geográficamente distantes e incluso por empresas distintas cuyo único fin era fortalecer el negocio del sector aéreo a nivel mundial en fuerte competencia con el resto de las compañías aéreas.

Con esta idea nacieron diversos sistemas de reservas a nivel internacional entre los que podemos citar los americanos SABRE, SYSTEM ONE y APOLLO, y los europeos GALILEO y AMADEUS, aparte de los nacionales que en España era SAVIA.

23.2. SISTEMA DE RESERVAS AMADEUS

Las líneas aéreas europeas no podían quedarse atrás ante el empuje americano y se constituyó como sociedad anónima AMADEUS GLOBAL TRAVEL DISTRIBUTION, siendo los socios actuales Air France, Iberia, Lufthansa y Continental Airlines.

Su finalidad es proporcionar un sistema de reservas a nivel internacional de diversos productos entre los que se encuentran: vuelos aéreos, hoteles, alquiler de coches, etc.

A este servicio se conectan las Agencias de Viaje y Compañías Aéreas mediante terminales informáticos. Desde estos terminales los adheridos realizan las reservas en nombre de sus clientes.

En España se realiza esta función a nivel nacional por medio de la compañía SAVIA, Sistema para las Agencias de Viajes, utilizando los servicios de los grandes sistemas informáticos de IBERIA.

Al sistema se pueden adherir también los proveedores de los servicios con el fin de que se puedan hacer reservas por medios informáticos para: compañías de líneas aéreas, servicios hoteleros, compañías de alquiler de coches, mayoristas de viajes, floristas, y un largo etcétera. Estos proveedores pueden estar directamente conectados o no, pero su información sí debe estar en la base de datos de AMADEUS.

Por lo tanto AMADEUS contrata servicios de proceso de datos y acceso a la base de datos de reservas para cualquier línea aérea que esté adherida a un sistema informático de reservas, programas de vuelos, disponibilidad de plazas y tarifas, al mismo tiempo que gestiona la red de comunicaciones, produce programas informáticos para la gestión de las Agencias de Viajes y también para la gestión de todo el sistema de reservas a nivel internacional.

IBERIA realiza la conexión de las Agencias de Viajes españolas al sistema AMADEUS para que puedan reservar cualquiera de los productos ofrecidos del proveedor de cualquier país, al mismo tiempo que posee su propio sistema de reservas y red de comunicaciones para sus Oficinas de Ventas y de las Agencias de Viajes.

Las Agencias de otros países pueden reservar productos de IBERIA en sistema AMADEUS y de cualquier otro proveedor nacional que tenga sus productos en la base de datos, aunque estén conectados a otro sistema de reservas dado que existen acuerdos comerciales entre ellos para facilitar información y venta de sus productos.

23.3. FACTURACIÓN ENTRE COMPAÑÍAS AÉREAS

Este trasiego de información es gratuito, pero cuando se realiza una reserva y la correspondiente emisión del billete para otra compañía aérea es necesario regularlo para que el importe recaiga sobre el auténtico transportista.

Si un pasajero solicita información y desea contratar un vuelo con una compañía aérea, por ejemplo Madrid-Londres, y ese trayecto lo realiza la misma, no existe facturación entre compañías.

Pero si el vuelo que desea realizar es: Madrid-Nueva York-Hawai-San Francisco-Nueva York-Madrid, y la compañía aérea no puede efectuar alguno de estos tramos por no disponer de autorización para realizar esos vuelos, existe un acuerdo entre las compañías aéreas de poder emitir el billete en las líneas de aquellas compañías que los explotan comercialmente.

Si a esto añadimos que en la ciudad o país donde está el cliente realizando la compra de sus vuelos, no existe representación de la citada compañía, se puede emitir el billete reservando los vuelos entre tramos, en aquella compañía que sí los puede realizar o resulte mejor por horarios o precios.

Supuesto: Volviendo al ejemplo se nos podía dar la siguiente casuística:

La oficina de ventas de IBERIA o Agencia de Viajes donde compra el billete con el logo de esta compañía, está situada en España y se utiliza la conexión vía SAVIA.

Madrid-Nueva York se reserva y lo realiza IBERIA.
Nueva York-Hawai se reserva y lo realiza American Airlines.
Hawai-San Francisco se reserva y lo realiza Carnival Airlines.
San Francisco-Nueva York se reserva y lo realiza Continental Airlines.
Nueva York-Madrid se reserva y lo realiza IBERIA.

La suma total de los importes de cada uno de los tramos los abona íntegramente a quien emitió el billete, en este caso con el logo de IBERIA y a través de la red de SAVIA, con la reserva en cada una de las compañías aéreas que efectuarán el correspondiente trayecto contratado.

Lógicamente cada una de éstas deberá recibir el importe del trayecto en el cual ha sido transportado el pasajero que pagó el importe por su reserva y emisión del billete.

Aquí aparece el concepto del BSP, *Bank Settelment Plan*, Plan de liquidación Bancaria, cuyas oficinas están en Ginebra donde se centralizan todas las operaciones funcionando como una Cámara de compensación. Para ello existe una fecha determinada, como límite cada mes, para hacer llegar los importes totales y desglosados para cada compañía aérea de cada uno de los billetes emitidos y realizados. La distribución de los Procesos BSP está basada en regulaciones de IATA, Asociación Internacional del Transporte Aéreo.

Para evitar el fraude, IATA facilita un control numérico del *stock* de billetes que se adjudica a cada compañía aérea y Agencia de Viajes y que sólo son válidos para aquellos miembros asociados a la citada organización, siendo esta numeración incorporada a los datos del pasajero para saber el billete que se le entrega con los trayectos que solicitó y la o las tarifas que abonó.

Cada Agencia de Viajes incorpora su propio número de Agencia IATA en la emisión del billete.

Esta información con la que incorpora los datos de la reserva efectuada figura en la base de datos.

23.4. CÓDIGO DE CONDUCTA PARA CRS

La Comunidad Económica Europea por mediación de El Consejo de las Comunidades Europeas aprobó, y publicó el Reglamento núm. 2299/89 de 24 de julio de 1989, por, el que se establece un código de conducta para los sistemas informatizados de reserva, posteriormente aprobó y publicó el Reglamento núm. 3089/93 de 29 de octubre de 1993, que modifica el Reglamento núm. 2299/89, por el que se establece un código de conducta para los sistemas informatizados de reserva.

Esta última modificación introduce conceptos en el reglamento sobre la protección de datos de carácter personal y la prohibición legal del uso de la información del billete por los sistemas de distribución, en este caso AMADEUS, aplicable a los propietarios de los sistemas nacionales, IBERIA.

El citado reglamento comunitario establece en sus artículos 4, 6 y 21, entre otras, las siguientes obligaciones:

4) Los Sistemas de Distribución (CRS's) deben asegurar que las facilidades de distribución están separadas de manera clara y verificable de las facilidades privadas de inventario, gestión y marketing de la compañía o compañías aéreas propietarias del mismo. Esta separación debe ser física o lógica por medio del software adecuado y las facilidades serán solamente conectables entre sí por medio de una interfaz entre ambas aplicaciones.

6) Es necesario proteger los datos y su difusión tanto los privados del pasajero como datos comerciales sobre las compañías aéreas participantes. Con respecto a dicha difusión se establece en concreto que:

Los datos de reservas, ventas o de marketing pueden ser puestos a disposición de todos los participantes con la condición de que:

- No se incluyan datos personales de los pasajeros o entidades.
- No exista discriminación entre el dueño del sistema con respecto a los participantes en lo que se refiere a la prontitud, el método de transmisión, la calidad de la misma, el precio, las condiciones, etc.

El CRS debe garantizar que las mencionadas facilidades se cumplen por medios técnicos que tengan las salvaguardas apropiadas en cuanto al software utilizado.

El CRS debe garantizar que el dueño del sistema no puede acceder a la información suministrada o creada para los demás participantes.

21) El cumplimiento de los requerimientos técnicos mencionados debe ser auditado por empresas independientes, por lo menos una vez al año.

Dado que IBERIA tiene subcontratado por AMADEUS el sistema de reserva y emisión de billetes, es por tanto susceptible de pasar la auditoría correspondiente con el fin de verificar la neutralidad de AMADEUS en su área de responsabilidad.

Al poseer los datos de los billetes de todas las compañías que se emiten por el sistema informático de IBERIA, aunque no se participe en el itinerario del mismo, hay que presentar toda la información necesaria que demuestre que no se hace uso comercial de dichos datos ni se deriven prácticas que alteren la libre competencia.

Al mismo tiempo presentar los procedimientos actuales y la descripción detallada de los mismos así como la aplicación de todas las salvaguardas necesarias para que en el sistema informático de IBERIA sólo se pueda acceder a los datos de otras compañías, para proporcionar la información necesaria al BSP.

Código de Conducta para los Sistemas Informatizados de Reservas menciona que los sistemas de reservas de vuelo informatizados están obligados a pasar una auditoría anual que puede afectar a cualquier entidad que forme parte de dicho sistema.

En cuanto a los datos de carácter personal, la base de datos de reservas del sistema AMADEUS en Alemania se encuentra registrada según la Ley de protección de datos federal alemana, e igualmente la correspondiente a IBERIA en la Agencia de Protección de Datos de España.

En cuanto a los procedimientos de acceso, rectificación y cancelación a los datos personales recogidos en el sistema de reservas, tal y como aparecen en la Ley Orgánica 5/92 de 29 de octubre, no están definidos en AMADEUS por carecer dicha entidad de la posesión y control sobre dichos datos. No obstante, cualquier ciudadano puede acceder a sus datos de reserva a través de la Agencia de Viajes en la cual se efectuó dicha reserva o a través de las compañías aéreas que aparecen en la misma, por medios informatizados.

Esto es motivado por el sistema transaccional de la aplicación en tiempo real que adjudica la propiedad de los datos a la Agencia de Viajes que realizó la entrada de datos quien tiene el contacto personal/comercial con el pasajero. Es una medida adicional de seguridad aplicable por todas las compañías aéreas para asegurar el negocio de las Agencias de Viajes y de la seguridad de la reserva del propio pasajero, evitando la posibilidad de cualquier divulgación y/o modificación en los datos.

La obtención de cintas magnéticas cuya información es de utilidad para procesos de estadística, está sujeta al artículo 6 del Código de Conducta de CRS. Ver bibliografía, Reglamentos de la Comunidad Económica Europea, números 2299/89 y 3089/93.

Asimismo ninguna de las empresas del sistema AMADEUS comercializa los datos personales del sistema de reservas.

23.5. PROCESOS INFORMÁTICOS

Las aplicaciones informáticas a las que se les practica la auditoría son dos, procesándose en plataformas informáticas diferentes.

Proceso TICKETING. Desarrollado para grandes sistemas UNISYS. Bajo este nombre, y para no complicar con nomenclaturas, vamos a reunir las numerosas aplicaciones que componen la información de vuelos, reserva de plazas y emisión de billetes además de los procesos de identificación de usuarios y terminales y la gestión de la red de comunicaciones.

Este proceso comienza por la solicitud de la Agencia de Viajes o Compañía aérea de la solicitud de los vuelos para un trayecto determinado, horarios de los mismos, disponibilidad de plazas, diversas tarifas, reserva de vuelo y asiento con su definitiva confirmación en la emisión del billete para el cliente.

IBERIA facilita la oportuna información y/o conecta a la Agencia de Viajes con el sistema AMADEUS, que posee además un computador exclusivamente para cálculo de tarifas, devolviendo la información completa, facilitando la oportuna emisión del billete y el importe a abonar.

La seguridad de la aplicación está basada en el SIGN-IN facilitado a la Agencia de Viajes en el momento de la contratación comercial del servicio. Esta contraseña permite identificar tanto a la oficina de ventas y a sus terminales como a las funcionalidades asignadas para la realización de las determinadas transacciones que está autorizado a utilizar, igualmente se guarda la identificación para que sólo esa Agencia y no cualquier otra con *sign-in* diferente, pueda modificar, eliminar o añadir datos al registro creado en la base de datos para la reserva y emisión del billete del pasajero.

La información del billete confirmado y cerrado será utilizada para realizar el *check-in* en el aeropuerto en el momento en que el pasajero embarque al avión.

Toda la información correspondiente al billete es mantenida en la base de datos hasta que el pasajero haya realizado el último tramo que figura en el mismo, momento en que será copiada a cintas magnéticas para usos estadísticos y conservación de tipo legal y borrada del sistema.

Los datos contables son traspasados al sistema IBM vía hyperchannel.

Proceso BSP. Desarrollado para grandes sistemas IBM. Los datos económicos del billete de vuelo son tratados en procesos de facturación y administración contable y de preparación para ser remitidos al Centro de compensación para la facturación entre compañías aéreas.

Existe una empresa nacional de BSP que reúne los datos correspondientes de IBERIA mediante proceso de captación de la información por medio de transmisión de archivos y también de las otras compañías aéreas nacionales y agencias de viaje para ser transferidos al centro de compensación en Ginebra.

La transmisión de estos archivos se formalizó mediante contrato exigiendo todas las medidas de seguridad necesarias y de acuerdo con la legislación nacional vigente y la no divulgación de los datos comerciales de las compañías participantes.

Las medidas de protección vienen dadas por clave *User-Id* asignada a personas significadas únicamente con autorización de lectura para los archivos determinados, con lo cual la confidencialidad, divulgación y no manipulación de la información queda asegurada.

Los datos se respaldan en cintas magnéticas mediante procesos backup siendo custodiadas en un centro off-site durante el período legal exigido.

23.6. AUDITORÍA INFORMÁTICA

Anualmente se recibe la visita de auditores que en cumplimiento del Reglamento Comunitario sobre Código de Conducta de CRS, vienen de Alemania, sede del sistema AMADEUS para realizar sus trabajos respecto a los procesos señalados en el punto anterior. El cumplimiento de esta auditoría es obligado, y en caso del no cumplimiento de lo estipulado en los artículos del reglamento se podría cancelar el contrato de servicio entre ambas empresas.

La finalidad de la auditoría es detectar posibles desviaciones para asegurar la correcta o incorrecta función neutral en la emisión del billete por parte de IBERIA como subcontratado de AMADEUS, así como asegurar las apropiadas salvaguardas, como los procedimientos internos y las medidas de seguridad conforme al Reglamento de la CEE núm. 2299/89, de 24 de julio 1989 y Reglamento CEE núm. 3089/93, de 29 de octubre 1993, por el que se establece un Código de Conducta para los sistemas informatizados de reservas y los requerimientos de AMADEUS incluidos en el contrato con la subcontratación de servicios de Ticketing con IBERIA en cuanto a información al cliente, calidad de los servicios y confidencialidad se refiere.

Breve descripción de los servicios de sistemas de información que facilita IBERIA.

- En general como operador aéreo, el transporte de pasajeros y carga, servicios en aeropuertos y operaciones de vuelo.

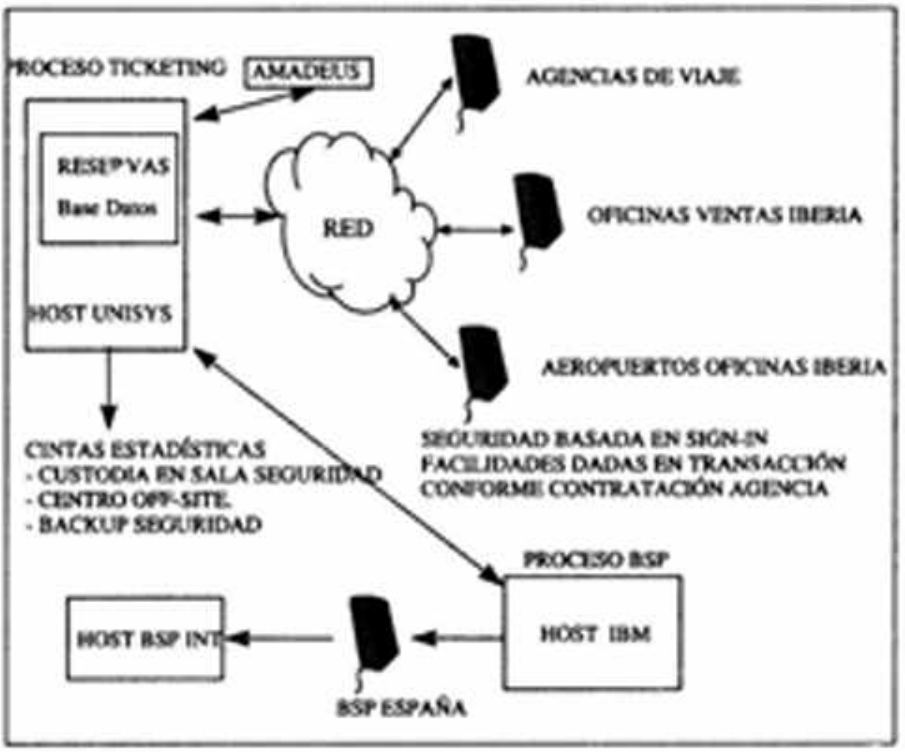
- En particular, desde el centro de proceso de datos de Madrid, ofrece sistemas de inventario (información de vuelos, plazas disponibles, tarifas), emisión de billetes, seguimiento de equipajes y operaciones de carga.

- Existen compañías aéreas conectadas al sistema informatizado de reservas de IBERIA con inventario privado y emisión de billetes.

- La información del billete consiste en datos del pasajero e información del vuelo, tarifa del mismo y forma de pago, que pueden ser impresos en la Agencia de Viajes conteniendo otros datos de seguridad como el número de

control del billete, control de stock del billete de información para el BSP. Todo ello para la emisión del billete de vuelo.

Estructura Sistema Informatizado Reservas de IBERIA



El primer paso después de preparar la agenda de entrevistas con los auditores, es recibir en IBERIA un cuestionario sobre determinadas preguntas que debidamente cumplimentado y comentado se les hace entrega el día de la visita.

Estas preguntas se concretan en cuatro apartados:

A) Datos personales

- Nuevas inscripciones de archivos en la Agencia de Protección de Datos, desde la última auditoría realizada.
- Realización de auditorías internas o externas concernientes a la seguridad y/o privacidad de los datos.
- Si fue interna, cuáles fueron los resultados.
- Aparición de nuevas regulaciones internas sobre confidencialidad o manejo de los datos de carácter personal o de la compañía.

- Aparición de violaciones concernientes a la privacidad de los datos de carácter personal.
- Reclamaciones de compañías aéreas respecto al manejo de sus datos.
- Reclamaciones desde otras compañías aéreas a los servicios de IBERIA.
- Reclamaciones desde otras compañías aéreas a los servicios de billetaje.

B) Datos BSP

- Si se ha incorporado alguna nueva compañía aérea que tenga su inventario en la base de datos de IBERIA desde la última auditoría realizada.
- Si esto obligó a modificaciones en las aplicaciones.
- Si hubo necesidad de adaptaciones en los sistemas informáticos, en el software, en los procedimientos o en la organización.
- Si se han incorporado nuevas reglas de BSP.
- Si han aparecido nuevos mercados en el BSP.
- Si han aparecido nuevas versiones de BSP.

C) Otras modificaciones y cambios

- Cambios en la política de seguridad de IBERIA desde la última auditoría realizada.
- Cambios en la política de respaldo y salvaguarda de la información.
- Cambios en los sistemas de seguridad y configuraciones en los sistemas informáticos de cada una de las plataformas.
- Cambios hardware y/o de sistemas operativos en cada una de las plataformas.
- Cambios en la organización separando responsabilidades desde la última auditoría realizada.
  - Entre Desarrollo y Explotación.
  - El grupo de desarrollo de la aplicación Ticketing mantiene las mismas responsabilidades.

D) Documentación

- Listados de los perfiles de seguridad de los archivos correspondientes a los procesos BSP y de los usuarios que están autorizados a su acceso y tratamiento.

Por su parte los auditores instalan procedimientos y medidas administrativas con el fin de asegurarse la seguridad en los datos del billete, cubriendo la separación de otros servicios y principalmente de cualquier función de inventario, entendiendo que AMADEUS facilita los mismos conceptos a todas las compañías aéreas conforme se detalla a continuación:

Establecimiento de Flujo de trabajo

Entrevistas con todos los responsables de las áreas de la aplicación Ticketing en orden a confirmar, completar o corregir las medidas, procedimientos y controles establecidos poniendo un mayor énfasis en los aspectos de seguridad.

Procedimientos de auditoría

Están basados en la separación organizacional y en la documentación solicitada con anterioridad.

Otro enfoque ha estado basado principalmente en la implantación de medidas y procedimientos de seguridad y sus controles distribuyéndolos en temas como:

- Seguridad Física.
- Sistemas de seguridad e integridad.
- Medidas de seguridad en las Aplicaciones y sus datos.
- Seguridad en el desarrollo de la Aplicación.

Seguridad Física

Se analizan los siguientes puntos:

- Control de accesos al edificio del Centro Proceso de Datos.

- Acceso a las diferentes áreas sólo por personal autorizado, y de visitantes.

- Acceso a la sala de computadores u otras dependencias críticas.

- Registros en libros de entrada/salida e inspección de bultos.

- Control de entrada y salida de vehículos de la zona y su registro.

- Control área suministro de energía, aire acondicionado y otros servicios por medio de CCTV.

- Centro off-site, para almacenamiento y custodia de cintas magnéticas y su control e identificación. Listas de personal autorizado y su autorización.

Sistema de Seguridad e Integridad

Se analizan los siguientes puntos:

- Acceso a los Sistemas Informáticos UNISYS.

  - Control de acceso a la aplicación Ticketing, mediante identificación del usuario y autorización de conexión al sistema informático correspondiente que tiene la aplicación.

  - Control de acceso del terminal identificado en el software del front-end de comunicaciones y en tablas del sistema operativo.

  - El terminal y la conexión física están previamente definidos en tablas con acceso protegido.

  - Se define a cuál aplicación de Ticketing se autoriza al terminal a conectarse definido en tablas con acceso protegido.

  - Estos tipos de acceso sólo están permitidos vía transacciones en tiempo real con funcionalidades predeterminadas en la aplicación.

  - Una aplicación no puede tener acceso, lectura o modificación en otra aplicación si no está previamente autorizada o requerida por su funcionalidad.

  - El usuario accede a la aplicación mediante Sign-in, el cual es único para esa Agencia de Viajes u Oficina de Ventas de IBERIA.

  - El acceso vía sistema conversacional requiere un Logon de entrada más User-Id y Password.

  - Existe auditoría de intentos de violación y control de accesos.

  - El acceso a los datos sólo es posible vía autorización de la aplicación.

  - Existen terminales autorizados para entrar en sistema de emergencia, asignados al personal técnico para la resolución de problemas.

- Acceso a los sistemas informáticos IBM.

  - Los terminales autorizados de acceso al sistema informático que contiene la aplicación están definidos en el software de la Unidad de Control de Comunicaciones y en las tablas del sistema operativo MVS, debidamente protegidos.

  - El acceso al sistema está controlado por User-id y Password.

  - Existen reglas de acceso a las aplicaciones por protección y tipo de acceso a los archivos, asignación de facilidades al usuario.

  - Existe auditoría de violación y control de accesos.

  - La seguridad consiste en identificación de usuario y su verificación, control de accesos y auditoría guardando sus resultados.

  - Se asegura que una aplicación no puede acceder a datos de otra aplicación.

  - Existen terminales autorizados para entrar en sistema de emergencia asignados al personal técnico para la resolución de problemas.

  - Todos los datos de contabilidad preparados en la plataforma UNISYS por la aplicación Ticketing son transferidos a la plataforma IBM por medio de transferencia de archivos y quedan almacenados debidamente protegidos por el producto de seguridad instalado en dicha plataforma. Antes de la transferencia son manejados por procesos batch.

Medidas de seguridad de las Aplicaciones y sus datos

Se analizan los siguientes puntos:

- Las definiciones de seguridad de la aplicación son coordinadas por los responsables de AMADEUS, IBERIA y SAVIA.

- SAVIA define la seguridad de acceso de la Agencia de Viajes a la Aplicación Ticketing y lo comunica a IBERIA para su inclusión en los sistemas informáticos. Incluye definición del terminal, Sign-in en la Aplicación con sus funcionalidades y autorizaciones, y la identificación del terminal de la Agencia de Viajes.

- Controles de acceso a la aplicación Ticketing:

  - El acceso a la aplicación es controlado por la identificación del terminal en común con el sign-in. Estas especificaciones están contenidas en tablas de la aplicación.

- Controles de acceso a la aplicación de otras Compañías aéreas:

  - El control de acceso del terminal a sus aplicaciones está en base a las autorizaciones asignadas al terminal. Por ejemplo, puede impedir el acceso a otros programas dentro de la aplicación.

  - Acceso restringido a transacciones que faciliten las tarifas y el número de control de stock del billete.

  - Restringir el acceso a aplicaciones inventario, (información de vuelos, disponibilidad de asientos y tarifas), desde terminales.

- Control de conectividad a otros servicios basados en sistemas remotos:

  - La aplicación también controla la conectividad a otros sistemas, incluyendo los protocolos de comunicación.
  - Acceso a aplicaciones basadas en sistemas remotos, están definidas en tablas que especifican el correspondiente programa, aplicaciones permitidas y las interfaces.
  - Accesos del terminal a las aplicaciones remotas son controladas por programas de la aplicación Ticketing y llevan el identificador del terminal.

- Control de acceso a sus bases de datos:

  - Los accesos a la información de las bases de datos están garantizados por los programas y transacciones controladas por la aplicación Ticketing, definidas las relaciones entre datos y programas en tablas.

- Control de accesos a utilidades:

  - Los accesos a utilidades están definidos, controlados y mantenidos por la identificación del terminal en tablas, siendo el grupo de desarrollo de la aplicación el único autorizado para ello.

- Control de obtención de respaldo de las bases de datos y programas de la aplicación:

  - Se asegura mediante la realización de procedimientos con períodos determinados de acuerdo con normas de seguridad publicadas.

- Las cintas magnéticas obtenidas son custodiadas en centro off-site.

– Control de Soporte (Help Desk) en SAVIA:

- El punto de entrada para las Agencias de Viaje conectadas a SAVIA funciona en dos niveles de soporte.

- El primer nivel de soporte lo facilita SAVIA desde un punto de vista funcional y técnico. Incluye la comprobación del entorno de la Agencia, como puede ser el hardware, configuración, software y conectividad.

- El segundo nivel, si con el primero no se resuelve el problema, es facilitado por SAVIA, y es el personal técnico de IBERIA como soporte de la aplicación Ticketing el encargado de la resolución. Este grupo es responsable del mantenimiento relativo al desarrollo de la aplicación, incluyendo toda la configuración y tablas de seguridad.

