Seguridad informática

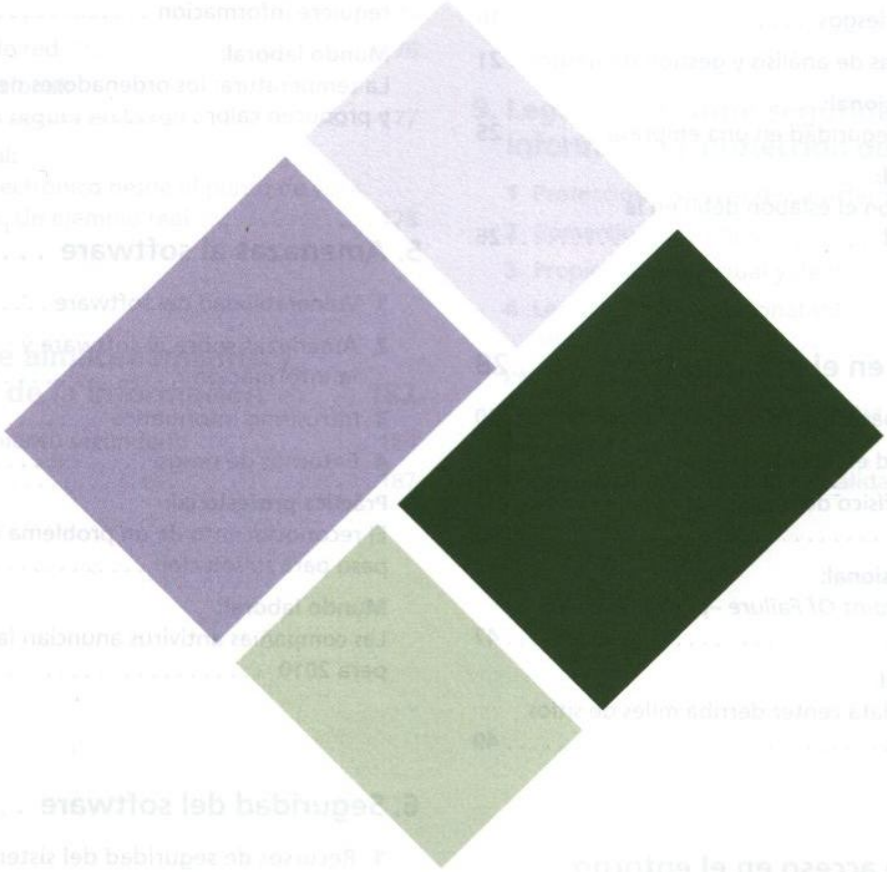
Purificación Aguilera

INFORMÁTICA Y COMUNICACIONES

EDITEX

Seguridad informática

Purificación Aguilera López



EDITEX

ÍNDICE

CÓMO SE USA ESTE LIBRO

El libro de **Seguridad Informática** consta de nueve unidades de trabajo. Cada una de ellas comienza con un **Caso práctico inicial,** que presenta una situación real o simulada muy cercana al mundo profesional y directamente relacionada con el contenido de la unidad, con los siguientes apartados:

- **Situación de partida:** descripción del caso, con los personajes, condiciones, hechos y datos relevantes para analizarlo.
- **Estudio del caso:** cuestiones que se plantean para facilitar el análisis de la situación.

El **desarrollo de los contenidos** aparece estructurado de forma clara y ordenada y acompañado de múltiples cuadros, tablas y esquemas que refuerzan los contenidos explicados facilitando su comprensión o muestran situaciones o técnicas que utilizarás durante el desempeño de tu trayectoria profesional.

En los márgenes aparecen textos complementarios con ampliación de información, vocabulario y recordatorios para profundizar en los conocimientos expuestos.

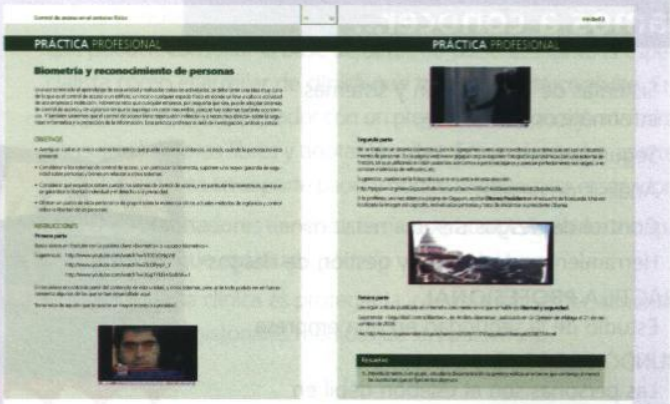
A lo largo de la unidad se destacan aquellos contenidos que tienen relación directa con el **caso práctico inicial,** y se explica dicha relación. Estas llamadas reiteradas en los contenidos convierten el caso práctico inicial en el **eje vertebrador de la unidad.**

Al finalizar cada epígrafe se incorporan **actividades** de carácter teórico-práctico y que pretenden aclarar los conceptos tratados con anterioridad.

Seguridad informática

En la sección **Práctica profesional** te planteamos varios casos prácticos elegidos entre los más comunes que puedes encontrar en la práctica de tu profesión, situaciones reales vinculadas con los temas tratados, de modo que puedas ver la aplicación práctica de los contenidos y, al mismo tiempo, tener una visión conjunta de los mismos.

Estas prácticas profesionales representan los **resultados de aprendizaje** que deberás alcanzar al terminar tu modulo formativo.

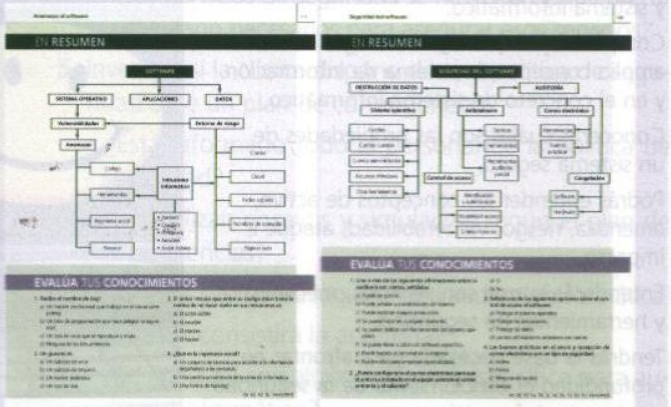


La sección **Mundo laboral** te enfrenta a la realidad de la profesión mediante la utilización de artículos aparecidos en prensa o en internet, sobre cuestiones de actualidad relativas a los contenidos tratados.

En esta sección se incluye también una serie de cuestiones que te ayudarán a reflexionar tras la lectura del texto y a debatir en clase con tus compañeros.

Finalmente, el apartado **En resumen** contiene un esquema organizado que destaca las ideas fundamentales de la unidad, diseñado para facilitar la consulta y el aprendizaje de los conceptos claves.

La unidad finaliza con el apartado **Evalúa tus conocimientos** consistente en una batería de preguntas tipo test que te permitirán comprobar el nivel de conocimientos adquiridos al término de la unidad.



→

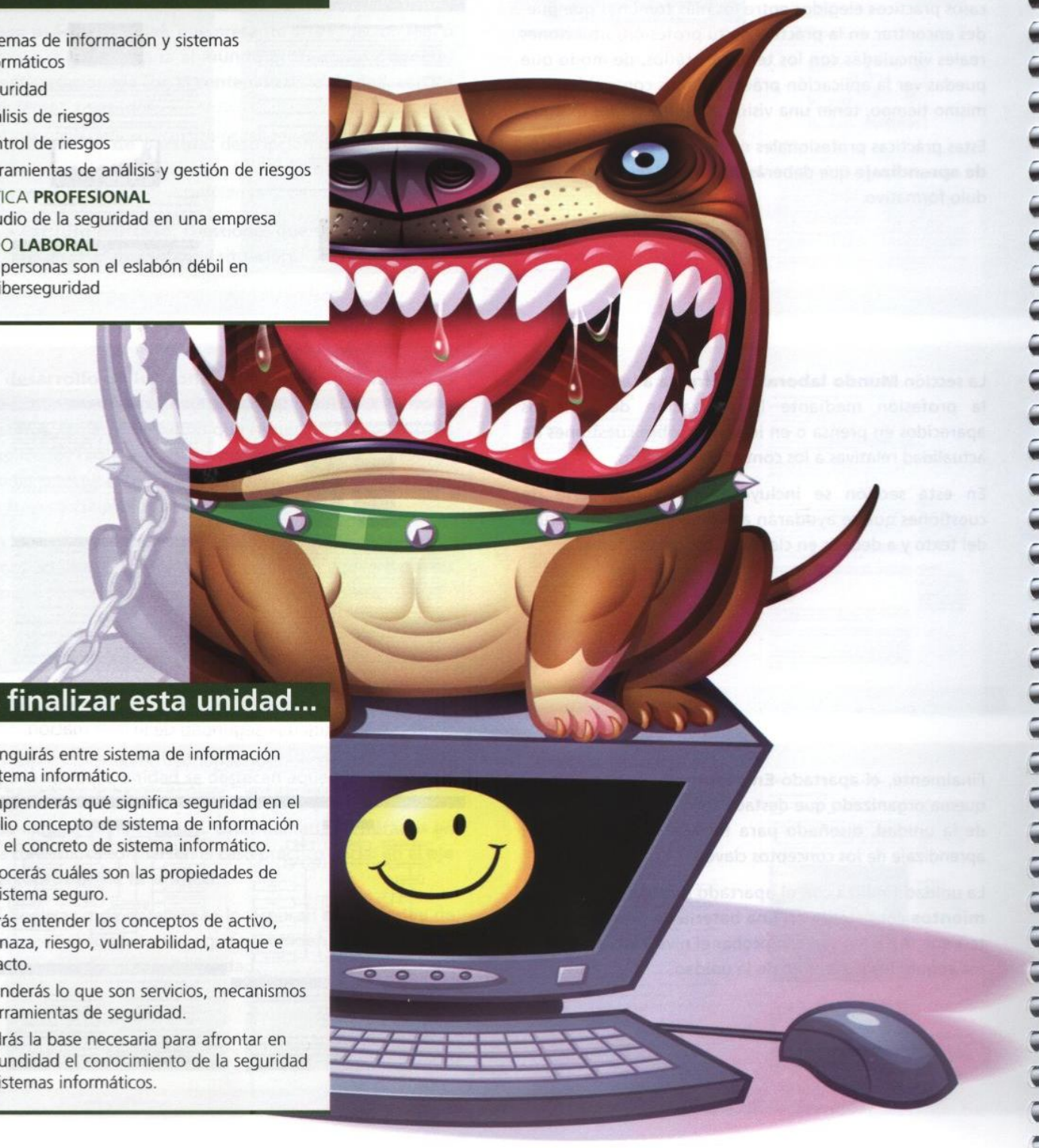
1 Introducción a la seguridad informática