- Solamente los terminales instalados en Help Desk están permitidos para usar estas facilidades, esto se asegura utilizando las tablas de identificación de los terminales vía la definición de tablas de configuración en el software de comunicaciones.

Seguridad en el desarrollo de la Aplicación

- El desarrollo de la aplicación Ticketing y sus funciones pertenece a AMADEUS, porque es un producto basado principalmente en el paquete estándar de la casa UNISYS para su aplicación en líneas aéreas.

- El grupo de desarrollo de IBERIA tiene la responsabilidad de integrarlo y probarlo en la plataforma UNISYS.

- Existe separación de entornos de Desarrollo y Explotación con procedimientos y normas muy concretas y seguras para el pase a explotación de programas y sus modificaciones.

- Los cambios para la aplicación de contabilidad y facturación en la plataforma IBM son iniciados por IBERIA o por la Cámara de compensación BSP.

- El desarrollo de los programas necesarios son probados en entorno separado en cooperación con las autoridades del BSP.

23.7. CONCLUSIONES

Problemas

- Es necesario un seguimiento de la legislación nacional e internacional en materia de la facturación entre compañías aéreas BSP para la adaptación de las aplicaciones a su contenido.

- Dejar bien claro en los aspectos contractuales con las Agencias de Viajes y Compañías aéreas que se incorporen a la base de datos de IBERIA las obligaciones y responsabilidades de cada parte según la legislación nacional e internacional.

- Las nuevas tecnologías pueden hacer variar las aplicaciones actuales, como por ejemplo la venta del billete electrónico y sobre todo las ventas por INTERNET, lo que obligaría a tomar medidas de seguridad adicionales.

Soluciones

- Las aplicaciones deben controlar fuertemente la identificación de los clientes, lo que hará variar y ampliar el desarrollo por el mundo INTERNET con nuevas soluciones en materia de seguridad, lo que a su vez obligará a desarrollar nuevas metodologías en el mundo de la auditoría informática.

23.8. LECTURAS RECOMENDADAS

a) Reglamento de la Comunidad Económica Europea núm. 2299/89, de 24 de julio de 1989, por el que se establece un código de conducta para los sistemas informatizados de reserva. Diario Oficial de las Comunidades Europeas, L-220, 29 de julio de 1989.

b) Reglamento de la Comunidad Económica Europea núm. 3089/93, de 29 de octubre de 1993, que modifica el Reglamento de la Comunidad Económica Europea núm. 2299/89 por el que se establece un código de conducta para los sistemas informatizados de reservas. Diario Oficial de las Comunidades Europeas, L-278, 11 de noviembre de 1993.

c) Informe de la Comisión de las Comunidades Europeas al Consejo sobre la aplicación del artículo 4 bis y el apartado 3 del artículo 6 del Reglamento de la Comunidad Económica Europea núm. 2299/89 del Consejo en su versión

modificada por el Reglamento por el que se establece un código de conducta para los sistemas informatizados de reserva. Bruselas 07.03.1995.

23.9. CUESTIONES DE REPASO

1. Nombre algunos sistemas de reservas que conozca.
2. ¿Qué es AMADEUS?
3. ¿Qué tipo de tratamiento de la información se necesita para un viaje con diversas escalas en las que el pasajero cambia de compañía aérea?
4. ¿Cómo afecta la LORTAD al sector aéreo?
5. ¿A qué aplicaciones principales se les hace auditoría en el sector aéreo?
6. Describa los servicios de sistemas de información que facilita una compañía como IBERIA.
7. ¿Qué aspectos se analizan en cuanto a la seguridad e integridad?
8. ¿Cuáles son las medidas de seguridad de las aplicaciones y sus datos?
9. ¿Cuáles son los problemas de adaptación de legislación internacional en materia de facturación?
10. ¿Qué nuevos riesgos entraña la venta del billete electrónico a través de Internet?

CAPÍTULO 24

AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN

Víctor Izquierdo Loyola

24.1. INTRODUCCIÓN

Constituye un juicio de valor generalmente aceptado decir que las Tecnologías de la Información y de las Comunicaciones (TIC) se han venido utilizando en la Administración española, desde los inicios del proceso de "mecanización" en los años sesenta hasta entrada la década de los noventa, para mejorar su funcionamiento interno, dejando de lado (salvo en excepciones que confirman la regla) su aplicación a las relaciones de la Administración con ciudadanos y empresas.

Este juicio de valor es compartido por el legislador en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJ-PAC), cuando en la Exposición de motivos dice:

"Las nuevas corrientes de la ciencia de la organización aportan un enfoque adicional en cuanto mecanismo para garantizar la calidad y transparencia de la actuación administrativa, que configuran diferencias sustanciales entre los escenarios de 1958 y 1992. La Ley de Procedimiento Administrativo de 1958 pretendió modernizar las arcanas maneras de la Administración española, propugnando una racionalización de los trabajos burocráticos y el empleo de máquinas adecuadas con vista a implantar una progresiva mecanización y automatismo en las oficinas públicas, siempre que el volumen de trabajo haga económico el empleo de estos "procedimientos". Este planteamiento tan limitado ha dificultado el que la informatización, soporte y tejido nervioso de las relaciones sociales y económicas de nuestra época, haya tenido hasta ahora incidencia sustantivo en el procedimiento

administrativo por falta de reconocimiento formal de la validez de documentos y comunicaciones emitidos por dicha vía. El extraordinario avance experimentado en nuestras Administraciones Públicas en la tecnificación de sus medios operativos, a través de su cada vez mayor parque informática y telemático, se ha limitado al funcionamiento interno, sin correspondencia relevante con la producción jurídica de su actividad relacionada con los ciudadanos. Las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas."

El presente capítulo sobre la auditoría informática en la Administración se centra en analizar las consecuencias que se derivan para esta disciplina de la entrada en vigor de la LRJ-PAC y de las disposiciones que la desarrollan. En particular, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas (EIT) por la Administración General del Estado.

Examinemos en primer lugar el tratamiento que reciben las TIC en la LRJ-PAC.

24.2. LAS TIC EN LA LRJ-PAC

Los dos preceptos esenciales para comprender el papel asignado a las TIC en el procedimiento administrativo por la Ley 30/1992 son el artículo 45 (Incorporación de medios técnicos) y el 38 (Registros). Existen otros en los que se contienen mandatos que afectan a la utilización de las técnicas EIT por parte de las Administraciones Públicas. Se trata, principalmente, de' los que se refieren al acceso a los registros y archivos, a las comunicaciones y notificaciones, al derecho a no presentar documentos que ya se encuentran en poder de la Administración actuante, a la validez y eficacia de documentos y copias o a la Informatización de registros.

Comencemos por el Artículo 45 que la Ley dedica a la "Incorporación de medios técnicos". En su primer apartado se recoge el siguiente mandato:

"Las Administraciones impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes."

De su lectura podemos extraer las siguientes conclusiones:

- Se trata de un mandato que afecta a todas las Administraciones a las que se aplica la Ley: la General del Estado, las de las Comunidades Autónomas y las Entidades que integran la Administración Local.

- No se refiere, como señala L. Ortega Álvarez, sólo a la utilización de las técnicas y medios EIT para el funcionamiento interno (desarrollo de su actividad), sino también a las relaciones con los ciudadanos (ejercicio de sus competencias).

- Se recuerda que el uso de los medios EIT se encuentra limitado por lo establecido en la Constitución (artículo 18.4) y las Leyes (principalmente la LORTAD).

El segundo apartado del artículo presenta posiblemente un mayor calado, ya que faculta a los ciudadanos a relacionarse con las Administraciones Públicas para ejercer sus derechos a través de técnicas y medios EIT, siempre que se satisfagan las siguientes condiciones:

- Cuando ello sea compatible con los medios técnicos de que dispongan las Administraciones Públicas. Nos encontramos aquí, por tanto, ante un problema de normalización.

- Cuando la relación ciudadano-Administración respete las garantías y requisitos previstos en cada procedimiento. En otras palabras más próximas al mundo de los sistemas de información, se trata de que la relación ciudadano-Administración respete las previsiones del Análisis de Requisitos del Sistema.

Los apartados 3 y 4 del artículo 45 recogen determinados requisitos a los que la Ley somete la utilización de técnicas y medios EIT:

- Así, el apartado 3, referido exclusivamente a los procedimientos que se tramiten y terminen en soporte informático, exige que quede garantizada la identificación y el ejercicio de la competencia por el órgano que lo ejerce. Nos encontramos en este caso ante un problema de autenticación.

- El apartado 4, que se aplica sólo a los programas y aplicaciones EIT que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, exige que estas aplicaciones sean previamente aprobadas por el órgano competente, el cual debe difundir públicamente sus características.

Finalmente, el apartado 5 se dedica a los *documentos electrónicos*, estableciendo los requisitos para que dispongan de validez y eficacia, tanto los originales como las copias. Éstos son los siguientes:

- Que quede garantizada su autenticidad, integridad y conservación.
- En su caso, la recepción por el interesado.
- El cumplimiento de las garantías y requisitos exigidos por la propia LRJ-PAC u otras Leyes.

Más adelante, en este mismo capítulo, nos referiremos a cómo la Administración General del Estado (una de las Administraciones afectadas por la Ley) ha regulado las previsiones del artículo 45 mediante el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

24.3. LA INFORMATIZACIÓN DE REGISTROS

Los registros tradicionalmente han constituido la "puerta de entrada" de los ciudadanos a la Administración. En el sistema registral definido en la LRJ-PAC se establece que los órganos administrativos deben llevar "un registro general en el que se hará el correspondiente asiento de todo escrito o comunicación que sea presentado o que se reciba en cualquier Unidad administrativa propia. También se anotarán en el mismo la salida de los escritos y comunicaciones oficiales dirigidas a otros órganos o particulares". Hasta aquí todo resulta bastante convencional. La novedad fundamental introducida por la LRJ-PAC consiste en la obligación, recogida en el artículo 38.3, de instalar en soporte informático todos los registros de las Administraciones Públicas, si bien en la forma y plazos que determine el Gobierno, órganos de Gobierno de las Comunidades Autónomas y Entidades que integran la Administración Local, en función del grado de desarrollo de los medios técnicos de que dispongan (Disposición adicional segunda).

Esta instalación en soporte informático es una condición necesaria para que los registros puedan llevar a cabo lo que podemos denominar funciones registrales modernas, que vienen a añadirse a las básicas del sistema administrativo registral español, constituidas por:

- Sellado de la documentación de entrada como medida de "constancia de la entrega". Se entrega al ciudadano una copia sellada de su escrito.
- Anotación del apunte en el Libro de registro.
- Si la entrada en el registro está asociada al pago de una cantidad en concepto de impuesto, precio o tasa, se vincula la anotación a la materialización del abono.

Entre las funciones más avanzadas que pueden encomendarse a los registros informatizados figuran las siguientes:

- Garantía de la identidad entre el original entregado y la copia "sellada".
- Archivo de seguridad, ante posibles pérdidas de la solicitud, escrito o comunicación dirigida por el ciudadano a la Administración.

- Publicidad registrar, que ofrece el acceso a los documentos, así como la posibilidad de señalar a un registro como depositario de una información previamente entregada a la Administración, para facilitar el ejercicio y la extensión del derecho reconocido en la Ley (Art. 35 f de la LRJ-PAC) a no presentar los documentos que ya se encuentren en poder de la Administración actuante.

- Integración de registros: generales y auxiliares, de distintos órganos o aun de distintas administraciones.

- Admisibilidad de comunicaciones a distancia, usando medios como el correo electrónico, EDI o el telefax.

24.4. LAS PREVISIONES DEL REAL DECRETO 263/1996, DE 16 DE FEBRERO, POR EL QUE SE REGULA LA UTILIZACIÓN DE LAS TÉCNICAS *EIT* POR LA ADMINISTRACIÓN GENERAL DEL ESTADO

El objetivo de esta norma es delimitar en el ámbito de la Administración General del Estado las garantías, requisitos y supuestos de utilización de las técnicas EIT. Para ello el Real Decreto aborda el desarrollo del artículo 45 de la LRJ-PAC, al que ya nos hemos referido anteriormente, y que en el preámbulo recibe la consideración de "verdadera piedra angular del proceso de información y validación de dichas técnicas [EIT] en la producción jurídica de la Administración Pública así como en sus relaciones con los ciudadanos".

El Real Decreto 263/1996 se estructura del siguiente modo:

- En primer lugar delimita su objeto y ámbito de referencia (Art. 1), y ofrece unas definiciones de conceptos clave en relación con la utilización de las técnicas EIT: soporte, medio, aplicación y documento (Art. 3).

- A continuación establece derechos y garantías generales en la utilización de soportes, medios y aplicaciones EIT.

Más adelante trata una, serie de supuestos concretos en los que se exige un grado de protección más elevado (Arts. 5 a 8) y que se refieren a:

- Programas y aplicaciones para el ejercicio de potestades.
- Comunicaciones.
- Emisión, copia y almacenamiento de documentos automatizados.

Finalmente, el Real Decreto recoge en su Capítulo III diversos preceptos de Acción administrativa, para concluir con una serie de disposiciones adicionales, transitoria, derogatoria y final.

Desde la perspectiva de la auditoría informática, uno de los aspectos esenciales es el de la identificación de los requisitos de seguridad, normalización y conservación recogidos en el texto del Real Decreto. En este entorno, la auditoría debe tener como uno de sus puntos principales de atención el cumplimiento de estos requisitos.

24.5. IDENTIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD, NORMALIZACIÓN Y CONSERVACIÓN EN EL TEXTO DEL REAL DECRETO 263/1996

Seguidamente se examinan de manera sistemática estos requisitos, presentando en paralelo el texto de un determinado artículo con los requisitos en él contenidos, todo ello de acuerdo con el análisis efectuado por el Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos personales (SSITAD) del Consejo Superior de Informática.

24.5.1. Garantías de seguridad de soportes, medios y aplicaciones

Art. 4

3. Las medidas de seguridad aplicadas a los soportes, medios y aplicaciones utilizados por los órganos de la Administración General del Estado y sus entidades de derecho público vinculadas o dependientes deberán garantizar.

a) La restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas.

b) La prevención de alteraciones o pérdidas de los datos e informaciones.

c) La protección de los procesos informáticos frente a manipulaciones no autorizadas.

4. Las especificaciones técnicas de los soportes, medios y aplicaciones utilizados en el ámbito de la Administración General del Estado en sus relaciones externas, y cuando afecten a derechos e intereses de los ciudadanos deberán ser conformes, en su caso, a las normas nacionales e internacionales que sean exigibles.

Requisitos:

Identificación	De personas autorizadas
Control de Accesos	Restricción de acceso a personas autorizadas
Calidad	Prevención de alteraciones o pérdida de los datos
Integridad	Protección de los procesos informáticos frente a manipulaciones no autorizadas
Compatibilidad	Conformidad con normas nacionales e internacionales

24.5.2. Emisión de documentos: procedimientos para garantizar la validez de los medios; integridad, conservación, identidad del autor y autenticidad de la voluntad

Art. 6.1

Los documentos emitidos por los órganos y entidades del ámbito de la Administración General del Estado y por los particulares en sus relaciones con aquellos, que hayan sido producidos por medios electrónicos, informáticos y telemáticos en soportes de cualquier naturaleza serán válidos siempre que quede acreditada su integridad, conservación y la identidad del autor, así como la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación.

En los producidos por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, dichos códigos o sistemas estarán protegidos de forma que únicamente puedan ser utilizados por las personas autorizadas por razón de sus competencias o funciones.

Requisitos:

De emisión de documentos

Integridad	Del documento
Conservación	En Registro, de la emisión del documento
Identificación	Del autor, dentro del documento
Autenticación	Del autor, dentro del documento

De autenticidad de la voluntad

Identificación	Del autor, en Registro
Autenticación	Del autor, en Registro

24.5.3. Validez de las copias: garantía de su autenticidad, integridad y conservación

Art. 6.2:

Las copias de documentos originales almacenados por medios o en soportes electrónicos, informáticos o telemáticos, expedidas por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, tendrán la misma validez y eficacia del documento original siempre que quede garantizada su autenticidad, integridad y conservación.

Requisitos:

Autenticación	Del autor de la copia, dentro de la copia
Integridad	Del documento original, dentro de la copia
Conservación	En Registro, de la emisión de la copia

24.5.4. Garantía de realización de las comunicaciones

Art. 7.1

La transmisión o recepción de comunicaciones entre órganos o entidades del ámbito de la Administración General del Estado o entre éstos y cualquier persona física o jurídica podrá realizarse a través de soportes, medios y aplicaciones informáticos, electrónicos y telemáticos, siempre que cumplan los siguientes requisitos:

a) La garantía de su disponibilidad y acceso en las condiciones que en cada caso se establezcan.

b) La existencia de compatibilidad entre los utilizados por el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseños de registro establecidos por la Administración General del Estado.

c) La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados.

Requisitos:

Disponibilidad	De medios para dar continuidad y calidad a la comunicación
Identificación	En Registro, señalando condiciones de acceso para el sujeto identificado

Compatibilidad	Tanto de códigos y formatos o diseños como de los medios utilizados
Confidencialidad	Del contenido de la comunicación, inutiliza la interceptación
Integridad	Del contenido de la comunicación, detecta la alteración
Control de Accesos	Rechaza las identificaciones no registradas

24.5.5. Validez de comunicaciones y notificaciones a los ciudadanos; constancia de transmisión y recepción, estampación de fechas y contenido íntegro, identificación fidedigna de remitente y destinatario

Art. 7.2

Las comunicaciones y notificaciones efectuadas en los soportes o a través de los medios y aplicaciones referidos en el apartado anterior serán válidas siempre que:

a) Exista constancia de la transmisión y recepción de sus fechas y del contenido íntegro de las comunicaciones.
b) Se identifique fidedignamente al remitente y al destinatario de la comunicación.
c) En los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos hayan señalado el soporte, medio o aplicación como preferente para sus comunicaciones con la Administración General del Estado en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa.

Requisitos:

Certificación	En Registro, dando constancia de la transmisión y recepción, con sus fechas y del contenido íntegro de la notificación
Autenticación	De ambos corresponsales, durante el proceso de comunicación
Compatibilidad	El soporte, medio o aplicación señalado como preferente ha de ser compatible con el/los de la Administración General del Estado

24.5.6. Comunicaciones por medios preferentes del usuario; comunicación de la forma y código de accesos a sus sistemas de comunicación

Art. 7.3

En las actuaciones o procedimientos que se desarrollen íntegramente en soportes electrónicos, informáticos y telemáticos, en los que se produzcan comunicaciones

caracterizadas por su regularidad, número y volumen entre órganos y entidades del ámbito de la Administración General del Estado y determinadas personas físicas o jurídicas, éstas comunicarán la forma y código de accesos a sus sistemas de comunicación. Dichos sistemas se entenderán señalados con carácter general como preferentes para la recepción y transmisión de comunicaciones y notificaciones en las actuaciones a las que se refiere este apartado.

Requisitos:

Identificación	Del código de acceso al sistema de comunicación del usuario
Compatibilidad	De la forma del acceso, con los medios disponibles por la Administración General del Estado

24.5.7. Validez de fechas de notificación para cómputo de plazos; anotación en los registros generales o auxiliares a que hace referencia el artículo 38 de la LRJ-PAC

Art. 7.4

Las fechas de transmisión y recepción acreditadas en las comunicaciones reseñadas en los apartados anteriores serán válidas a efectos de cómputo de plazos y términos, a cuyos efectos se anotarán en los registros generales o auxiliares a que hace referencia el artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

A estos efectos los Sistemas de Información que integren procesos de transmisión y recepción podrán constituirse en registros auxiliares cuando recojan todos los datos a que hace referencia el párrafo segundo del apartado 3 del artículo 38 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y se tenga acceso a ellos desde las unidades encargadas de los registros, generales correspondientes.

Requisitos:

Certificación	En Registro Auxiliar, de las fechas comunicadas al usuario
Control de Accesos	Al Registro Auxiliar, para asegurar que solamente acceden al mismo unidades de Registro General

24.5.8. Conservación de documentos; medidas de seguridad que garanticen la identidad e integridad de la información necesaria para reproducirlos

Art. 8.2

Los documentos de la Administración General del Estado y de sus entidades de derecho público vinculadas o dependientes que contengan actos administrativos que afecten a derechos o intereses de los particulares y hayan sido producidos mediante técnicas electrónicas, informáticas o telemáticas podrán conservarse en soportes de esta naturaleza, en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo.

Requisitos:

Identificación	En el Registro, del documento original
Certificación	En el Registro, de la información que asegura la integridad del documento original
Integridad	De la información capaz de reproducirlo y contrastarlo con la información de notarización

24.5.9. Acceso a documentos almacenados; disposiciones del artículo 37 de la Ley 30/1992, y, en su caso, de la Ley Orgánica 5/1992. Normas de desarrollo

Art. 8.3

El acceso a los documentos almacenados por medios o en soportes electrónicos, informáticos o telemáticos se regirá por lo dispuesto en el artículo 37 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y, en su caso, por la Ley Orgánica 5/1992, de Regulación del tratamiento automatizado de los datos de carácter personal, así como en sus correspondientes normas de desarrollo.

Requisitos:

Control de Accesos	Al Registro, donde se encuentre identificado el documento original

24.5.10. Almacenamiento de documentos; medidas de seguridad que garanticen su integridad, autenticidad, calidad, protección y conservación

Art. 8.4

Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos.

Requisitos:

Integridad	De la información contenida en el soporte
Autenticidad	Del soporte y de su contenido
Calidad	Del soporte
Conservación	Del soporte, del Registro del soporte, y del proceso que recupera la información del soporte
Identificación	En el Registro del soporte, del autor del soporte, y de quienes pueden acceder al soporte
Control de Accesos	Rechaza las identificaciones no registradas

De manera resumida, la situación de conjunto es la que se recoge en el siguiente cuadro resumen de requisitos de seguridad, normalización y conservación de las aplicaciones en el RD 263/1996.

1. Confidencialidad *2. Autenticación* *3. Integridad* *4. Disponibilidad*	*5. Control de accesos* *6. Identificación* *7. Certificación*	*8. Conservación* *9. Compatibilidad* *10. Calidad*

Articulado RD 263/1996 – Requisitos de Seguridad	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Garantías de seguridad de soportes, medios y aplicaciones (Art. 4.3, y 4.4)			■		■	■			■	■
Emisión de documentos (Art. 6.1)			■			■		■		
Autenticidad de voluntad (Art. 6.1)		■				■				
Validez de las Copias (Art. 6.2)		■	■							
Garantía de realización de las comunicaciones (Art. 7.1)	■		■	■	■	■			■	

Articulado RD 263/1996 – Requisitos de Seguridad	1	2	3	4	5	6	7	8	9	10
Validez de comunicaciones y notificaciones (Art. 7.2)										
Comunicaciones por medios preferentes del usuario (Art. 7.3)										
Validez de fechas de notificación para cómputo de plazos (Art. 7.4)										
Conservación de documentos (Art. 8.2)										
Acceso a documentos almacenados (Art. 8.3)										
Almacenamiento de documentos (Art. 8.4)										

24.6. CONCLUSIONES SOBRE EL PAPEL DE LA AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN ELECTRÓNICA

El concepto de "Administración electrónica", Administración virtual o de la Administración en la Sociedad de la Información ha tenido en los últimos años una relevancia creciente tanto en medios profesionales como para el público en general.

En las Actas de la 30ª Conferencia del Consejo Internacional sobre las Tecnologías de la Información en las Administraciones del Estado (ICA), celebrado en octubre de 1996 en Budapest, se recoge la siguiente definición de Administración electrónica:

- Es la posibilidad de que los ciudadanos accedan a los servicios administrativos de manera electrónica, 24 horas al día, 7 días a la semana, para la obtención de información.
- Además, es la posibilidad de efectuar trámites de manera electrónica con los ciudadanos, con otros órganos o Administraciones y con las empresas.
- También consiste en reducir y sustituir el papeleo gracias a la extensión del correo electrónico.

También se identifican los mecanismos a través de los cuales se favorece la introducción de la Administración electrónica:

- El principal es la demanda de los ciudadanos de servicios similares a los del sector privado.

- Los importantes ahorros en personal y en costes de mantenimiento.
- La simplificación de funciones y procesos.
- La resolución de problemas más rápida con sistemas en línea que a través de correspondencia escrita.
- La prevención del fraude, mediante una mejor identificación y auditabilidad de las transacciones electrónicas.
- La apertura de nuevas oportunidades para los usuarios. Pueden hacerlo por teléfono o a través de Internet en lugar de desplazándose a una oficina.
- La facilidad de uso.

En otras palabras, la estrategia para poner en práctica la Administración electrónica consiste en proporcionar servicios mediante técnicas EIT, con eficacia en el coste y accesibilidad para los ciudadanos, de acuerdo, entre otros, con los siguientes principios:

- *Elección* del medio como preferente, no exclusivo.
- *Confianza* en que la información recogida de ciudadanos y empresas será protegida de modo que no pueda ser accedida incorrectamente o manipulada.
- *Accesibilidad* a los servicios cómo, dónde y cuándo el cliente los requiera.
- *Difusión* de la información, siempre que ésta no deba ser protegida por razones de privacidad o de confidencialidad comercial.
- *Eficacia* en la prestación del servicio, simplificando trámites y reduciendo el tiempo de respuesta.
- *Racionalización*, evitando en lo posible la duplicación de esfuerzos y recursos que puedan ser compartidos.

En este contexto de la Administración electrónica, ya hemos visto como en España, en el caso de la Administración General del Estado, se dispone de un marco legal que no sólo permite, sino que impulsa, la utilización de las técnicas EIT para las relaciones con los ciudadanos. De este marco jurídico se deduce que existen unos requisitos concretos de seguridad, normalización y comunicación para hacer realidad este nuevo tipo de Administración. La Auditoría informática en la Administración tiene ante sí como una tarea especialmente relevante la de comprobar el cumplimiento de estos requisitos en aplicaciones o sistemas de información concretos, y más en particular, en aquellos sistemas, como los de informatización de registros, orientados a facilitar las relaciones de ciudadanos y empresas con las Administraciones.

24.7. CUESTIONES DE REPASO

1. ¿Qué se expone en la Ley de Régimen Jurídico de las Administraciones Públicas respecto a la utilización de las TIC en la Administración?

2. ¿Cuáles son los problemas de normalización que influyen en la relación de los ciudadanos con las Administraciones Públicas?

3. ¿Cuáles son los requisitos de validez y eficacia de los documentos electrónicos?

4. ¿Cuáles son los principales aspectos a auditar en la informatización de un registro?

5. ¿Cuál es el objetivo del Real Decreto 263/1996?

6. ¿Cuáles son los requisitos de seguridad en el texto del Real Decreto 263/1996?

7. ¿Qué tipo de requisitos impone la garantía de realización de las comunicaciones?

8. ¿Qué se especifica en cuanto acceso a documentos almacenados en la Ley 30/1992 y en la Ley Orgánica 5/1992?

9. Defina, ¿en qué consiste la administración electrónica?

10. ¿Qué mecanismos emplearía para favorecer la introducción de la Administración electrónica?

CAPÍTULO 25

AUDITORÍA INFORMÁTICA EN LAS PYMES

Carlos M. Fernández Sánchez

25.1. PREÁMBULO

25.1.1. Las PYMES y las tecnologías de la Información

El presente capítulo pretende ser una contribución que se sume al esfuerzo por conseguir una mayor rentabilidad de los sistemas de Información en las empresas y más concretamente en las denominadas PYMES (Pequeñas y Medianas Empresas). La importancia de las PYMES viene dada ante todo por su número –más de dos millones de empresas que conforman el tejido empresarial– así como por su potencialidad, ya que constituyen la base del desarrollo empresarial, siendo una fuente de generación del 170% del empleo total en España. Si analizamos la situación empresarial en los países iberoamericanos integrados en la OCDE comprobamos que la situación relevante de las PYMES es muy parecida a la española, con una aportación al PIB del 40% al 50%. A la vista de estos datos, es un hecho por fin asumido por todos los estamentos públicos y privados de la sociedad actual la necesidad de reformar la competitividad y rentabilidad de las PYMES favoreciendo su estabilidad y la que éstas aportan a la economía. Para contribuir a ello, el primer paso es abordar su problemática interna: su propio funcionamiento; y dentro del mismo, los sistemas de información que han de permitir la gestión y seguimiento de las principales variables del negocio, facilitando la correcta toma de decisiones, minimizando riesgos, y consiguiendo de este modo ampliar su competitividad en un mercado cada vez más abierto y liberalizado.

Es asimismo un hecho perfectamente demostrado que el Control Interno Informático y su auditoría permite gestionar y rentabilizar los sistemas de información de la forma más eficiente, optimizando, en suma, resultados. Por este hecho hemos creído de interés abordar en el presente capítulo la exposición de este método de AUDITORÍA INFORMÁTICA expuesto de forma breve y directa en la convicción de que, poniéndolo en práctica, se logrará que los Sistemas de Información sean fiables, exactos, y ante todo, den el fruto que los empresarios esperan de ellos.

25.1.2. Metodología de la Auditoría Informática

En la actualidad existen tres tipos de metodologías de Auditoría Informática:

- R.O.A. (RISK ORIENTED APPROACH), diseñada por Arthur Andersen.
- CHECKLIST o cuestionarios.
- AUDITORÍA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; Paquete de seguridad RACF, etc.).

En sí las tres metodologías están basadas en la minimización de los riesgos, que se conseguirá en función de que existan los controles y de que éstos funcionen. En consecuencia, el auditor deberá revisar estos controles y su funcionamiento.

De estas tres metodologías, la más adecuada a la Auditoría de las PYMES es a nuestro juicio la de CHECKLIST, por ser la de más fácil utilización.

25.2. INTRODUCCIÓN

25.2.1. ¿En qué consiste la guía de autoevaluación?

Esta guía de autoevaluación pretende ser un sistema sencillo y fiable de conocer la situación general del sistema de información de una empresa, así como definir el estado del control de dichos sistemas tomando como control la definición de la ISACA (Information System, Audit and Control Association).

"Los métodos que abarquen las políticas, procedimientos, prácticas, estándares y estructuras organizativas que aseguren la adecuación de la gestión de los activos informáticos y la fiabilidad de las actividades de los sistemas de información."

No se pretende con la misma eliminar las funciones del auditor (interno o externo) informático, sino que el responsable de los sistemas de información, el Gerente o Director de un departamento o de la misma empresa pueda hacerse una idea

suficientemente aproximada del estado de sus sistemas, pudiendo abordar, en caso necesario, un estudio más intenso o especializado de los mismos. Resulta, pues, un enfoque de Auditoría Interna tomando como base que la información es un activo más de la empresa y como Auditoría Informática:

"Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva eficazmente los fines de la organización y utiliza eficientemente los recursos de este modo, así como sustenta y confirma la consecución de los objetivos tradicionales del auditor."

Asimismo, con esta guía pretendemos que el usuario o el Auditor pueda comprobar por sí mismo la fiabilidad y consistencia de sus sistemas mediante una metodología que no le obligue a tener amplios conocimientos de informática ni de Auditoría propiamente dichos.

25.2.2. ¿A quién va dirigida?

Tal y como el título indica, esta guía está orientada a las Pequeñas y Medianas empresas, y dentro de las mismas, a los responsables de los sistemas de información, gerentes, directivos o auditores.

Consideramos que esta guía puede ser de gran utilidad a la hora de examinar y potenciar los sistemas de información y, en consecuencia, para mejorar substancialmente la gestión y control de la propia empresa.

El auditor podría ser un financiero con conocimientos de informática o un auditor informático junior.

25.2.3. Conocimientos necesarios

Según algunos autores, no resulta necesario tener conocimientos informáticos para realizar una auditoría informática mediante la técnica utilizada en esta guía (CHECKLIST). No obstante, creemos necesario un mínimo de formación específica para, al menos, saber qué es lo que se quiere analizar así como algunos conceptos no nos resulten excesivamente extraños. Fundamentalmente esos conocimientos serán de la índole de:

- Minicomputador.
- Red Local.
- PC.

- Periféricos.
- Software de Base.
- Eficacia de un servicio informática.
- Seguridad Lógica.
- Seguridad Física.
- Etc.

Asimismo será necesario conocer en profundidad el organismo o área a evaluar; su organización, composición y características principales, así como los medios de que se disponen: plantilla, datos técnicos, etc. Por supuesto es deseable que se tengan unos conocimientos informáticos más exhaustivos, pues pueden ayudar a la ponderación de los controles, pero insistimos en que no son indispensables.

25.2.4. Entornos de aplicación

Esta guía está enfocada hacia tres grandes entornos que son:

- Minicomputadores e informática distribuida.
- Redes de Área Local.
- PCs.

Dicho enfoque es, a nuestro entender, el más lógico, puesto que son los citados entornos los que se utilizan (quizá en casos determinados con alguna característica especial) en los círculos de la pequeña y mediana empresa.

25.2.5. Metodología utilizada

La metodología utilizada es la Evaluación de Riesgos (ROA Risk Oriented Approach) recomendada por ISACA (Information System, Audit and Control Association, Asociación Internacional de Auditores de Sistemas de Información).

Esta evaluación de Riesgos se desarrolla sobre determinadas áreas de aplicación y bajo técnicas de Checklist (Cuestionarios) adaptados a cada entorno específico; deberá tenerse en cuenta que determinados controles se repetirán en diversas áreas de riesgo. Esto es debido a que dichos controles tienen incidencia independiente en cada una y, que se pretende poder analizar cada área independientemente, es necesaria dicha repetición. Asimismo los controles generales y algunos controles de características especiales, como pueden ser los de bases de datos, se aplicarán teniendo en cuenta las particularidades de cada entorno.

25.3. UTILIZACIÓN DE LA GUÍA

Tal y como hemos apuntado anteriormente, la autoguía está dividida en varias áreas de riesgo, concretamente seis, que son:

1. Riesgo en la continuidad del proceso.
2. Riesgo en la eficacia del servicio.
3. Riesgo en la eficiencia del servicio.
4. Riesgos económicos directos.
5. Riesgos de la seguridad lógica.
6. Riesgos de la seguridad física.

25.3.1. Fases de la autoevaluación

Para aclarar un poco el enfoque vamos a tratar de explicar someramente el significado de cada uno de ellos, teniendo en cuenta que no existe una separación absoluta entre los mismos, sino que frecuentemente se solapan e incluso determinados riesgos conllevan otros que se han evaluado en diferente área. No obstante creemos que existe una cierta especificidad en los controles a llevar a cabo, además, se ha pretendido orientar el análisis a unas áreas lo más próximas a la empresa y sus intereses de forma que el directivo o empresario pueda hacer una evaluación directa sin descartar que posteriormente se pueda contar con la interpretación posterior más exhaustiva de un analista o auditor informático.

Riesgo en la continuidad del proceso

Son aquellos riesgos de situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y, por ende, llegar a perjudicar gravemente a la empresa o incluso también a paralizarla. Se deberá hacer especial hincapié en el análisis estricto de estos riesgos puesto que, si bien otros podrían afectar relativamente a la empresa o bien causarle perjuicios de diverso tipo, éstos podrían ocasionar un verdadero desastre. No pretendemos ser alarmistas y, por supuesto, no todos los riesgos analizados llevan a paralizar la empresa, pero insistimos en tener muy en cuenta el análisis exhaustivo de estos riesgos.

Riesgos en la eficacia del servicio informática

Entenderemos como eficacia del servicio la realización de los trabajos encomendados. Así pues, los riesgos en la eficacia serán aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

Riesgo en la eficiencia del servicio informático

Entenderemos como eficiencia del servicio la mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad de servicio. Hay que matizar en este aspecto que determinados controles podrían resultar una mejora considerable de la eficiencia del servicio pero igualmente podrían resultar económicamente poco rentables sobre todo para pequeñas empresas. La valoración de dichos controles deberá ser analizada por los responsables de la empresa en cuya mano estará la decisión de aplicación de los mismos.

Riesgos económicos directos

En cuanto a estos riesgos se analizarán aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse, e incluso aquellos gastos derivados de acciones ilegales con o sin consentimiento de la empresa que pudieran transgredir la normativa de la empresa o las leyes vigentes (LORTAD).

Riesgos de la seguridad lógica

Como riesgos en seguridad lógica entenderemos todos aquellos que posibiliten accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos. Incluiremos igualmente aquellos inherentes a transmisiones pese a que quizá en determinados ámbitos de aplicación podrían constituir un área independiente pero que se anexan con el fin de compactar el sistema de análisis.

Riesgos de la seguridad física

Los riesgos en cuanto a seguridad física comprenderán todos aquellos que actúen sobre el deterioro o apropiación de elementos de información de una forma meramente física.

Dadas estas áreas de riesgos, el usuario podrá valorar cada una independientemente según sus necesidades. Aun así, se consideran como más importantes, y casi podríamos asegurar que imprescindibles, las dos primeras:

- Riesgo en la continuidad del proceso
- Riesgo en la eficacia del servicio

por lo que cualquier análisis debería ser comenzado con las mismas.

Todas estas áreas están incluidas en cada ámbito de aplicación de acuerdo con su especificidad según la división que dimos al principio de minicomputadores, redes locales y PCs.

25.3.2. Valoración de resultados

La autoguía se compone de una serie de cuestionarios de control. Dichos cuestionarios podrán ser contestados mediante dos sistemas indicados en los mismos:

En el primer sistema se responderá con SÍ NO o N/A (NO APLICABLE si la respuesta no lo fuera por cualquier causa). Estos cuestionarios de respuesta directa tendrán un valor numérico de 1 a 10 anexo a la pregunta que habrá que poner en el lugar de la respuesta.

CONTROLES	SÍ	NO	N/A
¿Posee la instalación equipos de continuidad en caso de cortes de energía como puede ser los sistemas de alineación ininterrumpido?	7	4	

En el caso de que se dispusiera de UPS (Sistema de Alimentación Interrumpida), se pondría en la casilla del SÍ el valor 7, en caso contrario pondríamos el valor 4 en la casilla del NO. La diferencia de valoración puede estar determinada porque la existencia se considera una mejora sustancial, sin embargo, la no existencia podría ser de escasa importancia.

En el segundo sistema no existirá un número guía de ponderación y será el propio usuario quien deberá dar una valoración a la respuesta. Generalmente en estos casos los controles comenzarán con la propuesta EVALÚE... y la valoración que habrá que dar estará anexada a la pregunta con los valores mínimos y máximo; por ejemplo:

CONTROLES	SÍ	NO	N/A
Evalúe la carga de trabajo en época alta de proceso (Ponga el resultado en la casilla no) 1-30.	7	4	

Como habrá observado, también se le indicará en qué casilla deberá incluir el resultado de su ponderación. Dicha ponderación se podría obtener, y dado el caso de

la pregunta del ejemplo, mediante el número de horas extras del personal, horas de trabajo de los equipos, o simplemente mediante observación personal en los casos que fuera posible. Una vez finalizado el cuestionario se sumarán los valores de la casilla SÍ y se restarán los del NO, lo que nos dará un valor que podremos comparar con los estándares del cuestionario (que el usuario habrá valorado en un principio).

Por último existirán algunas cuestiones que no tengan valoración, sino que irán acompañadas de un asterisco. Estos controles son considerados de alto riesgo, y por tanto indispensables. La idea es que un sistema sin estos controles podría abocar al desastre informático y en algunos casos al desastre de la empresa. En ocasiones no se da la debida importancia a los mismos y solamente se ponderan en lo que valen al ocurrir el problema. Por tanto insistimos: estos controles deberán tenerse muy en cuenta a la hora de realizar la evaluación y, en caso de inexistencia, dar primacía a su implantación.

25.4. MINICOMPUTADORES E INFORMÁTICA DISTRIBUIDA. RIESGO EN LA EFICACIA DEL SERVICIO INFORMÁTICO

CONTROLES	SÍ	NO	N/A
Existen planes a largo plazo para el departamento de informática.			
Valore la conexión de esos planes con los planes generales de la empresa.			
Cubren los planes del D.I. los objetivos a largo plazo de la empresa, valórelo.			
Existen planes a largo plazo para el departamento de informática.			
Valore la conexión de esos planes con los planes generales de la empresa.			
Cubren los planes del D.I. los objetivos a corto plazo de la empresa, valórelo.			
Existe un comité de planificación o dirección del departamento de informática.			
Dicho comité está compuesto por directivos de departamentos de usuario.			
Existe en dicho comité algún miembro con conocimientos informáticos exhaustivos.			
El comité realiza algún tipo de estudio para analizar la coherencia de su departamento de información con los avances tecnológicos.			

CONTROLES	SÍ	NO	N/A
Valore la celeridad en la implantación de las recomendaciones del comité informático.			
Qué importancia le asigna la dirección de la empresa al comité/ dirección de informática.			
Valore la congruencia entre los planes a largo y corto plazo del D.I.			
Son adecuados los recursos asignados al D.I. para cumplir con los objetivos a corto plazo.			
Existe una adecuada vía de comunicación y control de cumplimiento de objetivos a corto y largo plazo por parte de la dirección.			
Valore la precisión en el cumplimiento de los planes a corto plazo del D.I.			
Existen políticas para la planificación, control y evaluación del D.I.			
Evalúe la integración de las directivas de política de alta dirección en el D.I.			
Existen estándares que regulen la explotación de recursos del D.I.			
Evalúe la calidad y vigencia de los estándares de explotación de recursos del D.I.			
Evalúe el cumplimiento de los estándares de explotación de recursos del D.I.			
Existen procedimientos sobre las responsabilidades, peticiones de servicio y relaciones entre los diferentes departamentos y el D.I.			
Dichos procedimientos están adecuadamente distribuidos en los diferentes departamentos.			
Evalúe el cumplimiento de dichos procedimientos por parte de los diferentes departamentos.			
El D.I. está separado orgánicamente en la estructura orgánica de la empresa.			
Es independiente la ubicación del D.I. de los otros departamentos de la empresa.			
Están claramente definidas las unidades organizativas en el D.I.			
Están separadas las unidades de desarrollo de sistemas y explotación.			
Están separadas las unidades de explotación y control de datos.			
Están separadas las unidades de administración de bases de datos y desarrollo de sistemas.			
Evalúe la independencia de las funciones del personal entre las diferentes unidades.			

CONTROLES	SÍ	NO	N/A
¿Existe una descripción por escrito (manual de operaciones y procedimientos) de cada puesto de trabajo en las diferentes unidades de D.I?			
¿La descripción del puesto de trabajo incluye definiciones de conocimientos y pericia técnicos?			
¿Los manuales de operaciones y procedimientos pasan una revisión mínima anual?			
¿Existe un método de evaluación para cubrir las vacantes del D.I?			
Evalúe la adecuación del método y políticas de selección para cubrir las antedichas vacantes.			
Evalúe la conformidad del personal del D.I. con las políticas y el sistema de selección			
¿Existe una política definida por la dirección del D.I. para promoción del personal?			
Evalúe la conformidad del personal del D.I. con las políticas y el sistema de promoción.			
¿Existe un programa de orientación formación y reciclaje de personal de plantilla?			
¿Tiene una revisión al menos anual dicho programa de reciclaje?			
¿Supone el programa de reciclaje al menos el 10% del presupuesto del D.I?			
Valore la formación interna recibida en el programa de reciclaje.			
¿Cuál es la valoración que da el personal al programa de formación y reciclaje?			
Contraste y evalúe la adecuación entre las fichas de formación del personal y las exigencias de conocimientos o pericia necesaria de los puestos.			
¿Existe algún método de control y evaluación de consecución de objetivos de cada puesto de trabajo?			
¿Está informado y comprende el personal el sistema de evaluación sobre consecución de objetivos?			
¿Existe una lista de aplicaciones de tratamiento de datos cuya explotación está programada regularmente?			
¿Se especifica en dicha lista tiempos de preparación y tratamiento?			
¿Se contrasta dicha lista con el nivel de acuerdo de servicio del D.I?			
¿Existe algún sistema de control para la carga de trabajo del D.I?			

CONTROLES	SÍ	NO	N/A
¿Ha establecido el D.I. prioridades de tratamiento de los diferentes trabajos?			
Evalúe la carga de trabajo del D.I. en época baja de proceso (ponga el resultado en no).			
Evalúe la carga de trabajo del D.I. en época alta de proceso (ponga el resultado en sí).			
Evalúe la capacidad de los equipos disponibles para satisfacer la demanda en la época alta de proceso (resultado en sí).			
Evalúe el exceso de capacidad de los equipos disponibles para satisfacer la demanda en la época baja de proceso (resultado en no)			
¿Qué valoración le dan los trabajadores del área de explotación a la disponibilidad de equipos en época alta de trabajo (resultado positivo en sí y resultado negativo en no)?			
Evalúe la capacidad de los recursos humanos para satisfacer la demanda en la época alta de proceso (resultado en sí)			
Evalúe el exceso de capacidad de los recursos humanos disponibles para satisfacer la demanda en la época baja de proceso (resultado en no).			
¿Qué valoración le dan los trabajadores del área de explotación a la disponibilidad de recursos humanos en épocas altas de trabajo (resultado positivo en sí y resultado negativo en no)?			
¿Existe un calendario de mantenimiento preventivo de material o logical?			
¿Se verifica que dicho calendario no incluya revisiones en períodos de carga alta de trabajo?			
¿Es el calendario de explotación lo suficientemente flexible como para acomodar tiempos de no funcionamiento a fin de realizar revisiones?			
¿Realiza la dirección del D.I. un control y seguimiento del flujo de trabajo y de las variaciones del calendario de explotación?			
¿Se registran las variaciones del calendario de explotación?			
¿Existe material de recambio para el tratamiento de programas que exijan alto nivel de disponibilidad?			
¿Existe un procedimiento para evaluar las causas de los problemas de tratamiento de datos?			
¿Existe un registro de problemas de tratamiento de datos?			
¿Se toman acciones directas para evitar la recurrencia de los problemas de tratamiento de datos?			

CONTROLES	SÍ	NO	N/A
¿Existe una preasignación para la solución de problemas específicos de tratamiento de datos?			
¿Se ha determinado una prioridad en la resolución de problemas de tratamiento de datos?			
¿Existe un inventario de contenido de la biblioteca de soportes?			
¿Existe un procedimiento para inventariar los contenidos de la biblioteca de soportes?			
¿Existe algún responsable de mantenimiento de la biblioteca de soportes?			
Evalúe la exactitud del inventario de la biblioteca de soporte.			
¿Identifican las etiquetas de los soportes: nombre de archivo, fecha de creación, programa que lo creó y período de retención de soporte?			
¿Existe algún sistema de control de entrada y salida de la biblioteca de soporte?			
¿Existe un procedimiento de selección de logical acorde con los planes a corto y largo plazo de la empresa?			
¿Se lleva a cabo dicho procedimiento a la hora de analizar necesidades de logical?			
Evalúe la satisfacción de los usuarios de software respecto a la última adquisición.			
¿Existe algún procedimiento de prueba antes de efectuar cambios de logical de sistemas?			
¿Existe alguna persona especializada en implementación de logical de sistemas?			
¿Existe algún registro sobre los cambios realizados sobre el logical del sistema?			
¿Existe algún procedimiento de revisión de cambio del logical de sistemas antes de pasarlos a explotación?			
¿Existe algún registro de problemas de logical de sistemas?			
¿Se identifican y registran exhaustivamente la gravedad de los problemas de logical de sistema, la causa y su resolución?			
¿Se corresponde la implantación del sistema de informática distribuida o red con las especificaciones de los planes a corto y largo plazo de la empresa?			
¿Se han desarrollado planes de implantación conversión y pruebas de aceptación para la red de informática distribuida de la empresa?			

CONTROLES	SÍ	NO	N/A
¿Ha sido desarrollado dicho plan conjuntamente por el departamento de informática y la dirección de los departamentos usuarios afectados?			
¿Contempla dicho plan la aceptación de estándares de implantación, conversión y pruebas en redes informáticas distribuidas?			
¿Ha sido desarrollado el logical del sistema de acuerdo con la metodología del ciclo de desarrollo de sistemas de la organización o mediante una metodología cimentada y reconocida?			
¿Incluye el plan de implantación o conversión de la red de informática distribuida a todos los usuarios productores de datos imprescindibles?			
¿Se ha contemplado en el plan cualquier riesgo especial asociado a las redes distribuidas?			
¿Existen procedimientos de control generales de la red de informática distribuida?			
¿Se realizarán dichos procedimientos de control con una periodicidad mínima mensual?			
¿Existe un control de actividades excepcionales que se podieran realizar en la red de I.D.?			
¿Ha establecido el departamento de informática, desde la implantación de la red, un mecanismo para asegurar la compatibilidad de conjunto de datos entre aplicaciones a crecer la misma?			
¿Se han distribuido a todos los departamentos afectados declaraciones escritas de procedimientos operativos de la red de I.D.?			
¿Están adecuadamente canalizadas las peticiones de cambios de procedimientos operativos de la red de I.D.?			
¿Existe algún control sobre cambios autorizados o no en los procedimientos operativos de la red?			
¿Son analizados los cambios de los procedimientos operativos para ver si responden a necesidades reales de los usuarios?			
¿Ha establecido el departamento de informática controles sobre utilización de los contenidos de las bases de datos de la red?			
¿Aseguran dichos controles la estandarización de las definiciones de datos compartidos?			
¿Se mantienen diccionarios de datos comunes a los diferentes usuarios de las bases de datos?			
¿Está asegurado el control del cambio de definición de datos comunes de las bases?			

CONTROLES	SÍ	NO	N/A
¿Existe un sistema eficaz para evitar que los usuarios cambien la definición de datos comunes de las bases?			
¿Existe una comunicación regular sobre cambios efectuados en las bases de datos comunes?			
¿Existe algún sistema de control que asegure la compatibilidad de los contenidos de las bases de datos de la red?			
¿Existen controles establecidos por el departamento de informática sobre utilización de contenido de las bases de datos de la red?			
¿Existe algún procedimiento de control sobre los cambios de contenido y procedimiento de dichos cambios en las bases de datos de la red?			
¿Existe algún control que asegure que los cambios introducidos en los contenidos de la base dé datos mantienen la compatibilidad de dichas bases?			
¿Existe algún procedimiento establecido que asegure en todos los puntos de la red que los cambios críticos en los contenidos de las bases se lleven a cabo con puntualidad?			
¿Se ha establecido una política para identificación y clasificación de datos sensibles de la red?			
¿Existen mecanismos de seguridad que impidan introducciones o modificaciones erróneas de datos sensibles?			
¿Existe algún mecanismo de control que asegure una adecuada carga de la red especialmente en los períodos de trabajo crítico?			
¿Se han establecido y comunicado a los usuarios procedimientos efectivos para coordinar la operación de los programas de aplicación y la utilización de los contenidos de las B.D?			
¿Poseen todos los usuarios de la red especificaciones sobre disponibilidades, horarios, tiempo de respuesta, almacenamiento, respaldo y control operativo?			
¿Se realizan reuniones periódicas entre los usuarios para coordinar calendarios de explotación, especificaciones de tratamiento y procedimientos operativos?			
¿Establecen todas las instalaciones de departamentos usuarios de la red previsiones sobre necesidades de material fungible?			
¿Existe siempre un remanente de material fungible que asegure la continuación de los procesos, en los departamentos usuarios?			
¿Existen procedimientos establecidos por el departamento de informática para la gestión y control del logical de comunicaciones?			

CONTROLES	SÍ	NO	N/A
¿Están incluidos en dicho procedimiento estándares sobre la utilización de dicho logical?			
¿Se han remitido descripciones escritas sobre los citados procedimientos a todos los departamentos usuarios?			
¿Se han establecido prioridades de transmisión asignadas a los mensajes enviados por la red?			
Evalúe la satisfacción de los usuarios sobre las transmisiones a través de la red, sobre todo en períodos críticos.			
¿Existen planes de formación para usuarios de la red?			
¿Existen responsables que evalúen el correcto uso de la red por parte de los usuarios?			
¿Están perfectamente identificados todos los elementos físicos de la red (unidades de control, módems cables etc.) mediante etiquetas externas adecuadas?			
¿Está asegurando en un tiempo prudencial la reparación o cambio de elementos físicos de la red?			
¿Se realiza por parte de personal especializado una revisión periódica de todos los elementos de la red?			
¿Existe algún sistema para controlar y medir el funcionamiento del sistema de informática distribuida de la red?			
¿Existe una estructura que asegure que la explotación de máxima prioridad se lleva a cabo y se transmite en primer lugar?			
¿Se han desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres del sistema (abrazos mortales)?			
¿Existe una rutina que asegure que ningún proceso o dato de baja prioridad va a estar sin procesar indefinidamente en la red?			
¿Existen mecanismos que controlen los tiempos de respuesta de la red y la duración de los fallos de operación de la misma?			
¿Se controlan regularmente todos los procesadores de la red?			

25.5. CONCLUSIONES

Dado que en los restantes capítulos de este libro se aborda tanto la auditoría de otros entornos (minicomputadores, Redes de áreas local y PCs) como sus áreas de riesgo, en el presente capítulo nos hemos limitado únicamente a analizar la auditoría de los minicomputadores con respecto a los riesgos en la eficacia del servicio

informático dentro de una PYME, siendo aplicable esta metodología a cualquiera de los otros entornos informáticos.