vamos a conocer...

1. Sistemas de información y sistemas informáticos
2. Seguridad
3. Análisis de riesgos
4. Control de riesgos
5. Herramientas de análisis y gestión de riesgos

PRÁCTICA **PROFESIONAL**
Estudio de la seguridad en una empresa

MUNDO **LABORAL**
Las personas son el eslabón débil en la ciberseguridad



y al finalizar esta unidad...

- Distinguirás entre sistema de información y sistema informático.
- Comprenderás qué significa seguridad en el amplio concepto de sistema de información y en el concreto de sistema informático.
- Conocerás cuáles son las propiedades de un sistema seguro.
- Podrás entender los conceptos de activo, amenaza, riesgo, vulnerabilidad, ataque e impacto.
- Entenderás lo que son servicios, mecanismos y herramientas de seguridad.
- Tendrás la base necesaria para afrontar en profundidad el conocimiento de la seguridad en sistemas informáticos.

CASO **PRÁCTICO** INICIAL

situación de partida

Una clínica dental se dirige a una empresa de servicios informáticos solicitando un estudio de sus equipos e instalaciones para determinar el grado de seguridad informática y los ajustes que se consideren necesarios.

Un trabajador de la empresa informática se dirige a la clínica y mantiene una entrevista con el titular de la misma, quien le informa de los siguientes aspectos:

El personal de la clínica está formado por: el titular, médico especialista en odontología. Como contratados: otro odontólogo, dos auxiliares de clínica y un auxiliar administrativo, que también ejerce como recepcionista, y una persona para la limpieza.

La clínica cuenta con dos consultas, cada una de ellas con un especialista en odontología. En cada consulta hay un ordenador desde el que pueden consultar la base de datos de pacientes tanto el especialista como el auxiliar de clínica que trabaja en esa consulta. En recepción hay otro ordenador con un programa de tipo agenda para consultar las horas libres y anotar las citas. En un despacho aparte están los archivos en soporte papel y donde se encuentra el servidor.

Todos los ordenadores tienen sistema operativo Windows, excepto el servidor que es Linux.

El objetivo de la clínica es proteger la información, especialmente la relativa a los historiales médicos de sus pacientes.

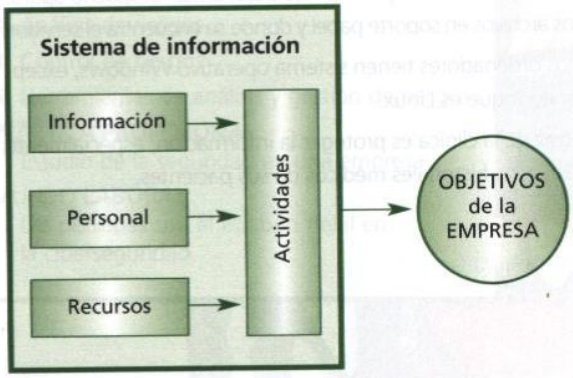
estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Elabora un listado de los activos de la clínica.
   - ¿Cuáles son los activos?
2. Observa qué sistemas de seguridad física y lógica están protegiendo actualmente el sistema. Si están revisados y actualizados.
   - ¿Qué es seguridad física y lógica?
3. Comprueba cuáles son las vulnerabilidades del sistema informático, tanto en el software, como en el hardware, el personal y las instalaciones.
   - ¿Qué propiedades debe tener el sistema de información para ser seguro?
   - ¿Qué amenazas y riesgos existen?
   - ¿Qué vulnerabilidades tiene el sistema?
4. Elabora una lista de servicios y mecanismos que incrementarían la seguridad de la información.
   - ¿Qué servicios de seguridad se necesitan y qué mecanismos son necesarios para asegurar esos servicios?
5. Investiga si la clínica dispone de una política de seguridad o de un plan de contingencias.
   - ¿Está informado todo el personal de la política de seguridad?
   - ¿Se realizan ensayos y simulacros según el plan de contingencias?
6. Determina si la clínica requiere una auditoría informática.
   - ¿En qué consistirá la auditoría?
   - ¿Se realizará con algún software específico para auditoría informática?

1. Sistemas de información y sistemas informáticos

Un **sistema de información** (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus **objetivos.**

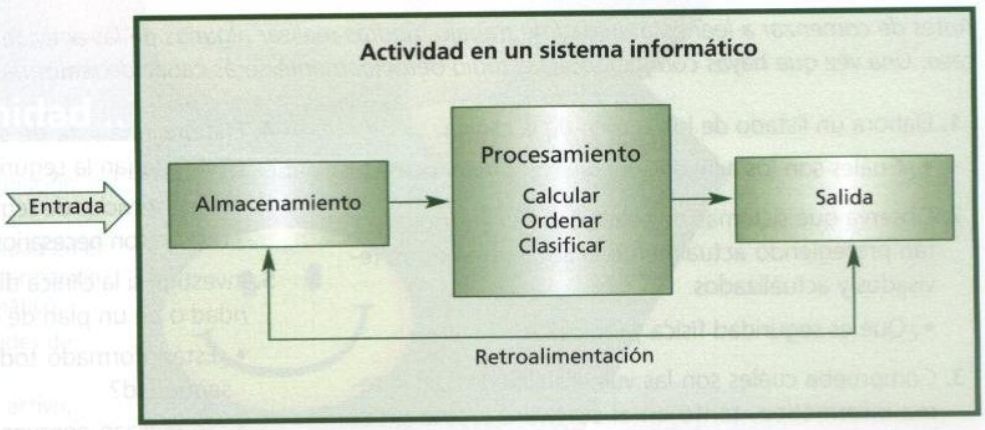


Estos elementos son:

- **Recursos.** Pueden ser físicos, como ordenadores, componentes, periféricos y conexiones, recursos no informáticos; y lógicos, como sistemas operativos y aplicaciones informáticas.
- **Equipo humano.** Compuesto por las personas que trabajan para la organización.
- **Información.** Conjunto de datos organizados que tienen un significado. La información puede estar contenida en cualquier tipo de soporte.
- **Actividades** que se realizan en la organización, relacionadas o no con la informática.

Sistemas informáticos

Un **sistema informático** está constituido por un conjunto de elementos **físicos** (hardware, dispositivos, periféricos y conexiones), **lógicos** (sistemas operativos, aplicaciones, protocolos...) y con frecuencia se incluyen también los elementos **humanos** (personal experto que maneja el software y el hardware).



Un sistema informático puede ser un subconjunto del sistema de información, pero en principio un sistema de información no tiene por qué contener elementos informáticos, aunque en la actualidad es difícil imaginar cualquier actividad humana en la que no se utilice la informática. A lo largo de este libro estudiaremos la seguridad en los sistemas de información, en general, y en los sistemas informáticos, en particular, como parte de aquellos.

2. Seguridad

2.1. Aproximación al concepto de seguridad en sistemas de información

Una de las acepciones de la RAE para el término seguro, que es la que aquí nos interesa, es la de estar **libre y exento de todo peligro, daño o riesgo.** Este es el concepto en el que se basa el contenido de este libro y tiene el mismo sentido aplicado a sistemas de información y sistemas informáticos.

↑ Sistema seguro.