En cualquier caso, siempre que se lleve a cabo una auditoría de empresa habrán de tenerse en cuenta, como mínimo, los siguientes controles generales:

Segregación de funciones, separación de los entornos de desarrollo y producción, control de programas fuentes y objetivos, procedimientos, estándares o nomenclatura para toda clase de objetivos en el sistema de Información, plan de seguridad lógica y física (copia de BACKUP o respaldo de datos y programas, plan de contingencia, etc.) y plan informático coordinado con el plan estratégico de la compañía.

Tanto a través de la guía de autoevaluación como a través de la auditoría de los mencionados controles generales se puede alcanzar el objetivo de gestión y certificación de los datos logrando conseguir la calidad total de los Sistemas de Información, rentabilizando así las inversiones en Tecnología de la Información.

25.6. LECTURAS RECOMENDADAS

Control Objetives for Information and Related Technology. 1996. Editorial Information System audit and Control Foundation.

Guía de seguridad informática. 1997. Vamos. Editorial SEDISI (Asociación Española de Empresas de Tecnologías de la Informática).

Emilio del Peso y otros. *Manual de dictámenes y peritajes informáticos* 1995. Editorial Díaz de Santos.

Marina Touriño, Carlos Manuel Fernández Sánchez y otros. *Papeles de Ávila: Expertos en Auditoría Informática.* 1986. Editorial CREI.

Seguridad en los Sistemas de Información. 1984. Fisher y traducido por Carlos Manuel Fernández Sánchez. Editorial Díaz de Santos.

EDP Auditing. 1992. Vamos. Editorial Auerbach Publishers.

Stanley & Coopers & Lybrand. *Handbook Of EDP Auditing.* 1985. Editorial Warren, Gorham Rlainont. INC.

Ron Weber. *EDP Auditing. Conceptual Foundations and Practice.* 1988. Editorial McGraw-Hill.

Dr. René Fonseca. *Auditoría Interna.* 1989. Editorial EDI ABACO.

Gonzalo Alonso Rivas. *Auditoría Informática.* 1988. Editorial Díaz de Santos.

J. Acha Iturmendi. *Auditoría Informática en la empresa.* 1994. Editorial Paraninfo.

Aurora Pérez Pascual. *La auditoría en el desarrollo de proyectos informáticos. 1988.* Editorial Díaz de Santos.

Carlos Manuel Fernández Sánchez. *Apuntes de la asignatura de Auditoría Informática.* Universidad Pontificia de Salamanca en Madrid. Curso académico 96-97.

Mi agradecimiento a D. Jesús Monedero Fernández, alumno de la asignatura de Auditoría Informática. Universidad Pontificia de Salamanca en Madrid.

25.7. CUESTIONES DE REPASO

1. ¿Por qué tiene tanta repercusión la auditoría informática de las PYMES?
2. ¿Qué tipo de metodología de auditoría informática es más adecuada para las PYMES?
3. Enumere los principales riesgos en la continuidad del proceso.
4. ¿Qué entiende por eficacia del servicio informático?
5. ¿A qué riesgos económicos directos se enfrentan las PYMES debido a la LORTAD?
6. ¿Cómo se puede evaluar la carga de trabajo de un equipo informático?
7. ¿Cómo mediría la satisfacción de los usuarios?
8. Segregación de funciones en las PYMES.
9. Elabore una lista de comprobación para auditar un computador personal.
10. ¿Cómo llevaría a cabo la auditoría de una hoja de cálculo?

CAPÍTULO 26

PERITAR *VERSUS* AUDITAR

Jesús Rivero Laguna

26.1. INTRODUCCIÓN

"Nunca segundas partes fueron buenas", afirma un viejo refrán castellano. No es éste el caso, sin embargo, de la segunda edición, que no reimpresión, de *Auditoría Informática. Un enfoque práctico.*

El éxito de ventas de la primera edición –motivado en buena medida por el hecho de haber sabido detectar sus Coordinadores una imperiosa necesidad de "conocimiento", además de por haber conseguido recopilar una cuidada y enciclopédica selección de temas y autores–, avala el obligado lanzamiento de esta *nueva* obra, con objetivos más allá del perfeccionamiento de la primera versión de 1997.

No me corresponde, pese a todo, a mí, y mucho menos en este lugar, discutir la aportación científico-didáctica de esta nueva obra, ya fuese tanto en su vertiente académica como profesional, si bien he estimado oportuno comenzar haciendo esta "introducción", habida cuenta de que no existía tal capítulo acerca de los *Informes, Dictámenes y Peritajes, Judiciales y Extrajudiciales* en la edición original, ni por supuesto acerca de los profesionales –con actividades afines a las de los auditores–, que los emiten a petición de terceras partes.

Aplaudo, pues, este buen criterio de los Coordinadores, en pro de una plena exhaustividad de su contenido inicial, confiando sólo en que su decisión también haya sido pertinente al proponerme la redacción de los apartados que siguen, donde he tratado de condensar parte de mi "capital intelectual" en esta área de conocimiento, atesorado inequívocamente en el Ejercicio Libre de la Profesión (ELP) en el Colegio Oficial de Ingenieros de Telecomunicación, como tal Ingeniero de Telecomunicación, especializado en el ámbito judicial y extrajudicial de las Peritaciones en Tecnologías de la Información, o de las ingenierías informática y de telecomunicación, no carente de posteriores iniciativas formativas de postgrado y profesionales en este contexto, en diversos ámbitos de actuación, privada e institucional, además de asociativa.

En el primer capítulo de la primera edición de esta misma obra, su autor –Alonso Hernández García–, comenzaba diciendo: "Definid y no discutiréis. Y aun sin la pretensión de que lo que se exponga en este capítulo sea indiscutible, parece muy conveniente delimitar el campo en que nos desenvolvemos". Pues bien, sería de necios no aplicarse la receta; por ello, y antes de aportar conocimientos específicos al tema objeto de este capítulo, dedicaré un primer apartado a "delimitar el campo", antes incluso que a "definir" conceptos.

26.2. CONSULTORES, AUDITORES Y PERITOS

Si el marco de comunicación con ustedes, amigos lectores, no fuese el formal de un texto escrito, me permitiría la licencia de relatarles en detalle –como acostumbro a hacer en mis conferencias y cursos–, aquel chiste de "la cigarra que se dirige al *Consultor* para preguntarle qué debería hacer para *vivir como una hormiga*, siempre feliz, trabajadora y absolutamente productiva". Seguramente conocerán el *desenlace*: "el Consultor facturó a la cigarra sus honorarios sólo por mostrarle un *Plan Estratégico*, dejándole a ella el problema de cómo desarrollar el oportuno *Plan Táctico* de ejecución".

Ciertamente, he podido constatar en repetidas ocasiones cómo los mismos profesionales confunden y superponen los campos de actividad de estas tres especialidades: *consultoría, auditoría y peritación*. Sin embargo, sus funcionalidades están bien delimitadas, y desde luego sus competencias, actuaciones y "productos", por los que facturan y se les abonan los oportunos honorarios.

De hecho, existen rígidas fronteras –establecidas incluso por mandatos jurídicos–, que impiden simultanear a un mismo profesional –o Compañía– ámbitos de actuación superpuestos con un mismo cliente; es decir, prestarle un servicio como "consultor", y antes/después como "auditor". Consecuencia de ello han sido las escisiones a nivel mundial de las grandes firmas de Consultores y Auditores, para dar cobertura legal a sus respectivas áreas de negocio, especialmente con determinados clientes estratégicos.

Hernández García, en el capítulo antes aludido ("La informática como herramienta del auditor financiero"), afirma, hablando de la auditoría, que aunque el "concepto permanece inamovible, lo que sí puede variar es su objeto y finalidad"; de ahí que surjan "confusiones, tanto entre los diferentes aspectos, áreas o enfoques en sí mismos, como por las debidas a la vertiginosa evolución que experimenta la especialidad".

Aunque no volveremos sobre lo ya tratado en este libro, sí utilizaremos por coherencia su esquema de discusión racional, para completar la visión de consultores y auditores, con la de los *peritos*. Así, seguiremos manteniendo la descomposición de "concepto" (PERITACIÓN, en este caso), en unos determinados elementos fundamentales; a saber: contenido, condición, característica temporal (introducido aquí por primera vez), justificación, objeto y finalidad.

ELEMENTOS CONCEPTUALES	***ÁMBITO DE ACTUACIÓN PROFESIONAL***		
	CONSULTORÍA	**AUDITORÍA**	**PERITACIÓN**
CONTENIDO	Consejo o asesoría	Opinión objetiva	Opinión subjetiva
CONDICIÓN (Carácter del "contenido")	Basada en la experiencia	Contrastada profesionalmente	Leal saber y entender
CARACTERÍSTICA (Momento en el tiempo)	A priori	A posteriori	A posteriori
JUSTIFICACIÓN (Base que sustenta el "contenido")	Análisis de datos	Procedimientos específicos (tendentes a proporcionar una seguridad razonable de lo que se afirma)	Examen real y directo de los hechos especificados en la prueba solicitada
OBJETO (Elemento sobre el que se aplica la "justificación")	Actividad o cuestión sometida a consideración y/o examen	Información determinada, obtenida en un cierto soporte	Elementos específicos proporcionados junto a la prueba propuesta
FINALIDAD ("Producto" final deseado)	Directrices recomendadas de actuación	Adecuación a la realidad, o fiabilidad de las expectativas atribuidas	Juicio de valor, aunque no vinculante para su receptor

*Tabla 26.1. Contextualización de la "**Peritación**", versus los ámbitos profesionales afines de la "**Consultoría**" y la "**Auditoría**"*

La Tabla 26.1 muestra el compendio de los tres ámbitos profesionales, extendiendo y perfeccionando lo ya visto para la consultoría y la auditoría. Nítidamente se pone de manifiesto la separación conceptual del ámbito de la "peritación" con respecto al de la consultoría y auditoría, ya de por sí diferenciadas[1], aunque

[1] Hernández García, Alonso (*Auditoría Informática* 1997, Cap. 1, pág. 10): "Especialmente el elemento *contenido* distingue claramente la auditoría de la consultoría. Dependiendo de que su contenido sea opinar sobre unos resultados *vs.* dar asesoramiento o consejo en relación con una actividad a desarrollar, se tratará de auditoría o consultoría".

existan opiniones afirmando que "las definiciones de la auditoría informática tienden a englobar el concepto de consultoría".

Entendemos que es importante hacer notar cómo la acción de peritar puede solicitarse en cualquier momento del proceso global, tanto de emisión de un "consejo o asesoría" (*CONSULTORÍA*), como de evacuación de una determinada "opinión objetiva" (*AUDITORÍA*), justamente para soportar técnicamente una determinada afirmación ("opinión subjetiva" de un experto en la materia, o *perito*), acreditándola como tal a partir del "juicio de valor" en la cuestión planteada, emitido en todo caso a posteriori, una vez establecida la "proposición de prueba" y aportados sus correspondientes "elementos específicos" a peritar .

Separados, por tanto, los tres ámbitos de actuación profesional convergen en su aplicación, quedando diferenciados en todo momento, en ocasiones con carácter imperativo.

26.3. DEFINICIÓN CONCEPTUAL DE PERITO

La *peritación* o *peritaje* es, según el *Diccionario de la Real Academia Española de la Lengua*, el trabajo o estudio[2] que hace un **perito**, para quien da tres acepciones diferentes o definiciones aclaratorias[3] que encierran en sí mismas matices distintos:

a) "sabio, experimentado, hábil, práctico en una ciencia o arte";

---

[2] Esta misma definición –tan simple– , de "trabajo, estudio o informe que hace el perito sobre una determinada materia" se encuentra en muchos otros diccionarios generales:
- *Gran Diccionario de la Lengua Española*
- *Diccionario Manual e Ilustrado de Lengua Española*
- *Diccionario General VOX, de la Lengua Española e Ilustrado*
- *Diccionario Enciclopédico ESPASA*
- *Diccionario Enciclopédico PLAZA & JANÉS*
- Diccionario ARISTOS
- etc.

[3] La triple acepción se menciona y comenta apartado c) de la página siguiente acerca del concepto de *Perito* es común a bastantes fuentes, incluso bien distintas en sus orientaciones:
- *Diccionario General VOX, de la Lengua Española e Ilustrado*
- *Diccionario Enciclopédico EDAF*
- *Gran Enciclopedia LAROUSSE*
- *Enciclopedia del Siglo XX*
- *Enciclopedia multimedia PLANETA AGOSTINI*
- *Enciclopedia universal interactiva CAJA MADRID*
- *Diccionario Enciclopédico ALFA, de SALVAT*
- *Enciclopedia ENCARTA, de MICROSOFT*
- Enciclopedia universal interactiva, de COLLIER, etc.

b) "persona que, poseyendo especiales conocimientos teóricos o prácticos, informa, bajo juramento, al juzgador, sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia"; y,

c) "persona que en alguna materia tiene título de tal, conferido por el Estado".

A los efectos que nos ocupan en esta obra apartaremos la acepción c), por su componente académica, vinculada a una titulación –universitaria, en general–, sin que ello quiera decir que no sea condición *sine qua non* su posesión en determinadas circunstancias.

También apartaremos de la discusión que pretendemos realizar inicialmente, la acepción b), por ser limitativa del concepto genérico de *perito*, no forzosamente vinculado a actuaciones judiciales en su quehacer profesional, pudiendo ser "*extrajudiciales*" u orientadas a la "*mediación y el arbitraje*".

El *Diccionario Enciclopédico SALVAT* aporta una cuarta acepción de conocida incidencia en nuestra sociedad, aunque bien pudiera quedar englobada en la primera de las acepciones, única con la que de hecho nos quedaremos para su discusión en este apartado. Así, según este diccionario de SALVAT, un *Perito* es un "práctico o conocedor de la naturaleza de un bien, de su mercado y de sus características y aplicaciones, que tiene por objeto atribuir un valor *(tasación pericial)* a ese bien"; no obstante, reconoce que "en ocasiones el peritaje no comporta tasación, y se limita a reunir un dictamen acerca de sus aplicaciones y características técnicas".

Queda pues claro, a partir de lo expuesto, el entorno definitorio de un Perito, delimitado por las siguientes características para estas "personas":

a) *con conocimientos*[4] en el ámbito de la opinión reclamada (hasta el límite de calificarle como "sabio"[5]);

b) *experimentados*, luego alguien que soporta su informe en vivencias adquiridas; y,

c) *hábiles o prácticos, en una ciencia o arte*, capaces de ejecutar y valorar resultados obtenidos a partir de la prueba planteada en un contexto tanto científico como artístico, según los casos.

De forma sucinta, podemos encontrar definiciones de perito auténticamente integradoras de estas características precedentes, como la aportada[6] por la *Gran*

---

[4] Según el *Diccionario de María Moliner*: "conocimientos especiales en una materia".
[5] Según el *Diccionario General Ilustrado de VOX:* "sabio experimentado".
[6] Entre otros diccionarios, tales como:
- *Enciclopedia del Siglo XX*
- *Diccionario del Español actual, de AGUILAR*
- *Diccionario enciclopédico SANTILLANA*

Enciclopedia LAROUSSE: "Experto, entendido en una ciencia o arte", o "en alguna rama del saber" (globalización del *Diccionario Enciclopédico GRIJALBO*), o "... en una ciencia, arte u oficio" (extensión de la *Enciclopedia Multimedia PLANETA AGOSTINI* y de la *Enciclopedia universal interactiva CAJA MADRID*).

26.3.1. Equivalencia con la denominación de "Experto"

De acuerdo con lo expuesto, podría inferirse que el término "Experto" es absolutamente equivalente al de "Perito", aunque sea este último el habitualmente utilizado.

Un recorrido por los diccionarios de sinónimos y antónimos[7] refuerza esto último:

- *sinónimos* de "Perito", son: *experto*, diestro, hábil, experimentado, conocedor, competente, especialista, técnico, práctico...
- *antónimos* de "Perito", son: *inexperto*, desconocedor, incapaz...

Lo mismo queda confirmado con un recorrido por diversos diccionarios de español-inglés:

- "Perito", se traduce[8] por "*Expert*", en general.
- Según los casos, puede añadirse un calificativo para precisar su campo de actividad[9]; por ejemplo: "*computer expert*", o "*expert in programming languages*". Pero, en todos los casos, especificando que se trata de "alguien con profundos conocimientos sobre algo" (*expert-person who knows a lot about something*), o desde luego con "conocimientos especiales, habilidades concretas o formación práctica en una determinada parcela del saber" (*person with special knowledge, skill or training in a particular field*)[10].

Un término alternativo acuñado para los "expertos", aunque menos utilizado con carácter genérico, es el de los *Peritos forenses*, muchas veces asociado al ámbito judicial y en áreas de conocimiento muy concretas como la medicina (caso de los "médicos forenses"). De hecho, existen categorías y áreas de peritaje forense privado que se utilizan habitualmente, tales como:

- "peritos forenses de grado superior" (desde médicos y psicólogos hasta ingenieros e informáticos, pasando por licenciados en arte o biólogos);

---

[7] *Diccionario Espasa de Sinónimos y Antónimos*, *Diccionario Manual de Sinónimos y Antónimos*, etc.

[8] *COLLINS, Dictionary, Dictionary of Information Technology*, etc.

[9] Dictionary of Information, Dictionary of Information Technology, etc.

[10] Oxford Advanced Learner's.

- "peritos forenses de grado medio" (desde ingenieros técnicos y aparejadores, a censores jurados de cuentas o topógrafos); y,
- "peritos forenses de grado técnico" (desde peritos calígrafos, gemólogos, filatélicos y numismáticos, a agentes de la propiedad inmobiliaria, pesadores y medidores...).

26.3.2. Acerca de la adquisición de *"expertise"*

Hemos visto cómo en una primera *vertiente conceptual*, o definitoria, podemos encontrar respuesta al concepto de "Perito" en los mismos diccionarios. También hemos visto cómo el término "perito" –experto en determinada materia, radicando su valor en los "conocimientos / experiencia" que "posee / ha adquirido"– no tiene una traducción precisa en otras lenguas, utilizándose "*expert*" –generalmente asociado a su rama específica de conocimiento–, por ejemplo en las lenguas anglosajonas.

La cuestión remanente sería entonces dónde ha adquirido *su experiencia*[11], porque "la experiencia es buena, cuando no se compra demasiado cara" *(Experience is good, if not bought too dear)*[12]. Dicho de otro modo, queremos entender la experiencia en el sentido de acumulación de conocimientos por estudio y/o vivencias de "hechos", no necesariamente "fracasos", en la acepción del poeta y moralista francés Paul AUGUEZ[13]: "la experiencia es la suma de nuestros desengaños".

Nuestra doctrina pues, iría más en consonancia con la de Francisco BANCES CANDAMO[14]:

> "Docta es, pero peligrosa,
> escuela la de los yerros,
> si en ellos ha de enseñarse.
> Porque si hay elección en ellos
> que puede costar la vida,
> ¿para qué es la conciencia? Luego,
> ¡feliz quien estudia a costa
> de los errores ajenos!"

Lo mismo, con palabras similares, nos han dicho muchas personas: desde Tito LIVIO[15] *(Eventus stultorum magister est)*, hasta Benjamín FRANKLIN[16] *(Experience keeps a dear School, yet fools will learn in no other)*.

---

[11] XIII Encuentro sobre "Informática y Derecho", Madrid, mayo 1999: "Peritajes en Tecnologías de la Información y Comunicaciones" (Ponencia de Jesús Rivero Laguna); Libro de Actas.

[12] Thomas FULLER (1654–1734): *Gnomología*.

[13] "L'expérience est le total de nos déceptions" *(Moderne et rococo)*.

[14] Autor español de obras teatrales (1662-1709): *El esclavo en grillos de oro*.

[15] *"La experiencia es el maestro de los necios" (Historias)*.

[16] *"Es una escuela muy cara la de la experiencia; sin embargo, los locos no aprenderán en ninguna otra" (Poor Richard's Almanach)*.

26.4. "PERITO" *VERSUS* "ESPECIALISTA"

26.4.1. Quién puede ser "Perito IT"

De modo genérico –conceptual o definitorio–, acabamos de comentar en el apartado precedente qué es un "perito". En una segunda vertiente, estrictamente *jurídica*, podemos leer en el *Diccionario Jurídico* de Julia Infante[17], que: "perito es la persona que informa en un procedimiento, bajo juramento (sobre cuestiones litigiosas relacionadas con su especialidad o experiencia)"; no obstante, se añade que esta persona "posee un título y es especialista en algo determinado".

Si admitimos las precisiones anteriores, nuestra respuesta a la pregunta de qué es un perito y sobre todo a la de quién puede ser, un *Perito IT* –en Tecnologías de la Información–, se concreta sustancialmente:

a) deberán poseer una titulación, en informática o de telecomunicación, entendemos que oficial y de carácter universitario: ingeniero técnico[18] cuando menos, o ingeniero[19], si bien podría admitirse la validez en determinadas peritaciones de otros titulados universitarios en ramas afines; y,

b) deberán, además, ser especialistas en el objeto de la pericia, en tanto que la titulación universitaria en sí misma no es garantía a priori de la competencia técnica necesaria para emitir un dictamen con reconocida autoridad, en un ámbito particular de conocimiento dentro del vasto y dinámico contexto de las tecnologías de la información.

Como en muchos otros ámbitos profesionales, la *praxis* es diferente. Cuántas veces hemos constatado formando parte de "ternas enviadas a Juzgados, para insaculación de sus miembros", que se desconocía el objeto de la pericia hasta ese momento, siendo el común denominador de los peritos propuestos exclusivamente la titulación universitaria que poseíamos, pero no, por tanto, la adecuación de nuestra especialización y en definitiva nuestra capacitación real para emitir el dictamen en cuestión. Los Colegios Profesionales no cuentan habitualmente con recursos administrativos para efectuar una mínima pre-selección de propuestas de candidatos a perito judicial en un determinado procedimiento, ni puede que quizás se lo permitiese el propio colectivo de colegiados: potenciales peritos. No entraremos en este debate, ajeno a nuestra competencia, pero dejaremos constancia de él.

---

[17] Peso Navarro, Emilio del: *Manual de Dictámenes y Peritajes informáticos;* Editorial DÍAZ DE SANTOS: Madrid, 1995 (págs. 13 y ss.).

[18] *Titulación universitaria oficial*, de primer ciclo.

[19] *Titulación universitaria oficial*, de segundo ciclo.

Sin duda, y para nuestra tranquilidad, el *sistema* dispone de sus propias salvaguardas:

- la deontología del propio perito insaculado, o simplemente propuesto, para declararse a sí mismo como "no competente" en dicho procedimiento; y,

- la declaración final que todo perito hará en el momento de firmar su dictamen: "según su leal saber y entender, que le lleva a someter su opinión a otra más cualificada o fundamentada técnicamente".

En una tercera vertiente estrictamente *profesional*, coincidimos en fin con quienes defienden que un **"Perito IT profesional"** es mucho más que un mero técnico competente, por supuesto titulado universitario en alguna rama de las Tecnologías de la Información y con experiencia ("*expertise*") en la materia objeto de la pericia de que se trate en cada momento. Concretamente, la AIPT[20] diferencia entre "perito" y "especialista", según se hace constar en el correspondiente documento de "Solicitud de Ingreso" en la misma[21]: "*el reconocimiento social y el prestigio de las actuaciones profesionales de los Ingenieros de Telecomunicación como Peritos, hacen deseable a juicio de la Agrupación que se satisfaga una doble condición:*

a) Experiencia y formación específica como Perito
b) Dedicación preferencial al Ejercicio Libre de la Profesión".

Con inusual rudeza y absoluta claridad, la Comisión Gestora de la AIPT puso de manifiesto que *"no basta con ser* ***especialista*** *para poder realizar buenos peritajes: o ya se ha adquirido una formación específica como Perito, ejerciendo esta actividad desde hace años, o se deberá adquirir"*. Asimismo, *"recuerda a los interesados en pertenecer a la Agrupación de Ingenieros-Perito que es necesario tener en cuenta las obligaciones de carácter fiscal y laboral que conlleva la realización de trabajos en ejercicio libre"*.

En síntesis, la argumentación de la AIPT es que debe *profesionalizarse* la actuación como Perito con una "dedicación preferencial" a dicha actividad, y que debe acreditarse su *competencia como tal perito* con experiencia acreditada al respecto, que no garantiza en sí misma la titulación universitaria oficial propiamente dicha (Ingeniero de Telecomunicación, en este caso).

En otras palabras, un "Perito IT profesional" no es un *temporero de las actuaciones judiciales*. Con todo respeto a su competencia técnica, estos otros profesionales serían los "*especialistas*" –que no "peritos"–, como distingue

---

[20] *Agrupación de Ingenieros-Peritos de Telecomunicación, del Colegio Oficial de Ingenieros de Telecomunicación.*

[21] COMISIÓN GESTORA DE LA AIPT: *"Actividad profesional libre-ejerciente, como Ingeniero-Perito del COIT"* (Solicitud de Ingreso); COIT: Madrid, 17 de mayo de 1999.

inequívocamente la AIPT: *"se entienden como tales, a aquellos compañeros que son expertos en una determinada materia, pero que carecen de plena disponibilidad de tiempo y desplazamiento en su trabajo principal (no como "libre-ejerciente") o no están interesados en asumir el riesgo de unos costos fijos anuales ocasionados por el alta en el IAE –Impuesto de Actividades Económicas– y el pago mensual como autónomo de la Seguridad Social"*.

En esta línea de selección de "peritos profesionales", encontramos una sólida iniciativa, sin duda fuertemente elitista por criterios de formación y deontología, tal cual es SESPES/Sociedad Española de Peritos Judiciales[22], quien exige a sus asociados:

1. Titulación universitaria oficial de segundo ciclo, como mínimo (el 50% de sus actuales miembros son doctores), en Derecho y/o carreras del ámbito de las TIs (Ingeniería Informática e Ingeniería de Telecomunicación, preferentemente).

2. Formación técnica especializada de postgrado en materia de peritajes, así como en deontología, que haya sido reconocida por la Fundación DINTEL, además de acreditar una adecuada experiencia profesional como Perito.

En concreto, los requisitos exigidos para ser admitido en SESPES, como tal "Perito IT profesional", son:

a) titulación universitaria oficial, de segundo ciclo, en Derecho o Tecnologías de la Información;
b) formación específica de postgrado en materia de peritajes;
c) compromiso de actuación profesional sujeta a códigos deontólogicos; y,
d) experiencia pericial acreditada.

Esta Asociación de Peritos profesionales –SESPES– justifica de hecho sus criterios de selección afirmando que en otras condiciones se estarían ofertando a aquellas Instituciones u Organizaciones que le solicitan sus servicios o colaboración, peritos seudo-profesionales, o sin "garantía de origen", lo que no significa que no puedan dar un adecuado "servicio" esos técnicos, en determinadas ocasiones. Y ello, sin entrar en las consideraciones fiscales y laborales que les exige asimismo la AIPT a sus miembros, según hemos visto en el párrafo anterior.

---

[22] *SESPES*, es la *Sociedad Española de Peritos Judiciales*, creada bajo los auspicios de la Fundación DINTEL, que agrupa a Peritos profesionales en Tecnologías de la Información. Promovida el 17 de abril de 1999 en un Acto Fundacional de diez profesionales (cinco doctores en Derecho y/o Tecnologías de la Información, Patronos de la Fundación DINTEL; y, cinco ex alumnos de su Programa de Alta Formación en Ingeniería Informática). SESPES está reconocida oficialmente –así como sus Estatutos– , e inscrita en el oportuno Registro de Asociaciones con el Nº 165.417 (*"Resolución de la Secretaría General Técnica del Ministerio del Interior"* : Nº 7.639, de 29 de julio de 1999).

26.4.2. Formación de "Peritos IT Profesionales"

Un "Perito IT" no nace: se hace, con formación específica. Efectivamente, hemos dicho que un perito, lo es en tanto a unos conocimientos (titulación) y una experiencia específica en este ámbito profesional. Desgraciadamente, en la Universidad no se incluyen este tipo de materias, ni los colectivos profesionales (hablamos exclusivamente del sector de las Tecnologías de la Información) dedican a este asunto todos los recursos formativos que aparentemente son necesarios. Por el contrario, nos constan algunas iniciativas aisladas en esta dirección, promovidas por la iniciativa privada:

- IEE, en colaboración con GRANADA: "Aula de Informática Legal"[23]; y,
- Fundación DINTEL: "Programa de Alta Formación en Ingeniería Informática" y "Proyecto formativo sobre Ejercicio Profesional y Autoempleo como Perito"[24].

Según SESPES, en el apartado de "formación específica en materia de peritajes", los *peritos profesionales* debieran tener conocimientos de:

a) *Fundamentos jurídicos:* El perito profesional tiene que desenvolverse en un entorno judicial, para lo cual necesita conocer ciertos conceptos jurídicos, vocabulario, etc.

b) *Técnicas de redacción de dictámenes*: El informe pericial es uno de los medios de prueba de que puede hacerse uso en un juicio[25], siendo aconsejable por tanto que sigan un cierto esquema de exposición.

c) *Criterios de minutación de honorarios*: El perito es un profesional libre ejerciente que deberá facturar sus honorarios, con criterios deontológicos desde luego, pero también con conocimiento acerca de cuáles son las tarifas de honorarios recomendadas, sus excepciones y salvedades, etc.

---

[23] "Aula de Informática Legal", organizada por IEE y GRANADA Business Continuity: *Dictámenes y Peritajes Informáticos*; Madrid, abril, 1998.

[24] En ambos casos, el uso del *know-how* de los Proyectos formativos ha sido cedido a la Fundación por el propietario exclusivo de todos sus derechos intelectuales y de explotación (Rivero Laguna, Jesús: *Proyecto formativo de Informes, Dictámenes y Peritaciones, Judiciales y Extrajudiciales;* MINISTERIO DE EDUCACIÓN Y CULTURA: Registro General de la Propiedad Intelectual, Nº 77.211). Los alumnos-peritos que superan el período de formación, basado absolutamente en casos reales, reciben un "Título Oficial de la Fundación DINTEL", avalado por un reputado Claustro de Profesores, todos ellos Profesionales de reconocido prestigio, con acreditada experiencia como Peritos en Tecnologías de la Información.

[25] Así lo establece específicamente el artículo 578 – apartado 5º, en la Sección Quinta de la vigente Ley de Enjuiciamiento Civil de 1881; y, el artículo 299 – apartado 4º, en el Capítulo VI de la Ley de Enjuiciamiento Civil 1/2000, que entrará en vigor al año de su publicación (en el apartado 7 de este capítulo se discutirán estas cuestiones en profundidad).

d) *Protocolos de actuación*: La actuación de un perito puede provenir de una decisión judicial directa, o a instancia de terceras partes; puede requerir obligatoriamente el Visado –previo o diferido– del correspondiente Colegio Profesional; etc.

Además, y en todo caso, un *perito profesional* debe:

- tener unos mínimos conocimientos laborales y fiscales para cumplir con los oportunos mandatos: su desconocimiento en modo alguno le exonera de responsabilidad;
- adquirir una mínima competencia comercial y de marketing, que le permita acceder al mercado laboral, con casos reales en los que poder ejercer su actividad profesional;
- etc.

26.4.3. Conclusión

Las nuevas tecnologías, en particular las *"IT-Information Technologies"* (Tecnologías de la Información), están de moda y son un campo de creciente interés en la presente Sociedad de la Información. Es en este marco tan dinámico e inestable, donde se impone la necesidad de efectuar peritaciones técnicas, aun cuando sus propios agentes (los "técnicos competentes") no las promoviesen. Surge pues, inevitablemente, la necesidad de disponer de *peritos profesionales*, más allá de los meros técnicos competentes.

En todo caso, debe distinguirse al "perito" (como "profesional"), del "*especialista*" (como "experto puntual"), al que no se le exige que posea una formación específica en áreas tales como: fundamentos jurídicos, técnicas de redacción de dictámenes, criterios de minutación de honorarios, etc.

26.5 DIFERENCIACIÓN ENTRE INFORMES, DICTÁMENES Y PERITACIONES

Antes de comentar la diferenciación que establece al respecto alguna Corporación de Derecho Público (COIT, Colegio Oficial de Ingenieros de Telecomunicación, en concreto), precisamente por su incidencia en el cálculo de los honorarios que una determinada actuación profesional provoca, haremos un recorrido por diversos

diccionarios generales con la finalidad de aportar una mayor perspectiva a estos términos, habitualmente identificados como equivalentes por los legos en la materia.

26.5.1 Acerca del término "Informe"

El *Diccionario de la Real Academia Española de la Lengua*[26] define *Informe* de modo genérico, como "noticia o instrucción que se da de un negocio o suceso, o bien acerca de una persona".

Bastantes diccionarios[27] introducen una cierta generalización –no exenta de confusionismo técnico, según aludíamos antes–, al definir *Informe* como "la acción y efecto de informar o *dictaminar*".

Sólo unos pocos aportan la precisión esperada:

- *Diccionario ARISTOS*: "acción de informar o dictaminar *una persona competente*".
- *Gran Enciclopedia LAROUSSE*: "exposición oral o escrita *del estado de una cuestión*".
- *Diccionario General de la Lengua Española VOX*: "Comunicación que *enumera con orden y detalle unos hechos, actividades o datos*, basándose en supuestos ya comprobados (*un informe técnico*)".

También los hay que matizan definiciones[28] en el ámbito del Derecho, asociando el término "Informe" a las "exposiciones orales que hace el fiscal o el letrado ante el tribunal que ha de fallar el proceso". En particular, algunos otros[29] asocian el término "informe" en el ámbito procesal, al contexto de pericial técnica: "diligencia acordada por el juez cuando, para conocer o apreciar algún hecho importante en el juicio, fuese necesaria la *intervención de un especialista con conocimientos científicos o profesionales*".

---

[26] Entre otros, tales como:
- *Diccionario María Moliner*
- *Diccionario Enciclopédico ESPASA*
- *Diccionario Enciclopédico PLAZA & JANÉS*
- etc.

[27] Caso del *Diccionario Enciclopédico ESPASA, LAROUSSE, Diccionario Enciclopédico Universal OCÉANO, Enciclopedia Universal Interactiva CAJA MADRID, Diccionario Enciclopédico ALFA de SALVAT*, etc.

[28] Caso del *LAROUSSE, Diccionario Enciclopédico Universal OCÉANO, Enciclopedia Universal Ilustrada ESPASA-CALPE, Enciclopedia ENCARTA de MICROSOFT*, etc.

[29] Caso de la *Enciclopedia Multimedia PLANETA AGOSTINI, Enciclopedia Universal Interactiva CAJA MADRID, Enciclopedia Universal Interactiva COLLIER*, etc.

26.5.2 Acerca del término "Dictamen"

El *Diccionario de la Real Academia Española de la Lengua*[30] define *Dictamen* de modo genérico, como "opinión o juicio que se forma o emite sobre una cosa".

Bastantes diccionarios matizan:

a) que quien expresa la opinión sobre dicha cosa, es "alguien con autoridad en la materia":

- *Diccionario María Moliner*
- *Diccionario del Español Actual*, de AGUILAR
- etc.

b) que se trata de una "opinión escrita y motivada, suscrita por uno o varios facultativos, sobre un asunto determinado de una especialidad":

- *Diccionario Enciclopédico ESPAÑA*
- *Diccionario Enciclopédico SALVAT*
- *Gran Diccionario de la Lengua Española*
- *Enciclopedia LAROUSSE*, de PLANETA
- etc.

La Enciclopedia *Gran Larousse Universal*, identifica no obstante *dictamen* (pericial), con "informe pericial", insistiendo en que "debe centrarse en cuestiones puramente técnicas, ya que los jueces no pueden delegar su poder decisorio... El *perito* es un mandatario de la justicia, habilitado para proceder a todas las investigaciones exigidas por el cumplimiento de su misión, del *dictamen*". Y añade inequívocamente al discutir la valoración de un *dictamen pericial* que "la apreciación que haga el juez del dictamen es libre, no estando obligado a sujetar su decisión a la opinión pericial; si no lo considera adecuado para fundamentar el fallo judicial deberá, no obstante, señalar los motivos que han dado lugar a su decisión".

El *Diccionario de Derecho Privado* de la Editorial LABOR, añade de su parte que "la ley utiliza la palabra *dictamen* para designar el informe emitido por los peritos durante el periodo de prueba en un proceso".

---

[30] Entre otros muchos, tales como:

- *Diccionario Enciclopédico ESPASA*
- *Gran Enciclopedia LAROUSSE*
- *Diccionario Enciclopédico EDAF*
- *Diccionario Enciclopédico PLAZA & JANÉS*
- *Diccionario ARISTOS*
- etc.

La consulta de diccionarios[31] de sinónimos, antónimos e ideológicos, no aporta mayor luz, al considerar sinónimos términos como informe, opinión y juicio, junto a otros más.

Lo mismo ocurre con las definiciones recogidas en diccionarios[32] de lengua extranjera: *report, opinion* y *judgement*. No obstante, sí puede considerarse relevante la diferenciación que introduce el *Diccionario de Términos Jurídicos* (Inglés-Español / Spanish-English) de Enrique Alcázar Varó y Brian Huges, de Editorial ARIEL, entre:

- *dictamen consultivo:* advisory opinion;
- *dictamen jurídico:* legal opinion (opinion of counsel);
- *dictamen motivado:* reasoned opinion; y,
- ***dictamen pericial:*** expert opinion (expert testimony), como sinónimo de *"peritaje"*.

26.5.3. Definiciones del COIT

Las anteriores similitudes terminológicas entre informe, dictamen y pericial quedan absolutamente deslindadas en los documentos oficiales del COIT, Colegio Oficial de Ingenieros de Telecomunicación, y más concretamente en su ANEXO II de "Fórmulas para Informes, Dictámenes y Peritajes".

Concretamente, entiende por:

- **INFORME**: El desarrollo, con explicaciones técnicas, de las *circunstancias observadas* en el reconocimiento o examen de la cuestión sometida a informe.
- **DICTAMEN**: La *exposición de la opinión* que emite el Ingeniero, sobre la cuestión sometida a dictamen.
- **PERITACIÓN**: El dictamen en que *se disciernen* cuestiones de orden técnico, o se definen circunstancias también del mismo orden.

Hasta tal punto es manifiesta la diferenciación conceptual asociada a los tres términos en cuestión, que el COIT especifica que "los honorarios en los casos de dictamen o peritación (H), serán el doble de los señalados para los informes (H')".

---

[31] *Gran Diccionario de Sinónimos*, de BRUGUERA; *Diccionario manual de Sinónimos y Antónimos*, de VOX; *Diccionario Ideológico de la Lengua Española*, de JULIO CASARES; etc.

[32] Oxford Advanced Learner's , COLLINS dictionary, etc.

Así, aun partiendo[33] de unos "honorarios mínimos" de 55.700 ptas., el COIT recomienda se aplique como fórmula general para cálculo de honorarios de los "Informes":

$$H' = B + 0'03 \times V \times C$$

siendo[34]:

- V = Suma de valores de materiales, mano de obra, amortizaciones, gastos, generales, etc. con la que ha habido que operar;
- B = 5.250 ptas.; y,
- C = Coeficiente reductor por tramos;

pero teniendo en cuenta que, para los "Dictámenes" y "Peritaciones", los honorarios (H) se duplicarán:

$$H = 2 \times H'$$

Esta filosofía de duplicación del valor (H') de los honorarios resultantes de aplicar la fórmula de los "Informes", se mantiene en cualquier otra situación en que no sea válida la fórmula general antes indicada. En concreto, el valor antes indicado de H', se calcularía:

- en el caso de "*Informes sobre Proyectos*", mediante:

  $H' = 0'5 \times B + 0'1 \times P$
  siendo P, los honorarios del *Proyecto;*

- en el caso de "*Informes sobre Obras*", mediante:

  $H' = 0'5 \times B + 0'1 \times O$
  siendo O, los honorarios del Proyecto de las *Obras informadas;*

- en el caso de "*Informes sobre Instalaciones* (máquinas, materiales, etc.)", mediante:

  $H' = 0'5 \times B + 0'1 \times I$
  siendo I, los honorarios del Proyecto de las *Instalaciones informadas;*

---

[33] *Baremos de Honorarios Orientativos para Trabajos Profesionales*, aplicables a los Ingenieros de Telecomunicación, en el Ejercicio Libre de la Profesión.

[34] En el año 2000.

- en el caso de "Informes sobre *Concursos de Proyectos*", mediante:

  $H' = 2 \times B + 0'05 \times C$

  siendo C, los honorarios de los *Proyectos* informados;

- en el caso de "Informes sobre *causas de avería* (en fábricas, instalaciones, maquinarias, artefactos, conducciones, etc.)", mediante:

  $H' = B + 0'05 \times A$

  siendo A, el valor de todas las *pérdidas producidas por la Avería;*

- en el caso de "Informes ante *Tribunales* (en situaciones especiales para las que no existe la tarifa correspondiente)", mediante:

  $H' = 0'5 \times B + 0'05 \times F \times (1+0'1xN)$

  siendo F el importe de la *Fianza* señalada por la autoridad judicial o el importe de la responsabilidad civil subsidiaria que sea objeto de la intervención judicial, y N la suma del número de escritos y comparecencias del ingeniero;

- en el caso de "*Informes sobre Patentes*", mediante:

  $H' = B\ (0'5 + 0'25 \times R)$

  siendo R el número de *Reivindicaciones* objeto del informe.

26.5.4. Tarifas diferenciadas de Honorarios de Ingenieros en Trabajos a particulares

La disquisición de honorarios descrita en el párrafo precedente, no es en realidad una particularidad del COIT. Antes bien, se trata de una adaptación de las Tarifas del COIT, a lo establecido por la Orden de 24 de julio de 1962 (Boletín Oficial del Estado de 31 de julio), por la que se aprueban las normas complementarias de aplicación de las tarifas de honorarios de los Ingenieros en trabajos a particulares, a propuesta del "Instituto de Ingenieros Civiles de España" –actualmente, *Instituto de la Ingeniería de España*–, y de acuerdo con lo establecido en la base general 13 del Anexo del Decreto 1998/1961 de 16 de octubre.

Así, de las 268 Tarifas que integran la Parte III del Anexo[35] al Decreto, dedicada a "Trabajos Especiales", se establece concretamente una *clase* denominada "Informes, dictámenes y peritaciones" (Tarifas 156 a 168, ambas inclusive), correspondiendo:

[35] La Parte I contiene todas las Tarifas de Honorarios relativas a Proyectos, ordenadas en trece "Grupos".

- la Tarifa 168, a la fórmula general;
- la Tarifa 156, a la fórmula largamente comentada de H = 2xH'; y,
- las Tarifas 157 a 160 (ambas inclusive) y la 168 y 166 y 167, a las explícitamente relatadas para cálculo particular de H': proyectos, obras, instalaciones, concursos de proyectos, causas de avería, informes ante Tribunales y patentes, respectivamente.

Inequívocamente, este Anexo al Decreto de Tarifas de Honcrarios de Ingenieros que se ha presentado, distingue pues entre "Informe", "Dictamen" y "Peritación", recogiendo de hecho las mismas definiciones dadas en el párrafo 5.3, en el preámbulo al bloque de Tarifas 156 a 168.

26.6. PERITACIONES EXTRAJUDICIALES Y ARBITRAJES

No profundizaremos aquí en este tema, por razones de espacio, pero no queremos pasar sin dejar constancia de su importancia explícita en el capítulo que tratamos.

El mismo Anexo del Decreto de Tarifas a que hicimos referencia en el apartado precedente, dedica explícitamente su Tarifa 220 a valorar este merester:

$$H' = 5 \times B + 0'05 \times V$$

siendo V la suma de valores con que se ha operado para resolver el arbitraje. En particular se establece que para su realización se supone que se proporcionan al Ingeniero toda clase de datos, y además de lo resultante de aplicar esta tarifa, habrán de abonársele los honorarios de los reconocimientos, informes, valoraciones, etc. que efectúe.

De los dos tipos básicos de arbitraje que existen –de *equidad* y de *derecho*–, sólo en el *de equidad* cabe pensar en principio que un técnico actúe como *árbitro*[36], ya que en este caso puede serlo cualquier persona natural que se elija para decidir sobre la cuestión litigiosa, según su leal saber y entender y sin sujeción a trámites, debiendo tan sólo dar la oportunidad a las partes para ser oídas y presentar las pruebas que estimen convenientes. Ello no impide que, en cualquiera de los casos, se requiera un informe, dictamen o pericial extrajudicial por las partes, a quienes asimismo corresponde la elección del tipo de arbitraje que desean[37].

[36] En el caso del "arbitraje de derecho" los árbitros deciden la cuestión litigiosa con sujeción a derecho, por lo que deberán ser letrados en ejercicio.

[37] En caso de que no hayan manifestado su voluntad en este aspecto, el arbitraje será de equidad.

El arbitraje, en tanto que sistema de resolución alternativa de conflictos, aporta múltiples ventajas: rapidez[38], discreción y confidencialidad, flexibilidad en el procedimiento y lugar de celebración, reducción de costas, voluntariedad en la fórmula de solución al litigio, eficacia, etc.

En particular, y totalmente en la línea que nos ocupa, cabe destacar como una notable ventaja el hecho de que las partes pueden escoger como árbitros ("de equidad") a personas que sean especialistas en la materia, ya sea por su profesión, cargo o actividad; no se olvide que serán estas personas, al actuar como árbitros, quienes tomarán la decisión que estimen más justa en conciencia, y que una vez sea firme el *laudo arbitral* dictado éste podrá ser objeto de ejecución forzosa, al igual que una "sentencia judicial firme".

Distinta es la fórmula de la "mediación", que se diferencia de la del arbitraje en que el mediador no tiene carácter de juez, sino de "hombre bueno" cuyo consejo puede ser aceptado o rechazado libremente.

En conclusión, según recoge la *Enciclopedia Gran Larousse Universal*: "Socialmente pues, el confiar la solución de conflictos al juicio-resolución de árbitros, significa la existencia de una comunidad sana y únicamente madura en la que los problemas interpersonales no alcanzan grados de continua agudización, y por el contrario se han conseguido en su seno altos niveles de convivencia."

En mayo de 1989, unos meses después de la entrada en vigor de la Ley de Arbitraje Española, se constituyó en nuestro país *ARBITEC*[39], con la finalidad de ofrecer una vía alternativa eficaz para la resolución de divergencias que tengan como fondo productos o servicios relacionados con las Tecnologías de la Información. En febrero de 1997 se convirtió en la primera institución española que admite soluciones de arbitraje a través de Internet, utilizando la *red* en todas las fases del procedimiento arbitral, excepto en aquellas diligencias en las que se requiere presencia de las partes[40].

---

[38] Existen, incluso, los denominados "arbitrajes acelerados", en los que se introducen ciertas modificaciones para garantizar que se pueda realizar en menor tiempo y con costos más reducidos aún.

[39] La imparcialidad de *ARBITEC –Asociación Española de Arbitraje Tecnológico–*, queda garantizada por el hecho de que la Comisión encargada de elegir a los árbitros está formada por un representante de la oferta y otro de la demanda:

a) el sector de las empresas suministradoras de Tecnologías de la Información, está representado por SEDISI; y,

b) los usuarios, están representados por la Asociación de Usuarios de Internet.

Los dos vocales garantizan la tutela de los derechos de las partes en el momento de la designación de peritos para el procedimiento arbitral.

[40] Para someterse al arbitraje ARBITEC, podrá tramitarse la solicitud, por ejemplo, a través del correspondiente formulario electrónico en la web: http://www.onnet.es/arbitec.

Además de ARBITEC, y desde luego de la *Corte Española de Arbitraje*, existe en nuestro país otra interesante organización: *ARyME, Arbitraje y Mediación*[41], única empresa privada española dedicada a promover e impulsar el arbitraje y la mediación como alternativas al procedimiento judicial ordinario, así como de administrar los asuntos que le son encargados.

26.7. EL DICTAMEN DE PERITOS COMO MEDIO DE PRUEBA

La versión actualmente vigente de la *LEC-Ley de Enjuiciamiento Civil* de 1881 –Real Decreto de 3 de febrero–, también llamada "Ley de Trámites Civiles", establece en su *Artículo 578 (Sección QUINTA, De los medios de prueba)*, que:

"Los medios de prueba de que se podrá hacer uso en juicio son:

1. Confesión de juicio
2. Documentos públicos y solemnes
3. Documentos privados y correspondencia
4. Los libros de los comerciantes que se lleven con las formalidades prevenidas en la Sección Segunda, Título II, Libro I
5. **Dictamen de Peritos**
6. Reconocimiento judicial
7. Testigos."

Debe hacerse notar que el artículo siguiente de la vigente LEC (el 579), no hace referencia alguna a las "Pruebas", entrando de lleno en la descripción de la "Confesión Judicial". No ocurre así, en la LEC – Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (todavía no vigente):

- se dedican dos artículos a los "Medios de Prueba" (Capítulo VI. *De los medios de prueba y las presunciones*), en el Título I (*De las disposiciones comunes a los procesos declarativos*) del Libro II (*De los procesos declarativos*):
  - *Art. 299. Medios de prueba*
  - *Art. 300. Orden de práctica de los medios de prueba*
- se modifican tanto las denominaciones de los medios de prueba, como el orden en que se podrá hacer uso de los mismos (*Art. 299*):
  1. Interrogatorio de las partes
  2. Documentos públicos
  3. Documentos privados

[41] ARyME, constituida a finales de 1996, ha desarrollado tanto un reglamento de arbitraje como un procedimiento de mediación, para desarrollar su trabajo.

4. **Dictamen de Peritos**
5. Reconocimiento judicial
6. Interrogatorio de testigos

- se precisa el orden de práctica de los medios de prueba (Art. 300), "salvo que el tribunal, de oficio o a instancia de parte, acuerde otro distinto":

1. Interrogatorio de las partes
2. Interrogatorio de los testigos
3. *Declaraciones de peritos sobre sus dictámenes o presentación de éstos, cuando excepcionalmente se hayan de admitir en ese momento*
4. Reconocimiento judicial
5. Reproducción[42] ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes.

26.7.1. Objeto de la "prueba pericial"

En todo caso, e independientemente de la versión considerada de LEC, el "objeto principal de la *prueba* son los hechos; más exactamente, las afirmaciones fácticas del proceso"[43]. O, si se prefiere, entendemos por *prueba*[44]: "la actividad que desarrollan las partes con el tribunal para adquirir el convencimiento de la verdad o certeza de un hecho o afirmación fáctica o para fijarlos como ciertos a los efectos de un proceso. Esta actividad se realiza tanto en procedimientos civiles como penales, sociales y contencioso-administrativos; siendo lo regulado para el procedimiento civil la norma básica que se aplica a todos los procedimientos".

Ahora bien, no todos los "hechos" son objeto de *prueba pericial*. Tal sería el caso de aquellos que no necesitan ser probados por considerarse notorios, o porque sean admitidos al no resultar controvertidos, además de determinadas presunciones.

De modo genérico, puede distinguirse entre "hechos fundamentales" y "hechos accesorios o indiciarios", en función de su correspondencia directa –o no– con lo que se trata de resolver en el proceso en cuestión.

Por otra parte, y aunque lo habitual es que sean las *partes* (actora y demandada) quienes propongan la *prueba*, bien puede ocurrir que sea el propio Juez o la Sala que conoce del litigio quien decida la necesidad de una prueba pericial, antes de dictar

---

[42] El artículo 299.2 de la LEC de enero de 2000, establece que "también se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso".

[43] Muñoz Martínez, Félix J., *Introducción al ámbito jurídico*, Ed. Fundación DINTEL: *Programa de Alta Formación en Ingeniería Informática* – Curso de "Informes, Dictámenes y Peritajes en Tecnologías de la Información", Madrid, abril 1999.

[44] Muñoz Martínez, Félix J., *Op. cit.*

sentencia; de ahí que se denomine a este tipo de pruebas periciales como "diligencias para mejor proveer".

26.7.2. El "Dictamen de Peritos" en la vigente LEC

La vigente LEC de 1881, dedica a este asunto los artículos 610 a 632, ambos inclusive.

Desde una perspectiva conceptual, orientada al ámbito técnico, según corresponde al contenido de esta obra, entendemos como significativos para nuestros fines los siguientes aspectos que comentamos:

- La prueba pericial procede emplearse cuando se dan dos circunstancias concretas (Art. 610):

  a) se necesitan, o son convenientes, conocimientos científicos, artísticos o prácticos; y,
  b) se persigue conocer o apreciar "hechos de influencia en el pleito".

- El objeto de la prueba pericial debe proponerse con claridad y precisión[45], por la parte a quien interese este medio de prueba (Art. 611).

- Los peritos, en número de uno o tres (Art. 611), "deberán tener título de tales en la ciencia o arte a que pertenezca el punto sobre el que han de dar su dictamen, si su profesión está reglamentada por las leyes o por el Gobierno" (Art. 615).

- La admisión de una Solicitud de prueba pericial, y desde luego su objeto definitivo, sólo corresponde al Juez (Art. 613), independientemente de la propuesta de las partes. Lo mismo ocurre con la valoración del dictamen emitido por el Perito (Art. 632), ya que "los Jueces y los Tribunales apreciarán la prueba pericial según las reglas de la sana crítica sin estar obligados a sujetarse al dictamen de los peritos".