La **seguridad informática** es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Un sistema de información, no obstante las medidas de seguridad que se le apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad en necesario conocer:

- Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- Cuáles son los **peligros** que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aportados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreos sobre el mismo.
- Cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas.

Todos los elementos que participan en un sistema de información pueden verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable. El hardware y otros elementos físicos se pueden volver a comprar o restaurar, el software puede ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano.

Seguridad informática

"Lo que no está permitido debe estar prohibido"

2.2. Tipos de seguridad

Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos.

2.3. Propiedades de un sistema de información seguro

Los daños producidos por falta de seguridad pueden causar pérdidas económicas o de credibilidad y prestigio a una organización.

Su **origen** puede ser:

- **Fortuito.** Errores cometidos accidentalmente por los usuarios, accidentes, cortes de fluido eléctrico, averías del sistema, catástrofes naturales...
- **Fraudulento.** Daños causados por software malicioso, intrusos o por la mala voluntad de algún miembro del personal con acceso al sistema, robo o accidentes provocados.

caso **práctico** inicial

Integridad, confidencialidad y disponibilidad de los datos son las propiedades que debería tener un sistema considerado seguro.

Se considera seguro un sistema que cumple con las propiedades de **integridad, confidencialidad** y **disponibilidad** de la información. Cada una de estas propiedades conlleva la implantación de determinados servicios y mecanismos de seguridad que se estudiarán más adelante.

Integridad

Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que esta se solicita, o dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado.

Para evitar este tipo de riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto.

Confidencialidad

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como «el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada».

Para prevenir errores de confidencialidad debe diseñarse un control de accesos al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones.

Disponibilidad

La información ha de estar disponible para los usuarios autorizados cuando la necesiten.

El programa MAGERIT define la disponibilidad como «grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información».

Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionadamente se hubiesen dañado o destruido.

saber más

MAGERIT

Es una metodología de análisis y gestión de riesgos de los sistemas de información. En inglés *Methodology for Information Systems Risk Analysis and Management.*

ACTIVIDADES

1. La biblioteca pública de una ciudad tiene mobiliario, libros, revistas, microfilms, varios ordenadores para los usuarios en donde pueden consultar libros electrónicos, y un ordenador en el que la bibliotecaria consulta títulos, códigos, referencias y ubicación del material bibliográfico.

   Indica a continuación de cada elemento con un **sí**, si forma parte del sistema informático de la biblioteca y con un **no** si no forma parte de él:

   a) Libros y revistas colocados en las estanterías.

   b) Mobiliario.

   c) Microfilms.

   d) Libros electrónicos.

   e) Ordenadores de los usuarios.

   f) Ordenador de la bibliotecaria.

   g) Datos almacenados en el ordenador de la bibliotecaria.

   h) Bibliotecaria.

2. De los elementos relacionados en la pregunta anterior, ¿cuáles pertenecen al sistema de información de la biblioteca?

3. Un incendio fortuito destruye completamente todos los recursos de la biblioteca. ¿En qué grado crees que se verían comprometidas la integridad, la confidencialidad y la disponibilidad de la información?

4. El informático que trabaja para la biblioteca, ¿forma parte del sistema informático de la misma?

5. El ordenador de la biblioteca tiene un antivirus instalado, ¿esto lo hace invulnerable?

6. ¿A qué se deben la mayoría de los fallos de seguridad? Razona tu respuesta.

7. ¿Podrías leer un mensaje encriptado que no va dirigido a ti? Busca en internet algunos programas que encriptan mensajes.

8. ¿La copia de seguridad es una medida de seguridad pasiva?

9. ¿Qué propiedades debe cumplir un sistema seguro?

10. ¿Qué garantiza la integridad?

3. Análisis de riesgos

A la hora de dotar de seguridad a un sistema de información, hay que tener en cuenta todos los elementos que lo componen, analizar el nivel de vulnerabilidad de cada uno de ellos ante determinadas amenazas y valorar el impacto que un ataque causaría sobre todo el sistema.

«La cadena siempre se rompe por el eslabón más débil».

La persona o el equipo encargado de la seguridad deberá analizar con esmero cada uno de los elementos. A veces el descuido de un elemento considerado débil ha producido importantes fallos de seguridad. Al estar interrelacionados todos los elementos este descuido puede producir errores en cadena con efectos insospechados sobre la organización.

3.1. Elementos de estudio

Para comenzar a analizar un sistema de información al que se pretende dotar de unas medidas de seguridad, hay que tener en cuenta los siguientes elementos: activos, amenazas, riesgos, vulnerabilidades, ataques e impactos.

Activos

caso **práctico** inicial

Los activos de un sistema de información: datos, software, hardware y sus accesorios, redes, soportes, instalaciones, personal y servicios.

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen: cómo afectaría en uno de ellos un daño ocurrido a otro.

Podemos clasificarlos en los siguientes tipos:

- **Datos.** Constituyen el núcleo de toda organización, hasta tal punto que se tiende a considerar que el resto de los activos están al servicio de la protección de los datos. Normalmente están organizados en bases de datos y almacenados en soportes de diferente tipo. El funcionamiento de una empresa u organización depende de sus datos, que pueden ser de todo tipo: económicos, fiscales, de recursos humanos, clientes o proveedores…

  Cada tipo de dato merece un estudio independiente de riesgo por la repercusión que su deterioro o pérdida pueda causar, como por ejemplo los relativos a la intimidad y honor de las personas u otros de índole confidencial.

- **Software.** Constituido por los sistemas operativos y el conjunto de aplicaciones instaladas en los equipos de un sistema de información que reciben y gestionan o transforman los datos para darles el fin que se tenga establecido.

- **Hardware.** Se trata de los equipos (servidores y terminales) que contienen las aplicaciones y permiten su funcionamiento, a la vez que almacenan los datos del sistema de información. Incluimos en este grupo los periféricos y elementos accesorios que sirven para asegurar el correcto funcionamiento de los equipos o servir de vía de transmisión de los datos (módem, router, instalación eléctrica o sistemas de alimentación ininterrumpida, destructores de soportes informáticos…).

- **Redes.** Desde las redes locales de la propia organización hasta las metropolitanas o internet. Representan la vía de comunicación y transmisión de datos a distancia.
- **Soportes.** Los lugares en donde la información queda registrada y almacenada durante largos períodos o de forma permanente (DVD, CD, tarjetas de memoria, discos duros externos dedicados al almacenamiento, microfilms e incluso papel).
- **Instalaciones.** Son los lugares que albergan los sistemas de información y de comunicaciones. Normalmente se trata de oficinas, despachos, locales o edificios, pero también pueden ser vehículos y otros medios de desplazamiento.
- **Personal.** El conjunto de personas que interactúan con el sistema de información: administradores, programadores, usuarios internos y externos y resto de personal de la empresa. Los estudios calculan que se producen más fallos de seguridad por intervención del factor humano que por fallos en la tecnología.
- **Servicios** que se ofrecen a clientes o usuarios: productos, servicios, sitios web, foros, correo electrónico y otros servicios de comunicaciones, información, seguridad, etc.

Amenazas

En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que –de tener la oportunidad– atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus, troyanos, gusanos) o el robo, destrucción o modificación de la información.

caso **práctico** inicial

Identificar las amenazas y las vulnerabilidades del sistema permitirá conocer los riesgos potenciales que amenazan la seguridad de un sistema.

En función del tipo de alteración, daño o intervención que **podrían producir sobre la información,** las amenazas se clasifican en cuatro grupos:

- **De interrupción.** El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.
- **De interceptación.** Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.
- **De modificación.** Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.
- **De fabricación.** Agregarían información falsa en el conjunto de información del sistema.

Según su **origen** las amenazas se clasifican en:

- **Accidentales.** Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.
- **Intencionadas.** Son debidas siempre a la acción humana, como la introducción de software malicioso –malware– (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa la introducción de malware en los equipos), robos o hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

Riesgos

Se denomina riesgo a la posibilidad de que se materialice o no una **amenaza** aprovechando una **vulnerabilidad.** No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

Vulnerabilidades

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son vulnerables a la acción de los *hackers*, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

Ataques

Se dice que se ha producido un ataque **accidental** o **deliberado** contra el sistema cuando se ha materializado una amenaza.

En función del impacto causado a los activos atacados, los ataques se clasifican en:

- **Activos.** Si modifican, dañan, suprimen o agregan información, o bien bloquean o saturan los canales de comunicación.
- **Pasivos.** Solamente acceden sin autorización a los datos contenidos en el sistema. Son los más difíciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento «víctima» directamente, o a través de recursos o personas intermediarias.

saber más

Algunos tipos de malware:

- Backdoor
- Botnet (Zombies)
- Exploit
- Gusano
- Hoax
- Keylogger
- Phishing
- Rogue
- Rootkit
- Spam
- Spyware/Adware
- Troyano

saber más

Algunos tipos de intrusos informáticos:

- Hacker
- Cracker
- Lamer
- CopyHacker
- Bucanero
- Phreaker
- Newbie
- Script Kiddie

saber más

El ataque cometido por parte de un *hacker* que utiliza ordenadores intermediarios para ocultar la propia identidad (IP) hasta llegar a su objetivo es un ataque indirecto.

Impactos

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado.

Los impactos pueden ser **cuantitativos**, si los perjuicios pueden cuantificarse económicamente, o **cualitativos,** si suponen daños no cuantificables, como los causados contra los derechos fundamentales de las personas.

3.2. Proceso del análisis de riesgos

Para implantar una política de seguridad en un sistema de información es necesario seguir un esquema lógico.

- Hacer inventario y valoración de los activos.
- Identificar y valorar las amenazas que puedan afectar a la seguridad de los activos.
- Identificar y evaluar las medidas de seguridad existentes.
- Identificar y valorar las vulnerabilidades de los activos a las amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.
- Determinar sistemas de medición de riesgos.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección.

caso práctico inicial

Analizar los riesgos de un sistema de información requiere un proceso secuencial de análisis de activos, sus vulnerabilidades, amenazas que existen, medidas de seguridad existentes, impacto que causaría un determinado ataque sobre cualquiera de los activos, objetivos de seguridad de la empresa y selección de medidas de protección que cubran los objetivos.

ACTIVIDADES

11. La ventana de un centro de cálculo en donde se encuentran la mayor parte de los ordenadores y el servidor de una organización se quedó mal cerrada. Durante una noche de tormenta, la ventana abierta ¿constituye un riesgo, una amenaza o una vulnerabilidad? Razona la respuesta.

12. Teniendo en cuenta las propiedades de integridad, disponibilidad y confidencialidad, indica cuáles de estas propiedades se verían afectadas por:

a) Una amenaza de interrupción.

b) Una amenaza de interceptación.

c) Una amenaza de modificación.

d) Una amenaza de fabricación.

13. Pon un ejemplo de cómo un sistema de información podría ser seriamente dañado por la presencia de un factor que se considera de poca relevancia y que explique de alguna manera que «La cadena siempre se rompe por el eslabón más débil».

14. ¿Qué elementos se estudian para hacer un análisis de riesgos?

4. Control de riesgos

Una vez que se ha realizado el análisis de riesgos se tiene que determinar cuáles serán los **servicios** necesarios para conseguir un sistema de información seguro (epígrafe 2.3). Para poder dar esos servicios será necesario dotar al sistema de los **mecanismos** correspondientes.

4.1. Servicios de seguridad

Integridad

Asegura que los datos del sistema no han sido alterados ni cancelados por personas o entidades no autorizadas y que el contenido de los mensajes recibidos es el correcto.

↑ Confidencialidad.

Confidencialidad

Proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

Disponibilidad

Permitirá que la información esté disponible cuando lo requieran las entidades autorizadas.

↑ Autenticación.

Autenticación (o identificación)

El sistema debe ser capaz de verificar que un usuario identificado que accede a un sistema o que genera una determinada información es quien dice ser. Solo cuando un usuario o entidad ha sido autenticado, podrá tener autorización de acceso. Se puede exigir autenticación en la entidad de origen de la información, en la de destino o en ambas.

No repudio (o irrenunciabilidad)

Proporcionará al sistema una serie de evidencias irrefutables de la autoría de un hecho.

El **no repudio** consiste en no poder negar haber emitido una información que sí se emitió y en no poder negar su recepción cuando sí ha sido recibida.

De esto se deduce que el **no repudio** puede darse:

- **En origen.** El emisor no puede negar el envío porque el receptor tiene pruebas certificadas del envío y de la identidad del emisor. Las pruebas son emitidas por el propio emisor.
- **En destino.** En este caso es el destinatario quien no puede negar haber recibido el envío ya que el emisor tiene pruebas infalsificables del envío y de la identidad del destinatario. Es el receptor quien crea las pruebas.

Control de acceso

Podrán acceder a los recursos del sistema solamente el personal y usuarios con autorización.

caso práctico inicial

Cuando se realiza un análisis de riesgos, hay que detectar qué servicios de seguridad cumple el sistema de información y cuáles quedan descubiertos o incompletos para poder aplicar los mecanismos necesarios que aseguren la consecución de los objetivos de seguridad de la organización

4.2. Mecanismos de seguridad

Según la función que desempeñen los mecanismos de seguridad pueden clasificarse en:

- **Preventivos.** Actúan antes de que se produzca un ataque. Su misión es evitarlo.
- **Detectores.** Actúan cuando el ataque se ha producido y antes de que cause daños en el sistema.
- **Correctores.** Actúan después de que haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

Cada mecanismo ofrece al sistema uno o más **servicios** de los especificados en el epígrafe anterior.

Existen muchos y variados mecanismos de seguridad. En esta sección se mencionan los más habituales, que se detallarán en otras unidades didácticas.

La elección de mecanismos de seguridad depende de cada sistema de información, de su función, de las posibilidades económicas de la organización y de cuáles sean los riesgos a los que esté expuesto el sistema.

caso **práctico** inicial

Hablamos de seguridad física o seguridad lógica según que el mecanismo utilizado para ofrecer seguridad sea físico o lógico.

caso **práctico** inicial

Los mecanismos físicos o lógicos de seguridad tienen como misión prevenir, detectar o corregir ataques al sistema, asegurando que los servicios de seguridad queden cubiertos.

Seguridad lógica

Los mecanismos y herramientas de seguridad lógica tienen como objetivo proteger digitalmente la información de manera directa.

- **Control de acceso** mediante nombres de usuario y contraseñas.
- **Cifrado de datos** (encriptación). Los datos se enmascaran con una clave especial creada mediante un algoritmo de encriptación. Emisor y receptor son conocedores de la clave y a la llegada del mensaje se produce el descifrado. El cifrado de datos fortalece la confidencialidad.
- **Antivirus.** Detectan e impiden la entrada de virus y otro software malicioso. En el caso de infección tienen la capacidad de eliminarlos y de corregir los daños que ocasionan en el sistema. Preventivo, detector y corrector. Protege la integridad de la información.
- **Cortafuegos** (*firewall*). Se trata de uno o más dispositivos de software, de hardware o mixtos que permiten, deniegan o restringen el acceso al sistema. Protege la integridad de la información.
- **Firma digital.** Se utiliza para la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos (por ejemplo, gestiones en oficinas virtuales). Su finalidad es identificar de forma segura a la persona o al equipo que se hace responsable del mensaje o del documento. Protege la integridad y la confidencialidad de la información.
- **Certificados digitales.** Son documentos digitales mediante los cuales una entidad autorizada garantiza que una persona o entidad es quien dice ser, avalada por la verificación de su clave pública. Protege la integridad y la confidencialidad de la información.

↑ Antivirus, seguridad lógica. Previenen, detectan y corrigen ataques al sistema informático.

↑ Firma digital.

Las redes inalámbricas (WiFi) necesitan precauciones adicionales para su protección:

- **Usar un SSID** *(Service Set Identifier)*, es decir, darle un nombre a la red, preferiblemente uno que no llame la atención de terceros que detecten esta red entre las disponibles. Cambiar con cierta frecuencia el SSID.
- **Protección de la red mediante claves encriptadas WEP** *(Wired Equivalent Privacy)* o **WPA** *(WiFi Protected Access)*. La clave WEP consume más recursos y es más fácilmente descifrable que la WPA y debería cambiarse con frecuencia. La WPA es de encriptación dinámica y mucho más segura al ser más difícil de descifrar. Cambiar periódicamente la contraseña de acceso a la red.
- **Filtrado de direcciones MAC** *(Media Access Control)*. Es un mecanismo de acceso al sistema mediante hardware, por el que se admiten solo determinadas direcciones, teniendo en cuenta que cada tarjeta de red tiene una dirección MAC única en el mundo. Puede resultar engorroso de configurar y no es infalible puesto que es posible disfrazar la dirección MAC real.

Detector de humos

SAI (Sistema de alimentación ininterrumpida)

↑ Elementos de seguridad física.

Seguridad física

Son tareas y mecanismos físicos cuyo objetivo es proteger al sistema (y, por tanto indirectamente a la información) de peligros físicos y lógicos.

- **Respaldo de datos.** Guardar copias de seguridad de la información del sistema en lugar seguro. Disponibilidad.
- **Dispositivos físicos** de protección, como pararrayos, detectores de humo y extintores, cortafuegos por hardware, alarmas contra intrusos, sistemas de alimentación ininterrumpida (para picos y cortes de corriente eléctrica) o mecanismos de protección contra instalaciones. En cuanto a las personas, acceso restringido a las instalaciones; por ejemplo, mediante vigilantes jurados o cualquier dispositivo que discrimine la entrada de personal a determinadas zonas.

ACTIVIDADES

15. Investiga el término *war driving,* que también puede expresarse como *wardriving* o *war xing*. ¿Crees que el *war driving* constituye un riesgo contra la confidencialidad?

16. ¿Qué relación hay entre servicios de seguridad y mecanismos de seguridad?

17. ¿Qué es el SSID de una red WiFi?

18. ¿Podrías explicar qué significa encriptar un mensaje? Inventa un sencillo sistema de encriptación (codificación). Imagina que envías a otra persona unas palabras codificadas según tu sistema inventado. ¿Qué necesita tener o saber la persona que recibe tu mensaje para poder descifrarlo?