- El Juez podrá pedir informe a la Academia, Colegio o Corporación Oficial que corresponda, cuando el dictamen pericial exija operaciones o conocimientos científicos especiales (Art. 631).

---

[45] Es por ello que, en base a su experiencia profesional, este autor ha propuesto en múltiples foros que el letrado forme *team* (equipo) con el perito ("experto" en la materia, como tal técnico en la misma):
- XIII Encuentro de "Informática y Derecho" (Universidad Pontificia Comillas / Instituto de Informática Jurídica): Madrid, 7 y 8 abril 1999;
- *Revista de Informática para Juristas* de Editorial ARANZADI: Nº 31, abril de 1999;
- etc.

26.7.3. El "Dictamen de Peritos" en la LEC, de enero de 2000

La LEC de 7 de enero de 2000, dedica a este asunto los artículos 335 a 352, ambos inclusive, constitutivos de la Sección 5ª del Capítulo VI del Título I del Libro II de la Ley. La redacción del articulado presenta en sí misma apreciables diferencias.

Con respecto al "objeto y finalidad del dictamen de peritos" (Art. 335) la nueva Ley coincide en lo sustancial con la vigente. Se insiste explícitamente, además, en que al emitir el dictamen, todo perito:

a) deberá manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible;

b) tomará en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes; y,

c) conocerá las sanciones penales en las que podría incurrir si incumpliere su deber como perito.

Ambas leyes siguen coincidiendo en lo sustancial, en cuestiones tales como:

- *Condiciones de los peritos (Art. 340)*

  Los peritos deberán poseer[46] el título oficial que corresponde a la materia objeto del dictamen y a la naturaleza de éste. Asimismo, podrá solicitarse dictamen de Academias e instituciones culturales y científicas que se ocupen de las materias correspondientes al objeto de la pericia[47].

- *Valoración del dictamen pericial (Art. 348)*

  El tribunal valorará los dictámenes periciales según las reglas de la sana crítica.

Ahora bien, la nueva LEC, introduce en el apartado de dictamen de los peritos novedades importantes: artículos 336 a 339. Así, se especifica en los artículos 336 y 337, que:

---

[46] Cuando se trate de materias que no estén comprendidas en títulos profesionales oficiales, los peritos habrán de ser nombrados entre personas entendidas en aquellas materias (*Art. 340.1*).

[47] También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello (*Art. 340.2*).

1. Los litigantes podrán aportar los dictámenes[48] que dispongan (elaborados por peritos por ellos designados), y que estimen necesarios o convenientes para la defensa de sus derechos (Art. 336).

2. Podrán aportarse dictámenes elaborados por peritos designados por las partes, con posterioridad a la demanda o contestación, anunciando oportunamente que lo harán en cuanto dispongan de ellos[49], para su traslado a la otra parte (Art. 337).

Desde luego, y pese a lo dispuesto en el artículo 337, las partes podrán aportar aquellos "dictámenes cuya necesidad o utilidad venga suscitada por la contestación a la demanda o por lo alegado y pretendido en la audiencia previa al juicio" (Art. 338). Es decir, se contempla también la posibilidad de aportación de dictámenes en función de actuaciones procesales posteriores a la demanda.

Por último, en el artículo 339 se contemplan:

- la solicitud de designación de peritos por el tribunal (y resolución judicial sobre dicha solicitud); y,

- la designación de peritos por el tribunal, sin instancia de parte.

Cuestiones relevantes son:

- si cualquiera de las partes fuese titular del derecho de asistencia jurídica gratuita, no tendrá que aportar el dictamen pericial con la demanda o la contestación, sino simplemente anunciarlo, a los efectos de que se proceda a la designación judicial de perito (Art. 339.1);

- la designación judicial de perito puede ser siempre solicitada en sus respectivos escritos iniciales, tanto por el demandante como por el demandado, "si entienden conveniente o necesario para sus intereses la emisión de informe pericial" (Art. 339.2); y,

- la emisión de un informe pericial elaborado por perito designado judicialmente se podrá solicitar con posterioridad a la demanda o a la contestación, "salvo que se refiera a alegaciones o pretensiones no contenidas en la demanda" (Art. 339.2).

---

[48] Los dictámenes se formularán por escrito, acompañados, en su caso, de los demás documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de la pericia (*Art. 336.2*).

[49] En todo caso, antes de iniciarse la audiencia previa al juicio ordinario o antes de la vista en el verbal (*Art. 337.1*).

Asimismo, consideramos significativo lo dispuesto en el *Artículo 345*, acerca de las "operaciones periciales y posible intervención de las partes en ellas":

- las partes y sus defensores podrán presenciar el reconocimiento de lugares, objetos o personas o la realización de operación análogas, si con ello no se impide o estorba la labor del perito y se puede garantizar el acierto o imparcialidad del dictamen (Art. 345.1); y,

- el perito deberá dar aviso directamente a las partes, del día, hora y lugar en que llevarán a cabo sus operaciones periciales, siempre que el tribunal haya aceptado la solicitud de aquéllas para estar presente (Art. 345.2).

26.7.4. Comentarios finales

La LEC, de 7 de enero de 2000, no entrará en vigor hasta un año después de su publicación en el Boletín Oficial del Estado[50], por lo que pudieran todavía introducirse ciertos cambios, si bien no es ello lo que cabe esperar, concretamente en lo que a nuestra parcela de interés compete.

Las novedades que han sido comentadas introducen aportaciones sustanciales con relación a la todavía vigente LEC de 1881. Deberíamos reflexionar pues sobre ellas, como un cercano futurible, además de muy posible en cuanto a su aplicación y obligatoriedad.

26.8. CONCLUSIONES

Peritar no es *Auditar*, ciertamente, al igual que tienen ámbitos de actuación profesional separados y bien definidos los consultores y los auditores. Puede en todo caso contextualizarse la "Peritación" como un ámbito profesional afín al de la "Consultoría" y la "Auditoría", con sus obligadas diferenciaciones en cuanto a elementos conceptuales comunes, tales como: contenido, condición o carácter del contenido, característica temporal, justificación o base que sustenta el contenido, objeto o elemento sobre el que se aplica la justificación, y finalidad o producto deseado y esperado tras la actuación profesional propiamente dicha.

Conceptualmente, son absolutamente equivalentes los "expertos" y los "peritos", si bien nada tienen que ver aquéllos con los "especialistas", cuando se valoran componentes de dedicación profesional con carácter preferencial. Cuestiones determinantes son la formación específica, el *back-ground* profesional, la actitud y la conducta ética en estos ámbitos, etc., además de su entorno y salvoconducto laboral

[50] Disposición final vigésimo primera de la Ley.

(licencia fiscal, cuotas e impuestos *ad-hoc*, etc.). Importante es, asimismo, la adquisición de "*expertise*".

Suelen identificarse, inapropiadamente, términos perfectamente diferenciados tales como "informe", "dictamen" y "peritación". No obstante, existen incluso tarifas oficiales de honorarios recomendados por las Corporaciones de Derecho Público, distintas para la realización de cada uno de estos tres tipos de trabajos a particulares, de los ingenieros en el marco del ejercicio libre profesional.

Las peritaciones no son sólo judiciales, sino que también pueden tener un carácter extrajudicial. Los arbitrajes, e incluso las "mediaciones", cobran fuerza cada día más, existiendo instituciones públicas y privadas que se ocupan de favorecer este tipo de salidas para la resolución de litigios entre las partes en desacuerdo. La firma del "perito profesional" se ubica con determinación en este nuevo contexto jurídico-social.

Tanto la vigente LEC / Ley de Enjuiciamiento Civil de 1881, como la LEC de 7 de enero de 2000 que entrará en vigor un año después de su publicación en el Boletín Oficial del Estado, reconocen explícitamente el "dictamen pericial" como uno de los medios de prueba. Su correcto planteamiento y uso, y la maestría en su redacción y defensa, pueden ser claves para la resolución judicial, aun cuando se valore por el tribunal "según las reglas de la sana crítica".

26.9. LECTURAS RECOMENDADAS

Peso Navarro, E.; *et al.*, *Manual de Dictámenes y Peritajes Informáticos*, Ed. Díaz de Santos, Madrid, 1995.

Fundación DINTEL (diversos autores), *Ejercicio Profesional y Autoempleo, como Perito, en Multimedia y Comunicaciones*, Proyecto Formativo, en colaboración con la Comunidad de Madrid y la Unión Europea: Manual del Alumno (Curso de 208 horas lectivas), Madrid, octubre 1999 (1ª Edición), y febrero 2000 (2ª Edición).

Fundación DINTEL (diversos autores), *Ejercicio Profesional y Autoempleo, como Perito, en Informática*, Proyecto Formativo, en colaboración con la Comunidad de Madrid y la Unión Europea: Manual del Alumno (Curso de 208 horas lectivas), Madrid, febrero 2000.

Fundación DINTEL (diversos autores), *Perito en Prevención de Riesgos Laborales Informáticos*, Proyecto Formativo, en colaboración con la Comunidad de Madrid y la Unión Europea: Manual del Alumno (Curso de 208 horas lectivas), Madrid, febrero 2000.

Rivero Laguna, J.; *et al.*: *Informes, Dictámenes y Peritaciones*; Ed. Fundación DINTEL: Serie "Monografías y Publicaciones", Colección "Peritaciones IT Profesionales"; Madrid, julio 2000.

Rivero Laguna, J.: *Peritajes en Tecnologías de la Información y Comunicaciones*; XIII Encuentro sobre "Informática y Derecho": 7 y 8 mayo, 1999; Universidad Pontificia Comillas / Instituto de Informática Jurídica, Actas del Encuentro.

Rivero Laguna, J.: "Procesos judiciales, arbitrajes y peritos profesionales, en Tecnologías de la Información"; Ed. ARANZADI: Rev. *Actualidad Informática Avanzada*, nº 31 (abril, 1999), páginas 10 y ss.

Verdera y Tuells, E.: *Algunas consideraciones en torno al arbitraje comercial*; Ed. CIVITAS.

Roca Aymar, J. L.: *El arbitraje en la contratación internacional*; Ed. ESIC & ICEX, Madrid, 1994.

26.10. CUESTIONES DE REPASO

1. Diferencie "consultoría" de "auditoría" y "peritación", a partir de la base que justifica su contenido conceptual y el producto final deseado.

2. Indique el contenido que define el ámbito de actuación profesional de un perito frente al de un auditor, e incluso al de un consultor.

3. Exprese tres acepciones diferentes para el concepto de "Perito".

4. Enumere diversas categorías y áreas de peritaje forense privado.

5. Cite aquellas áreas de formación específica que debiera tener un "perito profesional", frente a las actuaciones puntuales de un mero técnico competente o "especialista", en el ámbito del ejercicio profesional como tal.

6. Distinga entre informe, dictamen y peritación, en particular indicando la fórmula para calcular el valor de los honorarios que se aplicaría en cada caso, en una situación genérica.

7. Indique algunas fórmulas concretas para el cálculo de honorarios recomendados de "Informes técnicos", para su aplicación en el caso de trabajos de ingenieros a particulares.

8. Defina los dos tipos básicos de arbitraje entre los que pueden optar las partes para dirimir cuestiones litigiosas que les afectan.

9. Diferencie conceptualmente las figuras de "árbitro" y "mediador".

10. Enumere los medios de prueba establecidos en la vigente LEC / Ley de Enjuiciamiento Civil y las modificaciones introducidas al respecto por la LEC de enero de 2000, tanto en cuanto a denominación como en cuanto a orden de práctica de los mismos.

CAPÍTULO 27

EL CONTRATO DE AUDITORÍA

Isabel Davara Fernández de Marcos

27.1. INTRODUCCIÓN

A pesar de que nuestro análisis se centra en el contrato de auditoría, antes de comenzar con ello creemos conveniente intentar delimitar en esta introducción el concepto de Auditoría Informática. Para ello, empezaremos presentando varias definiciones doctrinales altamente reconocidas, luego pasaremos a plantear una ineludible comparativa con la Auditoría de Cuentas, esquema comparativo que se seguirá a lo largo del trabajo por ser la más próxima, aun con sus importantes diferencias, referencia legal disponible, y terminaremos este apartado introductorio con algunas notas sobre las funciones y fases de esta auditoría de los sistemas de información.

Una vez concretado en lo posible el ámbito de actuación de la Auditoría Informática, nos permitiremos una breve aproximación a la naturaleza jurídica del contrato analizado, y finalmente pasaremos a estudiar la figura contractual que constituye el marco legal en que se desarrolla esta actividad y que es el objeto de este trabajo. Para lograr este objetivo principal, y dado que en la definición de la figura jurídica en que consiste todo contrato como acuerdo de voluntades, hay que delimitar en todo caso tres elementos esenciales: consentimiento, objeto y causa (art. 1261 Código Civil), nuestro estudio seguirá esta estructura determinada legalmente. En cuanto al consentimiento, centraremos su estudio en el análisis de las partes intervinientes como prestadoras de dicho consentimiento, haciendo una especial

referencia al perfil del auditor informático, a su responsabilidad y a su pertenencia o no a la organización auditada. Con relación al objeto del contrato diferenciaremos las distintas áreas susceptibles de ser sometidas a la revisión y juicio de la auditoría. Finalmente, examinaremos las causas de la contratación de una auditoría y su posible obligatoriedad.

La Auditoría Informática "comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y análisis de los riesgos relacionados con la informática"[1].

La Information Systems Audit and Control Association (ISACA) define a la Auditoría de los Sistemas de Información como "cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o alguna sección/área) de los sistemas automatizados de procesamiento de información, incluyendo procedimientos relacionados no automáticos, y las interrelaciones entre ellos". Sus objetivos deben ser brindar a la Dirección una seguridad razonable de que los controles se cumplen, fundamentar los riesgos resultantes donde existan debilidades significativas.

Ya que no tenemos una definición legal de la Auditoría Informática, recurriremos, una vez más, a la de la Auditoría de Cuentas e intentaremos hacer un paralelismo entre sus elementos.

En España, la normativa en materia de Auditoría de Cuentas se circunscribe a: la Ley 19/1988 de Auditoría de Cuentas (LAC), de 12 de julio, el Real Decreto 1636/1990, de 20 de diciembre, por el que se aprueba el Reglamento de la Auditoría de Cuentas que desarrolla la LAC, las Normas Técnicas de Auditoría (NTA), y demás referencias dispersas en otras disposiciones de difcrente rango como pueden ser el Código de Comercio, la Ley de Sociedades de Responsabilidad Limitada, el Reglamento del Registro Mercantil, y, las consultas publicadas por el ICAC. En el ámbito comunitario europeo, en la actualidad el marco legal europeo en materia de auditoría se ciñe a la Octava Directiva (regula el ejercicio profesional), a la Cuarta Directiva y a las Normas Técnicas de Auditoría nacionales.

Así, el Reglamento de la Auditoría de Cuentas dispone en su artículo 1:

1. *Se entenderá por auditoría de cuentas la actividad, realizada por una persona cualificada e independiente, consistente en analizar, mediante la utilización de las técnicas de revisión y verificación idóneas, la información económico-financiera deducida de los documentos contables examinados, y que tiene*

[1] Ramos González, M. Á., "La auditoría informática", en *Actualidad Informática Aranzadi*, nº 14, enero de 1995, páginas 1 y ss.

como objeto la emisión de un informe dirigido a poner de manifiesto su opinión responsable sobre la fiabilidad de la citada información, a fin de que se pueda conocer y valorar dicha información por terceros.

2. *La actividad de auditoría de cuentas tendrá necesariamente que ser realizada por un auditor de cuentas, mediante la emisión del correspondiente informe y con sujeción a los requisitos y formalidades establecidos en la Ley 19/1988, de 12 de julio, en el presente Reglamento y en las normas técnicas de auditoría.*

En definitiva, pasando a estructurar comparativamente las definiciones:

	AUDITORÍA DE CUENTAS	AUDITORÍA INFORMÁTICA
Auditor	Cualificada = Auditor de cuentas Independiente	No existe titulación oficial ni Registro independiente
Función	Analizar: Información económico-financiera Deducida de documentos contables	Analizar información entornos informáticos deducida revisión y control de los mismos
Informe	Emitir informe Manifestando su opinión Responsable Sobre la fiabilidad de la información para que se conozca y valore por terceros	Emitir informe manifestando su opinón responsable sobre la fiabilidad de la información para que se conozca y valore por terceros
Reglamentación	sujeto a requisitos formalidades ley reglamento NTA	sujeto a requisitos formalidades normas de la profesión códigos de conducta de la profesión

En donde existen las principales divergencias entre las dos definiciones es, de un lado, en la inexistencia de una titulación oficial de la profesión de Auditoría Informática y, de otro lado, en la inexistencia de reglamentación específica de esta actividad.

En cuanto al primer aspecto relativo a la titulación, las ventajas de una titulación oficial son evidentes: se obtiene un consenso en la actuación, se establece una metodología común, se dispone de normas técnicas actualizadas por los propios profesionales, se establecen una serie de criterios de responsabilidad coherentes, se dota a la profesión de prestigio, y se impone la exigencia de actualización[2].

[2] Tourifio, Marina, Conferencia de apertura en el Seminario de Auditoría de los Sistemas de Información y Control Interno (AUDISI'2000), organizado por Informáticos Europeos Expertos, Madrid, febrero 2000.

En cuanto a la regulación y normas existentes, en la actualidad la Organización de Auditoría Informática (OAI), capítulo español de la ISACA, tiene tanto unas normas técnicas como un Código de Ética profesional. Entre las primeras destacan los Estatutos de Auditoría, la Independencia profesional, la Educación Profesional Continua, la Preparación del informe... En el segundo, se impone el cumplimiento de las normas de la Asociación, servir al beneficio de empleadores, accionistas, clientes y público en general, desempeñar las labores independiente y objetivamente, obtener y documentar suficiente material basado en hechos reales, informar a las partes apropiadas, mantener valores morales en la conducta y el carácter. A través de la OAI se puede obtener el certificado CISA, Certified Information Systems Auditor, de la ISACA.

De acuerdo con la reconocida doctrina que opta por seguir ur concepto amplio de la Auditoría Informática para evitar que se reduzca a un control de los aspectos informáticos de los sistemas de información, los objetivos de la misma pueden clasificarse en tres grandes grupos:

a) Colaboración con la Auditoría de Cuentas.
b) Auditoría de los propios sistemas informáticos.
c) Colaboración del jurista en la Auditoría jurídica de los entornos informáticos[3].

La utilización de la auditoría informática en la primera de sas vertientes, dentro de la auditoría de cuentas, se debe, principalmente, a la necesidad de ajuste en la especificación de los riesgos del negocio. Sin embargo, la auditoría informática es mucho más que eso, y se ocupa de distintos y amplios temas como el análisis estratégico de los sistemas implantados, su adecuación al negocio (actual y futuro), el tiempo de respuesta, la capacidad de la organización de responder a cambios e implantar soluciones a medida, etc. Entre las razones que explican la evolución de la auditoría informática destacan la dependencia de la informática por parte de cualquier entidad, los riesgos novedosos referentes a la informática, el cambio en la concienciación del empresario, el uso de los datos de carácter personal de forma automatizada, la seguridad en todas sus facetas...[4]. Y, en concreto, dentro del denominado riesgo de control se ha introducido un nuevo elemento de vital importancia y al que bien pudiera dársele categoría de elemento individual: la tecnología de la información, y que ha dado lugar a la utilización de la informática en los sistemas contables, que a través de la tecnología de la información, cada vez más sofisticada, ha propiciado sistemas de información que incorporan nuevos riesgos, peculiares y específicos que dan origen a la consultoría y auditoría informática[5].

---

[3] Del Peso, E., "La auditoría jurídica de la cosa informática", Conferencia pronunciada en el VI Congreso Iberoamericano de Derecho e Informática, páginas 545 y ss.

[4] Lane, David A., "La auditoría informática y su evolución", en *Partida Doble*, nº 95, diciembre 1998, páginas 76 y ss.

[5] Hernández García, A., "La cuantificación del riesgo en auditoría", en *Partida Doble*, nº 88, abril 1998, páginas 73 y ss.

La utilización de sistemas expertos en auditoría es, por lo tanto, un tema distinto que consiste en introducir el uso de la herramienta en la función de auditoría tradicional. No obstante, a pesar de que no se puede reducir el objeto de la auditoría informática a la auditoría realizada con computador o con herramientas informáticas, comporta ciertas ventajas hoy en día de todo punto imprescindibles: conserva el conocimiento experto de los auditores dentro de la empresa, aumenta la capacidad de los expertos para manejar grandes volúmenes de datos y realizar análisis complejos, asesora en la toma de decisiones, permite una comprensión más profunda del conocimiento de los expertos, perfecciona la productividad del personal, aumenta los servicios ofrecidos por las empresas de auditoría, y funciona como herramienta pedagógica y de formación del personal para transmitir el conocimiento de los auditores expertos a los nuevos.

En cuanto a las fases en que se puede descomponer un proceso de decisión en auditoría, una propuesta de esquema podría ser la siguiente[6]:

1. *Orientación*: el auditor obtiene conocimientos sobre las operaciones del cliente y su entorno y hace una valoración preliminar del riesgo y de la importancia relativa.
2. *Evaluación* preliminar de los controles internos.
3. *Planificación táctica* de la auditoría.
4. *Elección de un plan* para la auditoría.
5. *Prueba de cumplimiento* de los controles.
6. *Evaluación* de los controles internos basada en los resultados de las pruebas de cumplimiento.
7. *Revisión del plan* de auditoría preliminar.
8. *Elección de un plan revisado* para la auditoría.
9. *Realización de pruebas sustantivas.*
10. *Evaluación y agregación* de los resultados.
11. *Evaluación de la evidencia.* Podría dar lugar a unas pruebas más exhaustivas o formar la base de la elección de la opinión por el auditor.
12. *Elección de una opinión* que clasifique los estados financieros del cliente.
13. *Informe* de auditoría.

Para terminar con este apartado, una breve referencia a la debatida opción entre auditoría interna y externa, con relación a la problemática de la independencia, el mejor conocimiento de la organización en su conjunto y el necesario y constante mantenimiento y supervisión en razón del peculiar objeto de la auditoría informática.

La independencia es una característica esencial en la auditoría. Constituye un requisito nuclear sin cuya presencia se vicia todo el recorrido posterior. Por lo tanto, partiendo de esta premisa, el aseguramiento de la independencia es una exigencia

[6] Sánchez Tomás, Antonio, Sistemas expertos en auditoría, en *Técnica Contable*, volumen 45, 1993, páginas 529 y ss.

obligada, no siendo éste el lugar, en nuestra opinión, para profundizar en disquisiciones más o menos improductivas acerca de la mayor independencia a priori de la auditoría externa frente a la interna y viceversa. La independencia tiene que existir y ser manifiesta y constatable en el caso concreto.

De todas formas, no conviene olvidar que en el caso específico de la auditoría de los sistemas de información, donde se presentan las peculiaridades es principalmente en la especificidad del objeto de la auditoría en sí, lo que hace que sea imprescindible un conocimiento intenso de los sistemas de información y del flujo de la información en la empresa en cuestión. Y ésta es una de las principales razones que apoyan en esta materia la constitución de un departamento de control interno de los sistemas de información de manera institucionalizada en la organización en cuestión. Todo ello sin perjuicio de la recomendable compatibilidad de ambas opciones aunque sea de forma esporádica en función de la tan intocable eficiencia en los costes.

En todo caso, se opte por la alternativa que se opte, antes de encargar al exterior un trabajo de esta naturaleza se ha debido realizar un esfuerzo interno considerable, y se deben tener censadas las discrepancias, así como las diferentes alternativas en caso de litigio[7].

27.2. UNA BREVE REFERENCIA A LA NATURALEZA JURÍDICA DEL CONTRATO DE AUDITORÍA

Conviene empezar por asentar la casi total aceptación por parte de la doctrina del carácter contractual del vínculo que se establece entre la sociedad y el auditor, frente a las escasas discrepancias que abogan por una tesis "organicista". La calificación de contractual se apoya fundamentalmente en tres razones. En primer lugar lo establecido expresamente por el artículo 14.2 de la Ley de Auditoría de Cuentas que se refiere al "contrato de auditoría". En segundo lugar, la Ley de Sociedades Anónimas que deliberadamente excluye esta materia del capítulo de órganos sociales. Y, finalmente, porque su calificación como órgano sería insertar al auditor dentro de la estructura de la sociedad y considerarlo como parte integrante de la persona jurídica, lo que resulta contrario al espíritu de la ley que lo configura como una "instancia externa e independiente de control"[8].

Además de la dificultad añadida que supone la inexistencia legal de la figura de la auditoría informática, tampoco en la tradicional comparación analógica con la auditoría de cuentas existe unanimidad doctrinal en lo que a su naturaleza jurídica se refiere.

---

[7] Rincón, Emilio, "Aula Financiera: La Auditoría Informática: mito y realidad", en *Estrategia Financiera*, nº 62, abril 1991, páginas 26 y ss.

[8] Menéndez Menéndez, A., "El contrato de auditoría y la terminación unilateral del mismo por el auditor", en *Revista Crítica de Derecho Inmobiliario*, nº 622, Mayo-junio 1994, páginas 1485 y ss.

Sin pretender realizar una investigación exhaustiva de los posibles encuadres conceptuales de la figura, mencionaremos únicamente la divergencia doctrinal existente en cuanto a su concepción como un arrendamiento de servicios, aludiendo a la profesionalidad de la figura, o como un arrendamiento de obra, aludiendo a la ineludible necesidad de la materialización del contrato en el informe de auditoría que constituye el resultado que caracteriza al contrato como un arrendamiento de estas características.

Nuestra opinión se decanta por la figura de un contrato de arrendamiento de servicios, servicios que se desarrollan a lo largo de un periodo temporal determinado, y que, si bien se concretan en la emisión de un informe de auditoría, la libertad del auditor y la falta de capacidad de decisión del auditado sobre los contenidos de dicho informe le privan de la caracterización del resultado esperado a dicho contrato y le confieren una naturaleza de prestación de servicios cuyo resultado no se puede, por lo menos en gran medida, prever, o, mejor dicho, cuyo resultado, en cuanto a inclusión de contenidos, no se puede pactar.

Estas características se pueden contrastar en varios lugares. De un lado, si el resultado del contrato estuviera perfectamente delimitado, no habría lugar a la aparición del tan nombrado *gap de expectativas*, o diferencia de expectativas entre lo que los usuarios esperan obtener del informe de auditoría y lo que se obtiene realmente. De otro lado, no existirían tan diversas clases de informes de opinión, parte integrante de todo informe de auditoría que resume y concluye el juicio del auditor sobre las situaciones analizadas y los riesgos evaluados.