19. De los siguientes dispositivos indica cuáles son preventivos, detectores o correctores:

a) Cortafuegos *(firewall)*.

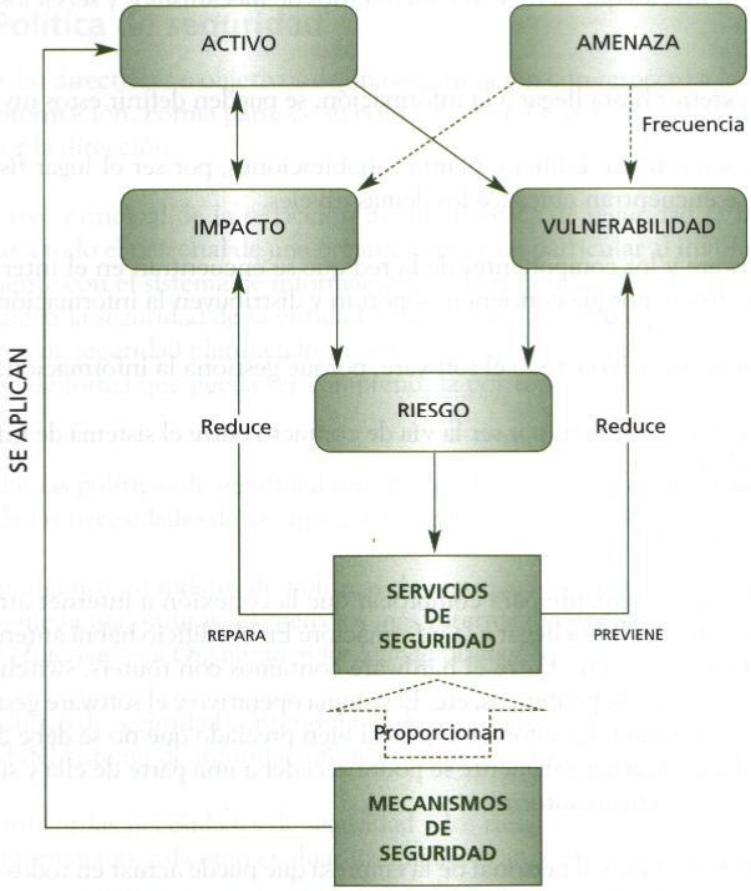
b) Antivirus.

c) Extintor de fuegos.

d) Detector de humos.

e) Firma digital.

En este gráfico se puede observar claramente la relación entre mecanismos y servicios de seguridad, y de ambos sobre los activos y los peligros que los acechan.



caso práctico inicial

Los mecanismos de seguridad proporcionan servicios de seguridad que reducen tanto las vulnerabilidades del sistema como la intensidad del impacto de posibles ataques a los activos.

ACTIVIDADES

20. Imagina esta situación: Quieres presentar a tu jefe una brillante idea que puede interesar a la competencia, pero te encuentras de fin de semana en un pueblecito donde los teléfonos móviles no funcionan, por suerte te has llevado tu portátil y el hotel rural donde te encuentras alojado dispone de servicio de internet. Así que decides enviarle un correo electrónico pero sin encriptar. Explica los peligros de este procedimiento.

21. Investiga qué es la esteganografía.

22. ¿Cómo escogerías una clave segura de acceso al ordenador de una empresa donde se guardan datos confidenciales de clientes?

23. Trabajas como técnico de informática y te llega una llamada de una oficina. Un empleado hacía cada semana una copia de seguridad de la carpeta Documentos Importantes. La copia la guardaba en otra partición del mismo disco duro. Una tormenta eléctrica ha dañado el disco y un experto en informática no ha hallado modo de restablecer su funcionamiento. Te piden que te acerques a la oficina para ver si existe la posibilidad de recuperar al menos los datos.

a) ¿Podrás recuperar los datos originales?

b) En su defecto, ¿podrán recuperarse los que hay en la copia de seguridad?

c) A tu juicio, ¿el empleado ha cometido alguna imprudencia con la copia de seguridad?

4.3. Enfoque global de la seguridad

recuerda

La seguridad de la información implica a todos los niveles que la rodean:

1. Edificio y habitaciones
2. Hardware y red interna
3. Sistema operativo y software
4. Conexión a Internet

En cada nivel intervienen personas.

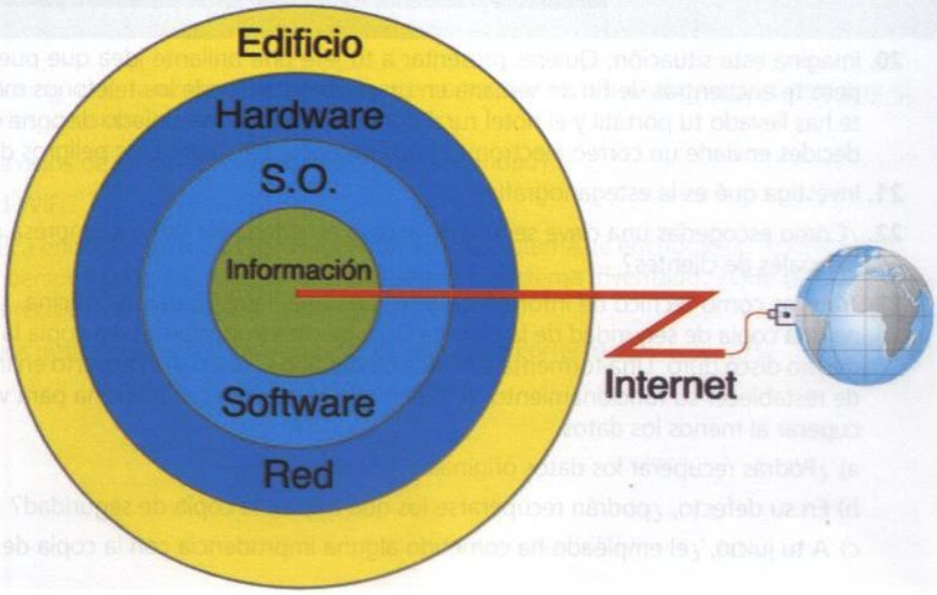
La información es el núcleo de todo sistema de información. Para proteger sus propiedades de integridad, disponibilidad y confidencialidad es necesario tener en cuenta a los niveles que la rodean para dotarlos de mecanismos y servicios de seguridad.

Desde el exterior hasta llegar a la información, se pueden definir estos niveles:

- La ubicación física. Edificio, planta o habitaciones, por ser el lugar físico en donde se encuentran ubicados los demás niveles.
- El hardware y los componentes de la red que se encuentran en el interior del entorno físico, porque contienen, soportan y distribuyen la información.
- El sistema operativo y todo el software, porque gestiona la información.
- La conexión a internet, por ser la vía de contacto entre el sistema de información y el exterior.
- La información.

Observa la figura siguiente para comprobar que la conexión a internet atraviesa los distintos niveles hasta llegar a la información: En el edificio habrá antenas, cableado en los muros, etc. Entre el hardware contamos con routers, switches, ordenadores, servidores, periféricos, etc. El sistema operativo y el software gestionan los accesos a internet. La información es el bien preciado que no se debe descuidar, pues desde internet solamente se podrá acceder a una parte de ella y siempre que los usuarios tengan autorización.

Una vez más aludimos al personal de la empresa que puede actuar en todos los niveles o en parte de ellos y por lo tanto es un factor a tener en cuenta.



5. Herramientas de análisis y gestión de riesgos

5.1. Política de seguridad

Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección.

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de seguridad planificados. Por tanto, la política de seguridad deberá redactarse de forma que pueda ser comprendida por todo el personal de una organización.

No todas las políticas de seguridad son iguales. El contenido depende de la realidad y de las necesidades de la organización para la que se elabora.

Existen algunos estándares de políticas de seguridad por países y por áreas (gobierno, medicina, militar...), pero los más internacionales son los definidos por la ISO (*International Organization for Standardization*).

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así como evaluar los impactos ante un eventual ataque.
- Relacionar todas las medidas de seguridad que deben implementarse para afrontar los riesgos de cada activo o grupo de activos.
- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización
- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
- Definir un plan de contingencias.

caso práctico inicial

Los objetivos y normas de seguridad están recogidos en la política de seguridad de la organización. Para la consecución de objetivos, el personal debe estar informado de cuál es la política de seguridad de la empresa.

EJEMPLOS DE HERRAMIENTAS DE ANÁLISIS Y GESTIÓN DE RIESGOS

MAGERIT. Es una metodología de análisis y gestión de riesgos de los sistemas de información. En inglés *Methodology for Information Systems Risk Analysis and Management.*

PILAR. Es un procedimiento informático-lógico para el análisis y gestión de riesgos, que sigue la metodología MAGERIT. De uso exclusivo de la Administración Pública Española.

5.2. Auditoría

caso práctico inicial

La auditoría, mediante pruebas analíticas sobre los activos y procesos que desarrolla la organización, descubre vulnerabilidades, establece medidas de protección y analiza periódicamente el sistema de información para detectar los riesgos no contemplados o de nueva aparición.

El estudio puede realizarse mediante software específico para auditoría de sistemas.

La auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Su finalidad es verificar que se cumplen los objetivos de la **política de seguridad** de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información.

Tras el análisis e identificación de vulnerabilidades, la persona o equipo encargado de la auditoría emite un **informe** que contiene, como mínimo:

- Descripción y características de los **activos** y **procesos** analizados.
- Análisis de las **relaciones y dependencias** entre activos o en el proceso de la información.
- Relación y evaluación de las **vulnerabilidades** detectadas en cada activo o subconjunto de activos y procesos.
- Verificación del cumplimiento de la **normativa** en el ámbito de la seguridad.
- Propuesta de **medidas** preventivas y de corrección.

Para evaluar la seguridad de un sistema de información se necesitan herramientas de análisis:

- **Manuales.** Observación de los activos, procesos y comportamientos, mediciones, entrevistas, cuestionarios, cálculos, pruebas de funcionamiento.
- **Software específico para auditoría.** Se le reconoce por las siglas CAAT *(Computer Assisted Audit Techniques)*. Los CAATS son herramientas de gran ayuda para mejorar la eficiencia de una auditoría, pudiendo aplicarse sobre la totalidad o sobre una parte del sistema de información. Proporcionan una imagen en tiempo real del sistema de información, realizan pruebas de control y emiten informes en los que señalizan las vulnerabilidades y puntos débiles del sistema, así como las normativas que podrían estar incumpliéndose.

saber más

Software de auditoría

- CaseWare
- WizSoft
- Ecora
- ACL

La auditoría puede ser **total,** sobre todo el sistema de información, o **parcial,** sobre determinados activos o procesos.

La auditoría de un sistema de información puede realizarse:

- Por personal capacitado perteneciente a la propia empresa.
- Por una empresa externa especializada.

ACTIVIDADES

24. Investiga qué es un test de intrusión.

25. Tu jefe te dice que ha detectado que el rendimiento de los trabajadores ha bajado considerablemente desde que la empresa tiene acceso a internet. Te pide que le propongas una solución.

26. En tu empresa acaban de crear unas claves de seguridad para los empleados. Dichas claves se envían por correo electrónico. ¿Esto es desconocimiento de las prácticas de seguridad?

5.3. Plan de contingencias

Determinadas amenazas a cualquiera de los activos del sistema de información pueden poner en peligro la continuidad de un negocio. El plan de contingencias es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto.

El plan de contingencias consta de tres subplanes independientes:

- **Plan de respaldo.** Ante una amenaza, se aplican medidas preventivas para evitar que se produzca un daño. Por ejemplo, crear y conservar en lugar seguro copias de seguridad de la información, instalar pararrayos o hacer simulacros de incendio.
- **Plan de emergencia.** Contempla qué medidas tomar cuando se está materializando una amenaza o cuando acaba de producirse. Por ejemplo, restaurar de inmediato las copias de seguridad o activar el sistema automático de extinción de incendios.
- **Plan de recuperación.** Indica las medidas que se aplicarán cuando se ha producido un desastre. El objetivo es evaluar el impacto y regresar lo antes posible a un estado normal de funcionamiento del sistema y de la organización. Por ejemplo, tener un lugar alternativo donde continuar la actividad si el habitual hubiese sido destruido, sustituir el material deteriorado, reinstalar aplicaciones y restaurar copias de seguridad.

La elaboración del plan de contingencias no puede descuidar al personal de la organización, que estará informado del plan y entrenado para actuar en las funciones que le hayan sido encomendadas en caso de producirse una amenaza o un impacto.

caso práctico inicial

El plan de contingencias contiene medidas preventivas, paliativas y de recuperación de desastres.

El personal no solamente debe estar informado del plan de contingencias sino preparado para actuar ante un peligro o un desastre. Ejemplo: simulacros de incendio.

ACTIVIDADES

27. El hecho de preparar un plan de contingencias, ¿implica un reconocimiento de la ineficiencia en la gestión de la empresa?

28. ¿Cuál es la orientación principal de un plan de contingencia?

29. Investiga: diferencias entre redes cableadas y redes inalámbricas WIFI.

30. ¿En qué se basa la recuperación de la información?

31. Tu jefe te pide que le hagas una buena política de copias de seguridad para que sea seguida por todos los trabajadores de la empresa. ¿Qué deberá contemplar?

32. Trabajas en una empresa donde además de la oficina central, hay una red de oficinas por varias ciudades. Se elabora un plan de contingencias exclusivamente para la oficina central, ¿es esto correcto?

33. En tu empresa se desarrolla un plan de contingencias que entre otras muchas situaciones, cubre las siguientes: un corte en la corriente eléctrica, el sol pasando a través de un cristal en pleno agosto, derramar una bebida en el teclado o sobre el monitor, olvidarse el portátil en un taxi, el robo del ordenador.

¿Crees que cubrir estos puntos es acertado?

5.4. Modelos de seguridad

Un modelo de seguridad es la expresión formal de una política de seguridad y se utiliza como directriz para evaluar los sistemas de información. Al decir formal queremos expresar que estará redactado fundamentalmente en términos técnicos y matemáticos.

Clasificación

En relación a las funciones u operaciones sobre las que se ejerce mayor control podemos clasificar los modelos de seguridad en tres grandes grupos:

- **Matriz de acceso.** Este modelo considera tres elementos básicos: sujeto, objeto y tipo de acceso. Un sujeto tiene autorización de acceso total o parcial a uno o más objetos del sistema. Aplicable a cualquier sistema de información, controla tanto la confidencialidad como la integridad de los datos.
- **Acceso basado en funciones de control** (RBAC –*Role-Access Base Control*–). Puede considerarse una modalidad del de matriz de acceso, pero, en este caso, el acceso no se define en función de quién es el sujeto, sino de qué función tiene. Por ejemplo, un determinado individuo puede ser alumno de una universidad en cuanto que está estudiando una carrera, pero también puede ser profesor de la universidad en otra especialidad distinta de la misma universidad. Tratándose del mismo individuo, en calidad de profesor tendrá un tipo de acceso al sistema y en calidad de alumno tendrá otro. También controla la confidencialidad y la integridad de los datos.
- **Multinivel.** Este modelo se basa en la jerarquización de los datos (todos los datos son importantes pero unos son más privados que otros. Por ejemplo, el nivel de protección de datos personales ha de ser superior que los nombres de los artículos con los que comercia una empresa). Los usuarios tendrán acceso a un nivel u otro de la jerarquía en función de las autorizaciones que les hayan sido dadas. Este nivel controla el flujo de datos entre los niveles de la jerarquía. Ejemplos de este grupo son el modelo *Bell-LaPadula* (controla la confidencialidad) y el modelo *Biba* (controla la integridad).

ACTIVIDADES

34. ¿Una misma política de seguridad puede servir a todo tipo de empresas?

35. ¿De qué modo debe ser redactada la política de seguridad de una organización?

36. Define con tus propias palabras qué es un plan de contingencias.

37. Investiga en internet sobre empresas especializadas en auditorías de sistemas de información (sugerencias: Hipasec, Audisis). Escoge una de estas empresas y contesta las siguientes preguntas:

a) ¿En qué fases realiza la auditoría?

b) ¿Qué tipos de auditoría realiza?

c) ¿Ofrece revisiones periódicas del sistema?

38. Investiga en internet para encontrar el software de auditoría: CaseWare, WizSoft, Ecora, ACL, AUDAP u otros. Escoge uno o varios y haz una lista de las operaciones que realiza para llevar a cabo la auditoría.

39. Averigua qué información tiene wikipedia sobre el modelo de seguridad Bell-LaPadula. Escribe la definición que hace del modelo.

PRÁCTICA PROFESIONAL

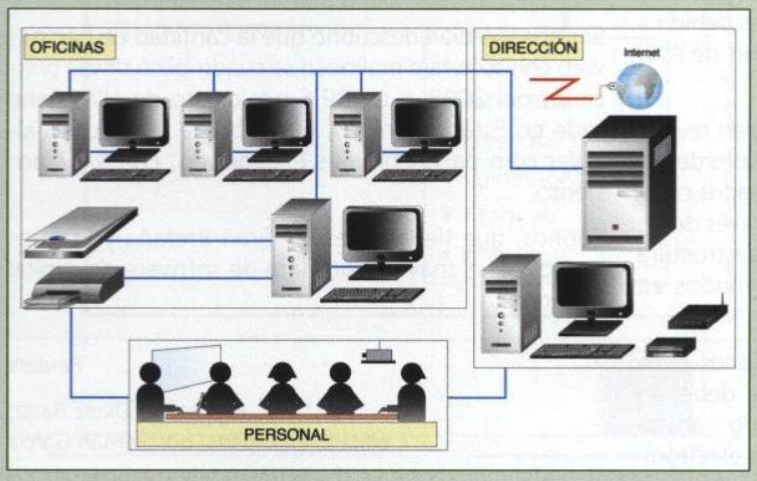
Estudio de la seguridad en una empresa

Empresa: asesoría laboral y fiscal.