La jurisprudencia, entendida en sentido amplio como todo pronunciamiento de tribunal en el ejercicio de sus competencias y no como la derivada del Tribunal Supremo que además cumple los requisitos de repetición e identidad, por su parte, ha definido lo siguiente: "... la auditoría de cuentas es, por lo tanto, un servicio que se presta a la empresa revisada..."[9].

27.3. PARTES EN UN CONTRATO DE AUDITORÍA. EL PERFIL DEL AUDITOR INFORMÁTICO

27.3.1. La entidad auditada

La empresa que solicitaba una Auditoría Informática, hasta la actual normativa que veremos más adelante, lo hacía porque constataba una serie de debilidades y/o amenazas provenientes de sus sistemas de información.

[9] Sentencia del Tribunal Superior de Justicia de Madrid, nº 415, 4 de mayo de 1994.

Por lo tanto, la empresa que necesitaba este tipo de servicios lo que estaba demandando en realidad era una solución a sus problemas en términos de eficiencia de sus sistemas, más que una verificación o una revisión del cumplimiento de los controles establecidos. Es decir, se pretendía un asesoramiento especializado en la gestión de dichos sistemas, función más cercana, como vemos, a la consultoría.

Sin embargo, cada vez más las empresas son conscientes de la relevancia del sometimiento del elemento si no imprescindible sí completamente esencial, constituido por los sistemas de tratamiento de la información, a una serie de revisiones y controles entre los que destacan el de seguridad, el de calidad o el de la protección de datos de carácter personal por su preponderancia en virtud de su obligatoriedad legal. Hoy es indispensable disponer en todo momento y de una forma rápida de información suficiente, actualizada y oportuna. Y esto sólo se puede garantizar manteniendo los sistemas de tratamiento de dicha información en perfecto estado que sólo se certifica mediante la correspondiente realización de la pertinente auditoría de dichos sistemas de información.

27.3.2. El auditor informático

Las nuevas tecnologías de la Información y las Comunicaciones están creando nuevos canales y herramientas para la gestión de negocios. El auditor tradicional, esto es, el auditor de cuentas, no se encuentra capacitado en términos de formación para afrontar los nuevos riesgos derivados de la utilización de las tecnologías. De ahí que se haga imprescindible la existencia de la Auditoría de Sistemas de Información[10].

Entre las características del auditor, y como ya hemos señalado en la comparativa expuesta al inicio del trabajo, destaca la independencia. Podemos definir la independencia del auditor como "la ausencia de intereses o influencias que permite al auditor actuar con libertad respecto a su juicio profesional, para lo cual debe estar libre de cualquier predisposición que impida su imparcialidad en la consideración objetiva de los hechos". Los problemas pueden clasificarse en tres grupos principalmente: la compatibilidad de la práctica de la auditoría con las asesorías legales, el interlocutor del auditor dentro de la empresa auditada, y la rotación del auditor[11].

En otro orden de cosas, a pesar de que calificamos de profesional al auditor, hay que precisar, remitiéndonos una vez más a la comparación con la auditoría de cuentas que la Ley de Auditoría de Cuentas, según aclara el Tribunal Constitucional respondiendo a una alegación referente a la vulneración por la LAC del artículo

---

[10] Mur Bohigas, Alfonso, *Los servicios de auditoría interna de sistemas de información*, Seminario Auditoría de los Sistemas de Información y Control Interno (AUDISI'2000), organizado por Informáticos Europeos Expertos, Madrid, febrero 2000.

[11] Lora Lara, B. y Serrano, F., "La auditoría a debate: presente y futuro", en *Partida Doble*, nº 65, marzo 1996, páginas 55 y ss.

regulador de la Ley de Colegios Profesionales, no regula exactamente una profesión liberal, sino una actividad que puede ser realizada por profesionales, pero ni los profesionales han de realizar sólo esa actividad, ni ésta ha de constituir exclusivamente el objeto de una profesión[12].

En cuanto a la sujeción legal del auditor, todos los profesionales que desarrollan su labor en el campo de la auditoría de cuentas están sometidos a una serie de normas que tipifican su capacidad profesional, la conducta para llevar a cabo su cometido y la forma de emitir el informe. Los auditores informáticos no son una excepción, aunque además deben cumplir una serie de requisitos y directrices que les son inherentes. Las diferencias no sólo afectan a las normas, puesto que su cometido también difiere y consiste en la revisión de la función informática o parte de ella, sus áreas de revisión son asimismo originales (organizacional del departamento de SI, de seguridad de accesos lógicos, físicos y controles medioambientales, de actuaciones frente a desastres con los planes de recuperación, del software de sistema en cuanto a las políticas sobre su desarrollo, adquisición y mantenimiento, de software de aplicaciones y de control de aplicaciones, así como las específicas de telecomunicaciones, bases de datos y usuarios) y, finalmente, también pueden ser diferentes sus técnicas utilizadas[13]. En este punto también es más que resaltable la existencia de unos condicionantes éticos imperantes en el ejercicio de esta profesión que por su especial autonomía precisan una especial atención. Pues si es verdad que existen todos estos referentes que delimitan profesionalmente la definición de la auditoría de sistemas de información, no es menos cierto que el asentamiento de la profesión requiere también de la creación y seguimiento de códigos deontológicos que apoyen los mínimos necesarios constituidos por los estándares normativos[14].

Las Normas Técnicas de Auditoría, siguiendo con el análisis comparativo del esquema normativo existente en la Auditoría de Cuentas, son un instrumento regulador propio de la profesión. Existen normas técnicas de carácter general, sobre la cualificación del auditor, la calidad de su trabajo en el ejercicio de su profesión y aspectos de ética profesional. También podemos encontrar normas técnicas sobre la ejecución del trabajo que determinan los procedimientos a aplicar por los auditores. Finalmente, encontramos también normas técnicas sobre elaboración de informes, donde el auditor informático debe exponer los objetivos de control no cubiertos adecuadamente así como las recomendaciones a practicar[15]. En cuanto a la naturaleza y eficacia de estas NTA, y de nuevo recurriendo a la inevitable analogía, hay que entender su carácter puramente normativo como su propia denominación indica, pues

---

[12] Brezmes M. de Villareal, A. M., "La Ley de Auditoría de Cuentas y los Órganos Jurisdiccionales", en *Partida Doble*, nº 94, noviembre 1998, páginas 14 y ss.

[13] Poveda Maestre, J. P., "Auditoría de Cuentas y Auditoría Informática. Análisis de las normas básicas", en *Técnica Contable*, Tomo 46, 1994, páginas 481 y ss.

[14] Páez Mañá, J., "Deontología del Auditor Informático y Códigos Éticos", en *Auditoría Informática: un enfoque práctico*, Ed. RA-MA, Madrid, 1998, 1ª edición, páginas 151 y ss.

[15] Poveda Maestre, J.P., *Auditoría de Cuentas y Auditoría Informática. Análisis de las normas básicas*, *op. cit.*, páginas 482 y ss.

son meras líneas generales de actuación, por lo que la alegación ante los tribunales de su falta de publicación en el Boletín Oficial del Estado es una insistencia sin fundamento, pues este requisito es exigible únicamente para las leyes, según el artículo 2.2 del Código Civil.

Con relación a las funciones del auditor informático, su actividad puede abarcar desde aspectos funcionales, como la adecuación de los sistemas de información a las necesidades reales, hasta la revisión de los tiempos de respuesta, pasando por la fiabilidad de los sistemas. Por supuesto, los aspectos técnicos son los que ofrecen un mayor campo de actuación: desde el comienzo con el computador y sus periféricos, los convenios utilizados para la codificación de datos, los procedimientos de captura de estos, la explotación, la programación, las comunicaciones, o, cómo no, toda la gran área de la seguridad, física y lógica, y de la calidad[16].

El auditor, en el desarrollo de su trabajo, ha de obtener evidencia de los hechos, criterios y elementos que está evaluando, con la finalidad de formarse una opinión. Dicha evidencia deberá ser suficiente y adecuada. Suficiente en cuanto a la cantidad de evidencia a obtener y adecuada con relación a la calidad de la misma, es decir, a su carácter concluyente. Pero para obtener la evidencia adecuada el auditor deberá guiarse por los criterios de importancia relativa y riesgo probable. El de la importancia relativa supone que no todos los hechos, criterios y elementos que forman parte de los documentos contables son de la misma importancia. Existen algunos cuya importancia es decisiva dentro del contexto general para la opinión que el auditor va a emitir. La importancia relativa, de otro lado, es un término de los encuadrables en la denominación jurídica de concepto jurídico indeterminado, pues la mayoría de los pronunciamientos profesionales dejan en manos del buen juicio y experiencia del auditor, aunque existen una serie de consideraciones generales que sirven de guía para fijarla, dependiendo de su aplicación al caso concreto del contexto[17].

El auditor de Sistemas de Información debe tener la capacidad y los conocimientos técnicos para revisar y evaluar el control interno del entorno en que se desarrollan y procesan los sistemas de información, capacidad para revisar riesgos y controles, evaluar y recomendar los controles necesarios de los sistemas de información, y capacidad para diseñar procedimientos y técnicas de auditoría específicas para este tipo de actividad. El auditor de sistemas de información empieza a ser un generalista, porque tiene que ser consciente de que los sistemas de información son un punto clave en una organización[18].

---

[16] Alonso Rivas, G., *Auditoría Informática*, Ediciones Díaz de Santos, S. A., Madrid, 1988, páginas 46 y ss.

[17] Almela Díez, B., "La importancia relativa en auditoría", en *Partida Doble*, nº 73, diciembre 1996, páginas 44 y ss.

[18] Touriño, Marina, Conferencia de apertura en el Seminario Auditoría de los Sistemas de Información y Control Interno (AUDISI'2000), organizado por Informáticos Europeos Expertos, Madrid, febrero 2000.

Otra cuestión tratada en la doctrina es la del desistimiento del auditor. Entre las causas que pueden considerarse suficientes destacan la imposibilidad física de cumplimiento del contrato, la necesidad de atender a otros deberes, las causas de incompatibilidad, la perturbación de las relaciones de confianza entre el auditor y los administradores de la sociedad auditada o los incumplimientos de los deberes de cooperación por parte de la sociedad. En cada uno de los casos habrá que dilucidar su procedencia o improcedencia a efectos de delimitar, entre otras cosas, las consecuencias jurídicas de dicha terminación unilateral del contrato[19].

La responsabilidad del auditor es otro tema polémico en la doctrina, en la Resolución del ICAC de 18 de junio de 1999 se somete a información pública, por seis meses, la Norma Técnica de Auditoría sobre "errores e irregularidades" cuyo objeto es establecer los procedimientos que el auditor tiene que aplicar cuando detecta, y en su caso informa, errores e irregularidades que pudieran existir en los estados financieros objeto de su auditoría así como delimitar su responsabilidad. La norma distingue entre irregularidades, como actos u omisiones intencionados o negligentes cometidos por el personal de la empresa o por terceros que alteren la información contenida en los estados contables, y errores, como actos u omisiones no intencionados que asimismo alteren dicha información. Cuando se derivase la posible existencia de errores e irregularidades, el auditor debe evaluar sus efectos potenciales en las cuentas anuales, y comunicar a la dirección, tan pronto como sea posible, su existencia. La norma propone que informe del asunto a un nivel superior al de las personas presuntamente implicadas y, cuando los últimos responsables de la gerencia estén también implicados, el auditor deberá obtener el adecuado asesoramiento legal.

En 1999 se ha creado una subcomisión que ha iniciado el estudio de la modificación de la Ley de Auditoría de Cuentas. Entre las demandas de los auditores destaca la necesidad de delimitar la responsabilidad del auditor. Los auditores opinan que el carácter ilimitado y solidario de su responsabilidad es excesivo, y así lo confirma el borrador de la Ley de Sociedades Profesionales que introduce esta reivindicación y exime de responsabilidad a aquellos socios de la firma de auditoría que no hayan firmado el informe. En la actualidad, a tenor de lo dispuesto en el artículo 11.2 de la LAC, un demandante puede actuar solidariamente contra cualquiera de los socios auditores de una firma[20].

Para terminar, queremos hacer referencia a una figura que está ganando una gran aceptación en la doctrina, en las organizaciones especializadas y, en definitiva, en la profesión: los Comités de Auditoría. El objetivo del comité es contribuir a la mejora

[19] Iglesias Prada, J. L., "La renuncia al cargo del auditor de cuentas: circunstancias justificativas y consecuencias jurídicas de la renuncia", en *Revista Crítica de Derecho Inmobiliario*, nº 622, mayo-junio 1994, páginas 1501 y ss.

[20] Almela Díez, B., "Novedades en Auditoría", en *Partida Doble*, nº 107, enero 2000, páginas 76 y ss.

de la gestión corporativa y garantizar la asunción de responsabilidades oportunas sobre el control interno[21].

Según se desprende de los informes de renombrados comités o comisiones de expertos en relación con estudios llevados a cabo sobre esta materia, los Comités de Auditoría constituyen una pieza clave en el cumplimiento de las responsabilidades de vigilancia que los Consejos de Administración tienen sobre la información financiera que las sociedades facilitan a sus accionistas y a terceros, sobre los controles internos que tienen establecidos y sobre los procesos de auditorías, tanto internas como externas. Un Comité compuesto exclusivamente de miembros independientes y sin responsabilidad ejecutiva alguna, redundaría necesariamente en una mejor supervisión de las actividades de la sociedad, lo que se traduciría en una mejor defensa de los intereses de los accionistas, presentes y futuros, así como de terceros interesados en la buena marcha de la sociedad. Los Comités de Auditoría de los Consejos de Administración son exigidos por la Bolsa de Nueva York como requisito para admitir una sociedad a cotización y para que puedan seguir operando las sociedades ya admitidas. Del mismo modo, los Comités de Auditoría han sido recomendados por el Informe Cadbury[22].

27.3.3. Terceras personas

La información financiera ha ampliado su campo de comunicación en el sentido de que ya no interesa sólo a los accionistas o propietarios de la empresa, sino también, en la medida en que ha atendido a las implicaciones de la responsabilidad social, ha ampliado la audiencia a la que va dirigida dicha información. Así pues, el actual concepto de usuario ya no se refiere sólo a propietario, sino que se extiende a todos los interesados en la actividad empresarial, entre los que se encuentra la colectividad en general[23].

Así se señala en la Sentencia del Tribunal Superior de Justicia de Madrid nº 415 de 4 de mayo de 1994 ya citada: "la auditoría de cuentas es un servicio que se presta a la empresa revisada y que afecta e interesa *no sólo a la propia empresa, sino también a terceros* que mantengan relaciones con la misma, habida cuenta que todos ellos, empresa y terceros, pueden conocer la calidad de la información económico-contable sobre la cual versa la opinión emitida por el auditor de cuentas".

En la declaración "A Statement of Basic Accounting Theory" en 1966 de la American Accounting Association, en que por primera vez se hace una referencia

[21] Ramírez, J., "La comisión de auditoría", en *Dirección y Progreso*, nº 159, 1998, páginas 115 y ss.

[22] López Combarros, J. L., "Propuestas para una modificación de la Ley de Auditoría de Cuentas", en *Partida Doble*, nº 71, octubre 1996, páginas 42 y ss.

[23] Lara Lara, L., "Una nueva Ley de Auditoría, de todos y para todos", en *Partida Doble*, nº 94, noviembre 1998, páginas 44 y ss.

expresa a la función social de la contabilidad, se establecen los objetivos de la información contable, uno de los cuales es facilitar las funciones y controles sociales, y así comienza la contabilidad a ser considerada como un medio a través del cual la sociedad puede ejercer su función de control sobre las unidades económicas. Si se añade a esta función social el carácter de bien público de la información contable emitida por un auditor independiente, entonces aparece la asunción de una responsabilidad social por parte del auditor como garante de la fiabilidad de dicha información[24].

La diferencia de expectativas alude al desacuerdo entre lo que esperan los usuarios de la auditoría y lo que ofrecen los auditores, teniendo en cuenta, además, que el tipo de auditoría que necesita la sociedad depende, en cada momento, del tiempo y del entorno concreto. En la literatura anglosajona se ha denominado "diferencias en las expectativas de la auditoría" *(audit expectations gap)*, o lo que es lo mismo, las diferencias existentes entre lo que los usuarios esperan de la auditoría y lo que los auditores consideran que es su trabajo[25].

Aunque el fenómeno del gap de expectativas tiene un alcance mundial, es en Europa donde ha alcanzado su mayor virulencia. Como prueba de la inquietud despertada, la Comisión de las Comunidades Europeas promovió un estudio sobre la función, posición y responsabilidad civil del auditor legal, que fue llevado a cabo por el Maastricht Accounting and Auditing Research Center (MARC), para conocer cómo era tratada la auditoría legal en la legislación de los estados miembros, publicado en 1996. La Federación de Expertos Contables Europeos por su parte publicó en enero de 1996 un resumen de recomendaciones desarrolladas por ella como resultado de la investigación llevada a cabo acerca también de la función, posición y responsabilidad civil del auditor legal en la Unión Europea. Posteriormente, en octubre de 1996, la Comisión de las Comunidades Europeas publicó su libro verde sobre los mismos aspectos que los tratados en el informe MARC y en el estudio de la FEE, y organizó una conferencia en Bruselas en diciembre de 1996 para debatir sobre los mismos. Además, en 1992 se había publicado el informe Cadbury sobre los aspectos financieros del gobierno de las sociedades en el Reino Unido, y las ocho mayores firmas internacionales de auditoría crearon en 1993 el "Grupo Europeo de Contacto" para considerar de qué forma la profesión contable en Europa podía responder al *expectation gap*, asumiendo que la profesión debería cambiar en cuanto a sus actuales enfoques y alcances si se pretendían reducir las diferencias en las expectativas[26].

Para terminar este apartado, quisiéramos señalar que ésta no es una tendencia exclusiva de esta actividad. En la literatura empresarial más reciente se ha acuñado el

---

[24] Prada Lorenzo, J. M., "La responsabilidad en auditoría", en *Técnica contable*, tomo 46, 1994, páginas 225 y ss.

[25] García Bernau, M. A. y Vivo Martínez, A., "¿Qué espera la sociedad de la auditoría?", en *Técnica contable*, nº extraordinario, 1998, páginas 17 y ss.

[26] López Combarros, J. L., "Reflexiones sobre algunos puntos relacionados con la auditoría", en *Partida Doble*, nº 85, enero 1998, páginas 24 y ss.

término de *stakeholders*, o interesados, más concretamente apostantes. Se apunta con esta denominación, que recuerda sin duda a los tradicionales primeros interesados o accionistas (*shareholders* o *stockholders*), que existe un modelo de "base ampliada" en el que es necesario que toda organización vea a los nuevos miembros, que en la literatura gerencial norteamericana se asimila a todos los ciudadanos porque se considera que el negocio de su país es la empresa. Al menos es posible identificar cinco grupos de "interesados" o "depositarios de dichas apuestas": los accionistas, los empleados, los clientes, las comunidades locales y la sociedad en general. Podríamos incluso detallar aún más e incluir a los mediadores y distribuidores, a los proveedores, a los competidores, a las instituciones financieras o los medios de comunicación[27].

27.4. OBJETO DEL CONTRATO DE AUDITORÍA INFORMÁTICA

Entendemos por objeto del contrato de auditoría, tras la explicación previa sobre la naturaleza jurídica del mismo, la definición y clasificación que hemos presentado como tales en la introducción del capítulo, y no la pura y simple emisión del informe de auditoría que constituye en esencia la fase final de dicho contrato y no el resultado del encargo que lo caracterizaría, de ser así, como dijimos, como contrato de arrendamiento de obra.

A pesar de su inexistencia en la regulación nacional actual, sobre todo en comparación a la existente en la auditoría de cuentas, el objeto de un contrato de auditoría informática está ampliamente diversificado y se encuentra en un período de auge inusitado que requiere de esfuerzos dogmáticos importantes para su estructuración.

Esta inexistencia legal, pues las referencias normativas que se quieren encontrar, si bien conceptualmente encuentran su calificativo idóneo en el término informático, especifican en todo momento la realización de una auditoría, a secas, sin calificativos, choca de una manera frontal con la espectacular amplitud de áreas de conocimiento y de gestión empresarial que cada vez más se ve abocada a controlar y con la acuciante demanda de profesionales en el mercado. Todo esto, obviamente, pasando por alto las voces discrepantes de algunos profesionales de la auditoría de cuentas que reclaman la denominación de auditoría en exclusiva relegando a las demás especialidades a adoptar la expresión de revisión o similares[28].

Entre las mencionadas "cuasi-referencias legales" se encuentran el artículo 28 e) del Estatuto de la Agencia de Protección de Datos (Real Decreto 428/1993, de 26 de marzo), la Norma Cuarta de la Instrucción 1/1995 de la Agencia de Protección de

[27] Fernández Fernández, J. L., *Ética para empresarios y directivos*, Ed. ESIC, 2ª edición, Madrid, 1996, páginas 179 y ss.

[28] Lara Lara, L., "Una nueva ley de Auditoría, de todos y para todos", *op. cit.*, página 46.

Datos, relativa a prestación de servicios sobre solvencia patrimonial y crédito, y el artículo 17 del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los archivos automatizados que contengan datos de carácter personal.

Aunque nos encontramos en un área que por sus propias características impide el listado de un *numerus clausus* de actividades susceptibles de ser sometidas a este tipo de auditoría, que, consecuentemente, en nuestra opinión, dan lugar a otros tantos subtipos de contratos específicos de auditoría de entornos informáticos, pasaremos a realizar una enumeración de las principales áreas en las que se desarrolla la "inexistente" auditoría informática actualmente.

En concreto, podemos distinguir los siguientes ámbitos principales en la realización de una auditoría informática de la que hemos catalogado como perteneciente a la auditoría jurídica de los entornos informáticos[29]:

1. Protección de datos de carácter personal
2. Protección jurídica del software
3. Protección jurídica de las bases de datos
4. Contratación electrónica
5. Contratación informática
6. Transferencia electrónica de fondos
7. Delitos informáticos

Todas estas áreas deben ser objeto de un análisis de la entrada, tratamiento y salida de la información en los sistemas de información de la empresa desde un punto de vista jurídico. Pasaremos a realizar unas breves observaciones al respecto remitiéndonos al capítulo en concreto de este libro en donde ya se trataban en la primera edición extensa y precisamente cada una de ellas[30].

27.4.1. Protección de datos de carácter personal[31]

Es quizá éste el aspecto que más importancia tiene en relación con la materia tratada, la Auditoría informática, pues ha tenido que esperarse hasta la plasmación por escrito y todo el posterior desarrollo legal del derecho fundamental prescrito, entre otros, por el artículo 18.4 de nuestra Constitución para contar con una referencia legal, como hemos dicho cuasi-explícita, de la existencia de la auditoría de los sistemas de información.

---

[29] Davara Rodríguez, M. Á., *Manual de Derecho Informático*, Ed. Aranzadi, Pamplona, 1997, 396 páginas.

[30] Del Peso, E., *Auditoría Informática: un enfoque práctico*, *op. cit.*, páginas 119 y ss.

[31] Davara Rodríguez, M. Á., *La protección de datos en Europa*, Ed. Grupo Asnef Equifax, Madrid, 1998, páginas 20 y ss.

La actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (LOPD) que supone la reforma de la anterior Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD) sigue obligando en su artículo 9 a la adopción de medidas de seguridad para los archivos, ya no sólo automatizados, que contengan dichos datos de carácter personal. El también artículo 9 de la LORTAD remitía a desarrollo reglamentario para su concreción.

Pues bien, dicho desarrollo reglamentario se plasmó en la práctica en el Real Decreto 994/1999, de 11 de junio, por el que se aprobaba el Reglamento de Medidas de Seguridad para los archivos que contuvieran datos de carácter personal. La nueva LOPD mantiene vigente este Reglamento, tal y como prescribe en su Disposición Transitoria Tercera.

El Reglamento, aplicable por lo tanto, clasifica en tres los niveles de seguridad (básico, medio y alto) a los que hay que someter a los archivos dependiendo del grado de sensibilidad de los datos de carácter personal almacenados. En concreto, se exige una auditoría al menos bianual para todos los niveles excepto para el básico. Entre todas las medidas cuyo cumplimiento se exige que se controle, destaca el procedimiento de respuesta y registro de las incidencias, el control de accesos, la constitución de un responsable de seguridad...[32] De esta auditoría, que puede ser tanto interna como externa, se obtendrá necesariamente un informe del cual el responsable de seguridad elevará las conclusiones al responsable del archivo, encontrándose a disposición de la Agencia de Protección de Datos en todo caso.

Si bien es cierto que esta auditoría no lleva calificativo legal alguno, no es menos cierto que encuentra en la Auditoría de Sistemas de Información su acomodo perfecto, en la conjunción de la auditoría de seguridad de los sistemas que tratan los datos y la calificación jurídica de los datos involucrados.

27.4.2. La protección jurídica del software[33]

La calificación jurídica del software ha sido objeto de discusión doctrinal, porque integra distintos elementos que pueden encuadrarse bajo diferentes órdenes de protección jurídica, unos amparables bajo la legislación de la propiedad industrial y otros bajo la de la propiedad intelectual. La inclusión bajo esta última, y en concreto bajo la figura de los derechos de autor, hace que asimilemos los programas de computador a las obras literarias, científicas o artísticas.

Como bienes objetos de esta protección, la auditoría a la que se tienen que someter debe verificar el cumplimiento de la misma, y, por lo tanto, investigar la

[32] Del Peso, E., y Ramos, M. Á., *LORTAD Reglamento de Seguridad*, Ediciones Díaz de Santos, S.A., Madrid, 1999, páginas 163 y ss.

[33] Davara Rodríguez, M. Á., *Manual de Derecho Informático*, *op. cit.*, páginas 103 y ss.

legalidad del software utilizado en dichos sistemas, evaluando el riesgo que se corre por permitir la ilegalidad, el "pirateo", y cuantificando monetariamente hablando el diferencial existente entre dicho riesgo y el coste de implantación y control de todos y cada uno de los programas utilizados en la entidad.

Los auditores informáticos tienen que eliminar los riesgos en esta área proporcionando de este modo un valor añadido a una buena gestión informática, siguiendo los criterios expuestos, entre otros, por la ISACA en su concepto de Value for Auditing Money para una mejor gestión y control de las licencias de software. En particular, se pueden concretar los riesgos que conlleva la realización de copias no autorizadas de software original como son las sanciones y multas, los problemas técnicos, la inexistencia de asistencia técnica, la obsolescencia tecnológica, el impacto negativo en la calidad del software, el deterioro de la imagen empresarial y los ataques intencionales[34].