Instalaciones: una oficina, una sala de reuniones y el despacho de dirección. Protección contra incendios y alarma contra intrusos.

Oficina: cuatro ordenadores en la oficina. Uno de ellos tiene conectados dos periféricos: una impresora y un escáner. Todos los ordenadores van conectados mediante cable a un servidor.

Dirección: un ordenador con conexión inalámbrica a la red. Un servidor conectado a internet. Además, en dirección se encuentra el archivo de todas las copias de seguridad de los datos, que se generan una vez al día.



Sala de reuniones: mesa y sillas para reuniones, un portátil, pantalla y proyector.

Recursos humanos: cinco personas, de ellas cuatro trabajan en la oficina; la directora de la asesoría, en su despacho.

Software: sistemas operativos, aplicaciones específicas para gestorías y asesorías, antivirus, *firewall*.

Situación: la asesoría tiene definida su política de seguridad, conocida por todo el personal. Recientemente le ha sido realizada una auditoría informática, y el estado de seguridad ha sido calificado como óptimo. Sin embargo, el ordenador de la dirección, debido a un pico de corriente, ha sufrido daños en la placa base y el disco duro. Ambos elementos deben ser reemplazados. La información contenida en el disco duro había sido previamente copiada y se encuentra archivada.

Resuelve

Con los conocimientos que posees tras haber estudiado esta unidad:

1. Enumera los activos del sistema de información de la asesoría.
2. ¿Se ha producido algún ataque? En caso afirmativo, responde cuál ha sido.
3. ¿Crees que ha sido importante para la empresa el impacto por los daños en la placa base y el disco duro? Comenta tu impresión.
4. Investiga si existe algún medio para evitar que los picos de corriente puedan dañar equipos o dispositivos físicos de un sistema informático.
5. El disco duro inutilizado contenía información personal y fiscal de clientes de la asesoría. Se ha decidido tirarlo a la basura, pero una empleada dice que ese método no es seguro. Haz tus investigaciones y comenta si has averiguado que la empleada está o no en lo cierto.

MUNDO LABORAL

Las personas son el eslabón débil en la ciberseguridad

La popularidad de Facebook y otros sitios muy visitados de redes sociales ha dado a los *hackers* nuevas vías para robar dinero e información, dijo la compañía de seguridad Sophos en un reporte publicado el miércoles.

Cerca de la mitad de las compañías bloquea parcial o completamente el acceso a las redes sociales debido a la preocupación por ciber-incursiones a través de esos sitios, de acuerdo al estudio.

«Los resultados de las investigaciones también revelaron que un 63 por ciento de los administradores de sistemas están preocupados porque sus empleados comparten demasiada información personal a través de los sitios de redes sociales, lo que pone su infraestructura corporativa –y los datos sensibles almacenados en ella– en riesgo», dijo el reporte de Sophos.

Esto ocurre a pesar de años de exhortaciones a los usuarios de computadoras respecto a que deberían mantener su información personal en privado y abstenerse de abrir archivos adjuntos de correos electrónicos provenientes de fuentes no conocidas.

Uno de los resultados es que una cuarta parte de los negocios ha sido afectada por tácticas como el *spam*, el *phishing* o ataques de software malicioso a través de Twitter u otras redes sociales, dijo Sophos.

El *phishing* es el envío de correos electrónicos a través de los cuales los estafadores tratan de convencer a sus potenciales víctimas para que revelen información personal como contraseñas o cuentas bancarias.

Sophos también descubrió que la cantidad de páginas web con software malicioso se cuadruplicó desde principios del 2008, y un 39,6 por ciento de ellas tiene sede en Estados Unidos, que alberga más que cualquier otro país. China es el segundo, con 14,7 por ciento.

Sophos, que tiene sedes en Gran Bretaña y Estados Unidos, es el mayor fabricante de software de capital privado.

Reuters

Reporte de Diane Bartz;
editado en español por Hernán García

http://lta.reuters.com/article/internetNews/idLTASIE56L08920090722

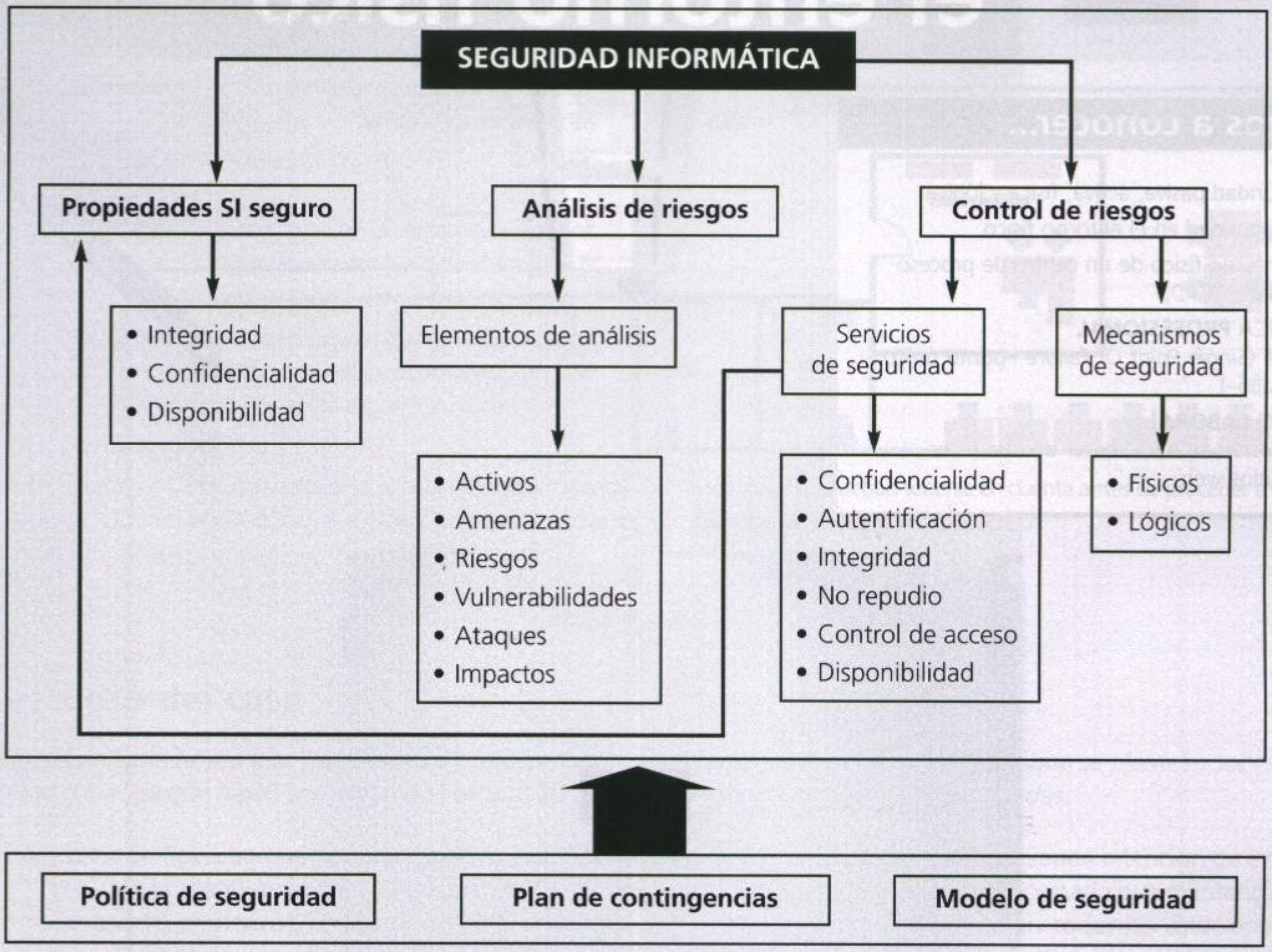
Washington, miércoles 22 de julio de 2009

Actividades

Lee el artículo y en vista de su contenido responde a las siguientes cuestiones:

1. ¿Qué propiedades de seguridad del sistema de información podrían verse vulneradas por negligencias cometidas por empleados de la empresa al publicar sus datos personales en redes sociales?
2. Indica alguna manera de que los administradores de un sistema de información puedan impedir que el personal de la empresa acceda a sitios que podrían poner en peligro las propiedades de seguridad del sistema.
3. ¿Qué proporción de negocios se ven afectados por *spam* o software malicioso debido al uso indebido de redes sociales por parte de los empleados?
4. En tu opinión, ¿consideras cierta la afirmación de que se producen más fallos de seguridad por la intervención humana que por errores en la tecnología?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. El conjunto de datos organizados que tienen significado se llama:
   a) Recurso.
   b) Actividad.
   c) Software.
   d) Información.
2. Señala cuál de estos elementos no forma parte de un sistema informático:
   a) Router.
   b) Usuario.
   c) Teclado.
   d) Estante.
3. Señala, en la siguiente lista, lo que es un activo:
   a) Inundación.
   b) Riesgo.
   c) Red local.
   d) Política de seguridad.
4. Indica la respuesta correcta que te sugiera la palabra disponibilidad:
   a) Asegura que los datos no han sido modificados.
   b) Protección contra la revelación de datos.
   c) Identifica personas.
   d) Permite el acceso solo a usuarios con autorización.