27.4.3. La protección jurídica de las bases de datos[35]

Una base de datos es un depósito común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada, para la resolución de un problema planteado en una consulta. Es decir, contiene datos, pero proporciona información. De nuevo nos encontramos con la figura jurídica de los derechos de autor como la adecuada para su posicionamiento, por la carga de creatividad que conlleva. Pero, además, surge la denominada protección mediante un derecho *sui generis* de las bases de datos, pues se pretende garantizar la protección de la inversión en la obtención, verificación o presentación del contenido de una base de datos, evitando que una copia de los contenidos de una base de datos determinada sometidos a unos criterios distintos de almacenamiento, indización, referencias y métodos de recuperación constituya una nueva base de datos que quede asimismo amparada bajo la figura de los derechos de autor.

Se establecen asimismo como requisitos necesarios para que la base de datos sea susceptible de dichas protecciones la existencia de un autor o autores identificables y relacionados con la obra realizada y el trabajo original que ha dado lugar a dicha base de datos.

En el planteamiento de los bienes y derechos objeto de protección, habrá que atender, de un lado, los derechos de los titulares de los documentos almacenados, de otro lado, los derechos de los productores de la base, pues su creación tiene también una carga de intelectualidad, y, por último, el derecho del titular de la base a impedir la extracción o reutilización total o parcial.

---

[34] *Guía de Auditoría de Software Original*, Business Sotware Alliance, Madrid, 2000, páginas 2 y ss.

[35] Davara Rodríguez, M. Á., *Manual de Derecho Informático*, *op. cit.*, páginas 133 y ss.

Pues bien, la auditoría en este caso tendrá del mismo modo que atender a los tres casos expuestos, analizando el cumplimiento para todos ellos de los controles establecidos, evitando por lo tanto copias o extracciones no autorizadas, y verificando la gestión y actualización por las personas competentes y autorizadas para ello.

El auditor debe en primer lugar analizar la metodología de diseño para determinar su aceptabilidad y luego comprobar su correcta utilización, después tendrá que examinar si los diseños se han realizado correctamente, una vez puesto en explotación deberá comprobar los procedimientos de explotación y mantenimiento, y finalmente deberá establecer un plan para después de la implantación. Del mismo modo, la formación del personal a lo largo de la vida del producto consituye un elemento permanente e indispensable[36].

27.4.4. Contratación electrónica[37]

Entendemos por contratación electrónica toda aquella que se realiza por algún medio electrónico. Con la generalización del uso de Internet el auge de este tipo de contratación empieza a ser constatable. Pero no sólo esta red mundial acapara el perfeccionamiento de contratos electrónicos, aunque es cierto que ha sido su implantación la que ha relegado al anterior sistema EDI (Electronic Data Interchange) utilizado principalmente para transacciones intraempresariales[38].

Hoy en día, en el comercio electrónico concretamente, y entendido en su más amplio sentido como cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación *como* Internet, se habla de la segmentación en la utilización de estos medios electrónicos en tres sentidos: en la dirección empresa-consumidor final (business to consummer, B2C), en la dirección empresa-empresa (business to business B2B), y finalmente, en la dirección empresa-administraciones públicas (business to administrations, B2A). Además podríamos separar al consumidor final o usuario como artífice activo de dicha contratación y añadir la contratación entre consumidores (consummer to consummer, C2C) y la gestión de las relaciones administrativas de los administrados electrónicamente.

Podríamos también diferenciar entre comercio electrónico directo como aquel que consiste en la obtención del bien o servicio íntegramente por el medio electrónico, por

---

[36] Piattini Velthuis, M., "Auditoría de las Bases de Datos y de los Almacenes de Datos" (datawarehouses), conferencia pronunciada en Seminario Auditoría de los Sistemas de Información y Control Interno (AUDISI'2000), organizado por Informáticos Europeos Expertos. Madrid, Febrero 2000.

[37] Davara Rodríguez, M. Á., *La protección de los intereses del consumidor ante los nuevos sistemas de comercio electrónico*, Ed. Confederación Española de Organizaciones de Amas de Casa, Consumidores y Usuarios (CEACCU), Madrid, 2000, páginas 37 y ss.

[38] Del Peso, E., "Auditoría jurídica de los entornos informáticos", en *Informática y Derecho*, nº 19-22, 1998, páginas 644 y ss.

ejemplo, la compra de un libro en formato electrónico, o el comercio electrónico indirecto en el que alguna de las actividades que perfeccionan la adquisición del bien o servicio no se realiza por medios electrónicos, ya sea el transporte, el pago o cualquier otra.

En la contratación electrónica hay que atender a tres aspectos fundamentales: en primer lugar a la inmediatez de las relaciones, cuestión que se solventará en caso de relación mercantil por el momento de emisión de la aceptación y en caso de otro tipo de relación por el momento en que llega a conocimiento del oferente, en segundo lugar a la calidad del diálogo, y excluyendo el teléfono o la videoconferencia habrá que asemejar la aceptación a la hecha por correspondencia escrita en soporte papel, y, en tercer lugar, desde el punto de vista de la seguridad. Pasamos a dedicar un especial párrafo a este aspecto.

En lo que a seguridad se refiere, en las transmisiones electrónicas de datos se busca garantizar la autenticidad, la integridad y el no repudio (en origen y en destino) de las mismas. Actualmente existe un mecanismo que puede garantizar estos extremos: la firma digital. España ha sido una vez más pionera en estos temas regulatorios de los aspectos jurídicos de la denominada sociedad de la información. En efecto, antes de que se apruebe la Directiva europea sobre firma electrónica, se aprobó el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, y la Orden de 21 de febrero de 2000 aprobó en su Anexo el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica. Aunque no es objeto de este trabajo su análisis exhaustivo no queremos dejar de mencionar las características más importantes de esta novedosa normativa. El Real Decreto ley 14/1999 distingue entre dos clases de firma electrónica, la simple y la avanzada o digital. La firma digital tiene que cumplir una serie de requisitos, entre otros el ser emitida por un prestador de servicios acreditado y su eficacia jurídica es idéntica a la de la firma manuscrita. El prestador de servicios, en terminología comunitaria ahora adoptada por la legislación nacional que ha preferido no utilizar la calificación de autoridad de certificación y despojarle así de ninguna pretendida competencia pública, se constituye en una tercera parte de confianza, creándose el "fedatario electrónico", que puede identificar y autenticar a las partes intervinientes, por medio de técnicas de cifrado de claves con las arquitecturas de clave pública o Public Key Infraestructure (PKI) que se basan en la utilización de algoritmos de clave asimétrica de entre los cuales destaca el R.S.A, garantizar la integridad de los mensajes transmitidos, y asegurar el no repudio de las comunicaciones, en origen, que quien hizo la oferta lo niegue, y en destino, que quien la aceptó lo haga. Además se puede añadir la función de sellado temporal en la que se certifique fecha y hora del perfeccionamiento de dicho acuerdo. No obstante, estas funciones únicamente las puede garantizar un prestador de servicios acreditado, pues si bien la constitución de estos prestadores se realiza en un régimen de libre competencia sin que la falta de acreditación pueda conllevar la inexistencia de tal prestador, sólo los acreditados podrán expedir certificados reconocidos que lleven aparejada dicha firma digital que tiene plenos efectos jurídicos.

Desde el punto de vista de los controles a los que se puede someter este tipo de contratación se requiere un asesoramiento técnico para que la redacción jurídica se adecue a la ingente potencialidad de la herramienta utilizada que hace que la mera traslación de las categorías conceptuales tradicionales al medio virtual no sea posible sin el previo sometimiento a unas especificaciones y aclaraciones de todo punto imprescindibles en virtud del modo de perfeccionarse estos contratos que, sin ser un elemento esencial como hemos mencionado para los restantes tipos contractuales, se hace necesario por las consecuencias jurídicas que se pueden derivar de su inobservancia.

Es decir, la aparición de estas nuevas formas de contratación, traspasa las fronteras de la mera forma para constituirse en elementos definitorios de cuestiones tan relevantes en la práctica contractual como la delimitación y en su caso exoneración de responsabilidades, la prestación de garantías o la división de obligaciones entre las partes que no pueden sin más asemejarse a las categorías convencionales, entre otras cosas por la globalización y por tanto intersección de legislaciones nacionales. Ni siquiera los términos tradicionalmente constituidos en usos del comercio, que según nuestra legislación mercantil tienen carácter de fuente de Derecho son absolutamente trasladables a este entorno, y ejemplo claro de ello es el intento de definición de unos "e-terms", en una clara regulación paralela a los utilizados y reconocidos incoterms en el tráfico mercantil internacional.

27.4.5. La contratación informática[39]

Definiéndola como la contratación de bienes o servicios informáticos. Bienes informáticos son todos aquellos elementos que forman el sistema en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, así como todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en conjunto, conforman el soporte físico del elemento informático. Asimismo, se consideran bienes informáticos los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático. Los servicios informáticos son todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella.

Podemos dividir en dos grandes grupos diferenciados: respecto al objeto, debido a las características especiales de los distintos objetos sobre los que pueden versar estos contratos, y respecto al negocio jurídico, debido a que los contratos informáticos más comúnmente realizados se han llevado a cabo bajo una figura jurídica determinada (compraventa, arrendamiento financiero, mantenimiento, préstamo...) en

[39] Davara Rodríguez, M. Á., *Manual de Derecho Informático*, *op. cit.*, páginas 191 y ss.

la que han encontrado acomodo pero que en casi todos los casos ha sido necesario adecuar.

La contratación de bienes y la prestación de servicios informáticos no tiene una calificación uniforme para situarla en un modelo o tipo de contrato. Los contratos informáticos están formados por elementos tan dispares que exigen la mezcla o unión de dos o más tipos de contratos. Asimismo, el desconocimiento por el usuario, en términos generales, de las posibilidades y límites de la informática, hace que no todo en el contrato pueda estar basado en el principio de autonomía de la voluntad de las partes. En muchas ocasiones son contratos de adhesión, en los que una de las partes fija las cláusulas del contrato y la otra se adhiere a las mismas, sin tener posibilidad de modificar ninguna de ellas.

La contratación informática resulta extremadamente complicada en la redacción de los contratos y en la fijación de los derechos y obligaciones de las partes. A ello hay que añadir la inexistencia de una normativa adecuada a los mismos y la dificultad en la fijación del objeto cuando son contratos complejos. Se deben redactar teniendo en cuenta un equilibrio de prestaciones y evitar en lo posible la existencia de cláusulas oscuras. Y es aquí, de nuevo, donde la figura del auditor informático cobra toda su importancia asesorando e implantando en dicho acuerdo los requisitos técnicos y los términos específicos que delimitan y concretan los aspectos imprescindibles cuyo cumplimiento debe ser objeto de los controles a los que se someta este tipo de contratación cuyas particularidades requieren un asesoramiento especializado y experto.

27.4.6. Transferencia electrónica de fondos[40]

Éste es un tema común a la contratación electrónica, a la protección de datos de carácter personal y al pago electrónico. En concreto este último adquiere una relevancia en la práctica inusitada y en constante crecimiento. Esta relevancia y sus particularidades justifican su tratamiento independiente. Nos referiremos en concreto a los medios de pago electrónicos ya conocidos, esto es, las tarjetas de crédito y de débito, o el caso particular de las asociadas a un determinado establecimiento mercantil para la realización de compras en el mismo, y sólo mencionamos aquí el naciente fenómeno de los micropagos y del dinero electrónico propiamente dicho y de las consecuentes entidades emisoras de dinero electrónico.

No obstante, y dado que una vez más tenemos que recordar el objeto de este capítulo, no es éste el lugar donde analizar las fases de la transferencia electrónica de fondos, ni los derechos y obligaciones de las distintas partes implicadas, el emisor del instrumento de pago y el usuario, ni la nueva situación de desequilibrio derivada de la

[40] Davara Rodríguez, M. Á., *Manual de Derecho Informático*, *op. cit.*, páginas 237 y ss.

utilización de nuevo de los contratos de adhesión, ni la confidencialidad ni seguridad de los datos de carácter personal involucrados, ni la delimitación de las responsabilidades y riesgos existentes en el uso de este medio de pago.

La tarea específica de este ámbito para el auditor informático, aparte de la posible y probable intersección de alguno de los otros ámbitos especificados, reside en la comprobación de la interoperabilidad entre los sistemas de lectura de las tarjetas y las redes de comunicaciones.

27.4.7. El delito informático[41]

Éste es un tema debatido en la doctrina tanto en su definición, más allá, en cuanto a su existencia legal, como en su clasificación. De un lado, los elementos integrantes de la definición estricta de delito en la doctrina criminalista, son difícilmente encontrables en la utilización de medios informáticos, en su más amplio sentido, en la comisión de ilícitos. De otro lado, en la clasificación de todas las acciones ilegales dolosas instrumentalizadas de este modo tampoco existe unanimidad. Parece claro que son los fraudes los que más importancia cualitativa y cuantitativa encuentran dentro de este delito. Pero tampoco en la ordenación de los mismos se especifica una selección única. A modo de ejemplificación, baste enumerar los virus informáticos, la actuación de los llamados piratas informáticos, o el mero robo y otras acciones físicas similares contra los elementos físicos y lógicos de los equipos informáticos, donde destaca sobremanera, la piratería del software ya mencionada más arriba[42].

Como no es el objeto de este capítulo el desarrollo intenso de este tema, remitimos de nuevo a la parte específica de esta obra donde se detalla su contenido y pasamos a intentar circunscribir el ámbito de la auditoría de sistemas de información con relación al denominado delito informático. La intervención del auditor informático reviste aquí, sin lugar a dudas, una especial utilidad. Si, como hemos mencionado, en cuanto a los errores e irregularidades detectables en la auditoría de cuentas tiene un deber de diligencia y cuidado profesional que determina su comunicación a la empresa auditada, en cuanto a la detección de delitos existe una prescripción legal que, por la experiencia y profesionalidad, del auditor le constituye en el sujeto idóneo para no sólo la constatación de estos delitos sino también para ayudar en su delimitación conceptual a efectos de su inclusión en una u otra categoría, otorgándole, por otra parte, por estas mismas consideraciones una especial responsabilidad en dicha detección.

---

[41] Davara Rodríguez, M. Á., *De las autopistas de la información a la sociedad virtual*, Ed. Aranzadi, Pamplona, 1996, páginas 164 y ss.

[42] Del Peso, E., *Manual de dictámenes y peritajes informáticos. Análisis de casos prácticos*, Ediciones Díaz de Santos, S.A., Madrid, 1995, páginas 153 y ss.

27.5. CAUSA

Para terminar con el análisis de los elementos esenciales de todo contrato, pasamos a examinar la causa del contrato de auditoría.

De todo lo anterior cabe deducir que la exigencia LEGAL de la Auditoría de los Sistemas de Información en la actualidad es, en puridad, nula. No existe ni una sola disposición de ningún rango que determine la realización de una auditoría de estas características.

No obstante, toda la actual regulación en materia de protección de datos de carácter personal aconseja y suena a su imposición. No cabe, hermenéuticamente hablando, la posibilidad de que se esté refiriendo en este cuerpo normativo a una auditoría de las "convencionales". Aparece, de este modo, la "figura legal" de la Auditoría Informática, si se opta por no someterse a la literalidad de la Ley, en cuyo caso conduciría a la única auditoría existente por el momento a efectos de reconocimiento legal: la auditoría de cuentas, y acudir a la ya tradicional y aceptada corriente de interpretación del espíritu de la norma, a efectos de conseguir una conclusión más adecuada y realista, que lleva ineludiblemente a la aceptación de la Auditoría Informática como la idónea para este análisis.

Por lo tanto, es posible, en nuestra opinión, concluir que la causa puede tener en este contrato, dentro de su licitud, sus dos orígenes: de un lado, partiendo de la autonomía de la voluntad, principio rector en materia de Derecho contractual prescrito en el artículo 1255 del actual Código Civil, puede ser solicitada a simple voluntad de la empresa auditada, y, de otro lado, como cumplimiento de la exigencia legal prevista en la normativa de protección de datos de carácter personal y en concreto en el artículo 17 del Reglamento de Seguridad.

27.6. EL INFORME DE AUDITORÍA

El informe de auditoría constituye el producto final del trabajo de auditoría y la única documentación que va a llegar a quien la ha encargado. Sus objetivos principales consisten en permitir al que revisa entender el trabajo realizado, las circunstancias que afectan a su fiabilidad y las conclusiones del auditor, así como prevenir una interpretación errónea del grado de responsabilidad asumido por el auditor[43].

El informe debe estar escrito e ir firmado. En él deben constar los antecedentes, el objetivo del proceso de auditoría, las posibles limitaciones, y un resumen para la

[43] Bernal Montañés, R. y Coltell Simón, O., *Auditoría de los Sistemas de Información*, Universidad Politécnica de Valencia, Valencia, 1996, páginas 123 y ss.

Dirección en términos no técnicos. En cada punto debe explicarse por qué es un incumplimiento o una debilidad, y alguna recomendación. Ha de discutirse con los auditados antes de emitir el definitivo. En algunos casos incluso se pueden recoger las respuestas de los auditados[44].

El informe de auditoría de cuentas anuales, obligatorio para ciertas entidades que cumplan unos determinados parámetros, es un documento donde se pone de manifiesto la opinión del auditor, respecto de la fiabilidad de la información contable auditada, de manera que cualquier tercero pueda valorar dicha información y, en su caso, tomar decisiones sobre la base de la misma con auténtico conocimiento de causa. Estas características son, de nuevo, aplicables al informe consecuente de la realización de una auditoría informática.

Un informe debe constar de las siguientes partes: título, destinatario (a quién va dirigido y quién efectuó el nombramiento), identificación de la entidad auditada, párrafo de alcance (NT utilizadas y excluidas en su caso), párrafo de comparabilidad (respecto a ejercicios anteriores), párrafo de salvedades (detallando su efecto sobre las cuentas anuales o su naturaleza), párrafo de énfasis, párrafo de opinión (especialmente recalcando el principio general contable de representación de imagen fiel), párrafo sobre el informe de gestión, firmas y fecha (que coincida con la de terminación del trabajo en la oficina de la entidad auditada)[45].

Para que el auditor pueda transmitir de forma satisfactoria su trabajo a los colectivos interesados, el informe de auditoría debe ser un documento que ha de ser leído y comprendido sin que los lectores encuentren dificultad o dudas en la interpretación del mensaje que contiene. En términos generales, se ha producido un rechazo al informe corto y la aceptación generalizada de su alargamiento, de nuevo como una forma más, entre otras cosas, de acortar el tan nombrado *gap* de expectativas[46].

27.7. CONCLUSIONES

Estas conclusiones tendrán dos partes diferenciadas: En primer lugar, extraeremos los puntos más resaltables en cuanto a los elementos del contrato analizado, y después pasaremos a realizar un más extenso análisis de la situación actual normativamente hablando de la auditoría informática, pues es en este punto donde encontramos que se debe hacer hincapié a la vista de lo estudiado anteriormente.

---

[44] Ramos González, M. Á., Auditoría informática, en *Informática y Derecho*, nº 19-22, 1998, páginas 657 y ss.

[45] López Corrales, F., "Cumplimiento de las normas técnicas en la emisión de informes", en *Partida Doble*, nº 94, noviembre 1998, páginas 68 y ss.

[46] García Bernau, M. A. y Vico Martínez, A., "Tendencias internacionales en la elaboración de los informes de auditoría", en *Técnica Contable*, Tomo 48, 1996, páginas 11 y ss.

El contrato de auditoría informática, como todo lo que afecta a la regulación jurídica de las Nuevas Tecnologías de la Información y las Comunicaciones, no es algo que se encuentre delimitado. La inseguridad jurídica es palpable. El objeto propio de esta contratación, además de su multiplicidad, se caracteriza por la dificultad de su configuración jurídica. La profesión de auditor informático, aparte de su falta de regulación, sufre, entre otras cosas, de intrusismo profesional y de extralimitación de sus funciones. La empresa que solicita una auditoría informática suele tener dudas en cuanto a su objeto y a su resultado. La diferencia de expectativas es aquí mayor porque ni siquiera se tiene claro lo que se espera, pues se espera todo, se espera una solución, no una detección de los problemas. En cuanto a los terceros, menos claro tienen aún la existencia y delimitación de la figura. Por otra parte, la causa, como hemos visto, es escasamente legal en cuanto a periodicidad en la obligación.

No vamos a abandonar en este último apartado el obligado, esperamos que no por mucho tiempo, esquema comparativo respecto a la auditoría de cuentas que hemos venido siguiendo, y, por lo tanto, nos aprovecharemos del análisis de la situación actual de la misma e intentaremos sintetizar los puntos más relevantes para basar nuestras "reivindicaciones".

Comencemos por resaltar una vez más lo novedoso de su normativa. Sólo a partir de la LAC (1988) se regula por primera vez la profesión de auditoría de cuentas, determinándose quién puede ser auditor de cuentas, cómo debe actuar el auditor de cuentas en el ejercicio de su profesión, los plazos para la contratación, el régimen de incompatibilidades y las responsabilidades y mecanismo sancionador. Para una profesión que se remonta a los orígenes de las civilizaciones más antiguas, resulta cuando menos llamativo.

Pero además, la auditoría tiene aún pendientes numerosos problemas que afectan tanto al contenido de sus normas de trabajo, como al alcance del mismo, o a la forma de su expresión como actividad profesional. Temas como la autorregulación profesional, la unificación de criterios, la internacionalización de los principios contables, conceptos como los de empresa en marcha, importancia relativa, fraude e ilegalidad, la compatibilidad de las funciones de auditor profesional y la consultoría, sobre los procesos de concentración, las relaciones con las autoridades, los controles deontológicos, o la calidad del trabajo. También es necesaria una normativa común europea sobre aspectos relacionados con la independencia y objetividad del auditor, las reglas de contratación, las responsabilidades exigibles, los seguros de responsabilidad profesional, y el régimen de control y supervisión y de sanciones aplicables por conductas impropias[47].

[47] Sánchez Fdez. de Valderrama, J. L., "La auditoría en el contexto económico actual", en *Técnica Contable*, nº extraordinario, 1998, páginas 37 y ss.

Apoyando esta afirmación, como hemos visto, el *Libro Verde* sobre la función, posición y responsabilidad civil del auditor legal en la Unión Europea[48], publicado por la Comunidad en 1996, pone de manifiesto la necesidad de homogeneizar el ejercicio de la auditoría en aspectos como su definición, la forma y el contenido del informe, la independencia del auditor legal, la forma de realización del control de calidad, la responsabilidad del auditor legal... en orden a establecer las bases que permitan el desarrollo del mercado interior de los servicios de auditoría. El Parlamento Europeo, por su parte, analizó el citado *Libro Verde* y aprobó una Resolución en enero de 1998 en la que consideraba, entre otras cosas, la necesidad de concretar los objetivos más inmediatos, la idoneidad de la constitución de un subcomité técnico, la necesidad de armonizar el ejercicio de la auditoría en la UE resaltando la relevancia de las normas profesionales, la independencia del auditor y el ejercicio del control de calidad, la responsabilidad civil de los auditores, aconsejando la suscripción de un seguro mínimo... En resumen, que para que se desarrolle el mercado interno de los servicios de auditoría es imprescindible que se disponga de un modelo común de organización de la actividad. La Comisión Europea, como continuación del anterior análisis del Parlamento, presentó un documento denominado "La auditoría legal en Europa: el camino a seguir", donde se especifica que el fin de protección del interés público, el aumento de la armonización de la información financiera y el incremento de la fiabilidad de la misma convierten a la auditoría en un elemento importante para el establecimiento y funcionamiento del mercado único. La Comisión es consciente de la falta de unanimidad sobre la función, posición y responsabilidad civil del auditor legal y de la necesidad de adoptar un modelo común que a su vez respete los estándares internacionales en la ejecución del trabajo, en la emisión de la opinión y en los controles establecidos para mejorar la calidad de los citados informes[49].

En definitiva, si una profesión tan antigua como la auditoría convencional adolece de tantas imperfecciones legales, con tantos problemas y aspectos sin definir y con extremos tan absolutamente indefinidos, y dado el muy superior ritmo de crecimiento e importancia de la auditoría informática, entendemos que ya se está a un nivel de importancia, aunque sea pretendidamente soslayada, y de presencia real de la profesión, como para reclamar el reconocimiento de una identidad y particularidad. Así, en un futuro cercano esperamos tener que dejar de realizar análisis comparativos nada satisfactorios en el estudio de las características originales y propias de esta profesión.

"Aprovechemos", pues, las similitudes existentes y la indefinición legal que sufre en muchos puntos la auditoría de cuentas para comenzar un proceso normativo propio que delimite la figura de la auditoría de sistemas de información en todos sus aspectos: desde los subjetivos, definiendo el perfil del auditor informático, hasta los objetivos,

---

[48] *Libro Verde: función, posición y responsabilidad civil del auditor legal en la Unión Europea* (96/C321/01).

[49] Gómez Ciria, A., "Décimo aniversario de la Ley de Auditoría de Cuentas", en *Partida Doble*, número 94, noviembre 1998, páginas 4 y ss.

en cuanto a la regulación legal principalmente, y los instrumentales u organizativos. Es preciso lograr una regulación, del tipo que sea, propia y delimitadora, declarativa que no constitutiva, de lo que es una realidad creciente en número e importancia: la profesión de auditoría informática.

27.8. LECTURAS RECOMENDADAS

Davara Rodríguez, M. Á., *Manual de Derecho Informático*, Editorial Aranzadi, Pamplona, 1997. *La protección de los intereses del consumidor ante los nuevos sistemas de comercio electrónico*, Editorial CEACCU, Madrid, 2000.

Ramos González, M. Á., La auditoría informática, en *Actualidad Informática Aranzadi*, nº 14, enero de 1995.

VV.AA., Del Peso Navarro, E. (Director), *Manual de dictámenes y peritajes informáticos: Análisis de casos prácticos*, Ediciones Díaz de Santos, Madrid, 1995.

VV.AA., Del Peso Navarro, E. y Piattini Velthuis, M. G. (Coordinadores), *Auditoría informática: un enfoque práctico*, Ed. Ra-Ma, 1ª edición, Madrid, 1998.

27.9. CUESTIONES DE REPASO

1. Comparativa entre las definiciones "legales" de la auditoría de cuentas y la auditoría de sistemas de información.
2. ¿Cuál es la naturaleza jurídica del contrato de auditoría? ¿Por qué?
3. Las Normas Técnicas de Auditoría.
4. Auditoría interna frente a Auditoría externa en sistemas de información.
5. Las terceras personas o interesistas y la información en el contrato de auditoría.
6. Utilidad de los Comités de Auditoría.
7. Distintos objetos en el contrato de auditoría informática.
8. La auditoría en la protección de datos de carácter personal.
9. La causa en el contrato de auditoría.
10. Características del informe de auditoría.