Soluciones: 1d, 2d, 3c, 4d

2 Seguridad en el entorno físico

vamos a conocer...

1. Seguridad pasiva, activa, física y lógica
2. La seguridad en el entorno físico
3. El entorno físico de un centro de proceso de datos (CPD)

PRÁCTICA **PROFESIONAL**

SPOF (*Single Point Of Failure* –punto único de fallo–)

MUNDO **LABORAL**

Explosión en data center derriba miles de sitios web

y al finalizar esta unidad...

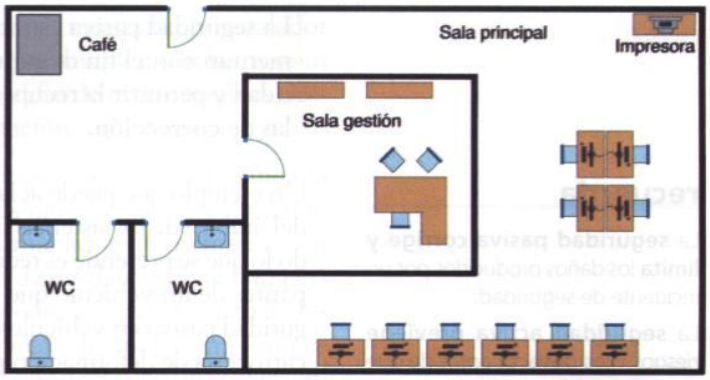
- Comprenderás la importancia de la seguridad en el entorno físico (estancias, plantas y edificios) de un sistema de información.
- Conocerás algunos sistemas de control de acceso a personas al recinto.
- Sabrás cuál es la temperatura y la humedad idóneas para las distintas áreas de equipamiento informático.
- Podrás conocer el riesgo del agua y del fuego y detectar si se han aplicado las medidas de seguridad activas y pasivas necesarias.
- Sabrás que es importante que un técnico informático conozca el estado en que se encuentra el recinto que aloja un sistema de información en cuanto a seguridad de los espacios físicos.

CASO **PRÁCTICO** INICIAL

situación de partida

Carlos trabaja como técnico montador de sistemas. En su localidad están montando un establecimiento para dar servicios de internet al público. El local está dividido en tres zonas distintas:

- Una sala central de gestión, con cristal antiasalto alrededor, en la que se va a instalar un servidor, un ordenador para la gestión del negocio y un escáner.
- Una más grande en la que se crearán diez espacios de acceso a internet con sus correspondientes ordenadores, una impresora en red y una máquina expendedora de cafés.
- La zona de lavabos.



Le han pedido a Carlos que visite el local para comprobar la seguridad de la instalación eléctrica y asesorar sobre otras medidas de seguridad que deban tenerse en cuenta antes de proceder a la instalación de los equipos y periféricos.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Carlos comprueba que la potencia de la electricidad contratada es suficiente para abastecer a todos los ordenadores, periféricos, iluminación, aire acondicionado y otros elementos menores. Sin embargo, le comentan que la instalación eléctrica es antigua, por lo que procede a comprobarlo y verifica que el cableado es suficiente pero que no dispone de toma de tierra.
   - ¿Por qué es importante la toma de tierra?
   - ¿Qué acción debe aconsejar Carlos a los dueños del local con respecto a la electricidad?
2. En cuanto a los lavabos, tienen recién instalada la fontanería y cuentan con un sumidero especial para fugas de agua. Ninguna tubería pasa por los muros que dan a la sala principal ni a la de gestión. Verifica también que las ventanas del local son solamente luminosas, que no se pueden abrir ni cerrar.
   - ¿Hay riesgo de inundaciones por el agua de los lavabos, por lluvia o tormentas?
   - ¿Dónde aconsejaría Carlos que se colocasen los ordenadores y periféricos, sobre el suelo o sobre alguna otra superficie?
3. Los propietarios del local tienen intención de instalar un aparato de aire acondicionado que mantenga una temperatura constante en todas las estaciones del año, y le preguntan a Carlos sobre la temperatura ideal para las personas y para los equipos informáticos a la vez.
   - ¿Qué temperatura es la adecuada dado que en todas las zonas del local habrá personas y ordenadores?
4. Por último, los dueños le preguntan a Carlos sobre qué otras medidas de seguridad deberían instalar en el local y en particular en la zona de gestión, dado que ahí se conservarán ficheros importantes con datos de clientes, proveedores, Administración pública, etc.
   - ¿Se debería contar con un extintor de incendios? ¿De qué tipo?
   - ¿Es necesario dotar al local de todas las medidas de seguridad que utilizaría un *Data Center* o CPD?
   - ¿Se debe restringir el acceso de personas al local? ¿Y a la sala de gestión?
   - ¿Se debería instalar una alarma? ¿De una o de más zonas activables?

1. Seguridad pasiva, activa, física y lógica

1.1. Seguridad pasiva

La seguridad pasiva está constituida por el conjunto de medidas que se implementan con el fin de minimizar la repercusión debida a un incidente de seguridad y permitir la recuperación del sistema. A estas medidas podemos llamarlas de **corrección.**

recuerda

La **seguridad pasiva corrige y limita** los daños producidos por un incidente de seguridad.

La **seguridad activa previene** riesgos y los **detecta** antes de que produzcan daños en el sistema.

Un ejemplo que puede aclarar el concepto de seguridad pasiva –aunque al margen del ámbito de los sistemas informáticos– podría ser la seguridad en carretera, cuando lo que se pretende es reducir el riesgo de lesiones y de muerte de las personas ocupantes de un vehículo que ha sufrido un accidente. Algunas de las medidas de seguridad pasiva en vehículos son los cinturones de seguridad, airbags, reposacabezas, carrocería de deformación programada o sistemas de seguridad para bebés.

La seguridad pasiva se aplica tanto a los elementos físicos del sistema de información, inclusive a las habitaciones, plantas o edificios en donde esté ubicado, como a los sistemas operativos, a las aplicaciones y a la información. Todos estos elementos del sistema pueden sufrir incidentes de seguridad y, por tanto, necesitan medidas de reparación y recuperación.

Los **mecanismos** y **servicios** que proporcionan seguridad pasiva en un sistema de información pueden ser de tipo físico y de tipo lógico.

1.2. Seguridad activa

Los mecanismos y procedimientos que permiten **prevenir** y **detectar** riesgos para la seguridad del sistema de información constituyen la seguridad activa del mismo.

recuerda

Las medidas de seguridad se han de aplicar atendiendo a las características de la organización que las demanda, a sus prioridades de seguridad y a su presupuesto económico.

Al igual que los mecanismos de seguridad pasiva, los de seguridad activa se aplican a la parte física y a la parte lógica del sistema de información y en todo caso pueden ser físicos y lógicos.

1.3. Seguridad física y seguridad lógica

saber más

También son entorno físico los equipos móviles (furgonetas, autobuses y otros vehículos) que llevan material informático en uso. Por ejemplo: vehículos de vigilancia, ambulancias, bibliotecas digitales móviles, etc.

Llamaremos **seguridad física** a la que tiene que ver con la protección de los elementos físicos de la empresa u organización, como el hardware y el lugar donde se realizan las actividades: edificio o habitaciones. **Seguridad lógica** es toda aquella relacionada con la protección del software y de los sistemas operativos, que en definitiva es la protección directa de los datos y de la información.

Existen unas medidas de seguridad elementales que ha de cumplir cualquier sistema informático o de información, desde el hogar hasta las macro empresas, pasando por las pequeñas y medianas empresas. Sin embargo, a mayor envergadura de la organización la información está mucho más comprometida pues comprende no solo la economía y los bienes y servicios, sino también la información relativa a personas que mantienen contacto con la empresa: personal, clientes, pacientes, proveedores…

2. La seguridad en el entorno físico

Se entiende por entorno físico la sala, conjunto de salas o edificio en el que se encuentran los equipos informáticos, el sistema de red y los periféricos.

El edificio cuenta con unas instalaciones que un técnico montador o instalador de sistemas informáticos debe conocer, para verificar que cumplen con las normas de seguridad y, en su caso, solicitar la reparación con el fin de evitar posibles riesgos futuros sobre el hardware, el software y la información.

No sirve de nada la aplicación de medidas de nivel lógico cuando se descuida la seguridad de las instalaciones físicas. Ha habido casos muy sonados en el mundo informático de empresas de cierta relevancia que contaban aparentemente con todas las salvaguardas imaginables para la protección de sus datos, y que han perdido buena parte de la información en un incendio producido en el recinto de los servidores. Al igual que un ladrón de información puede detenerse ante un potente sistema lógico de seguridad si le resulta más cómodo acceder a una sala y llevarse un soporte que contiene los datos que le interesan.

2.1. Acceso de personas al recinto

El espacio en el que se encuentre el hardware debe contar con diferentes restricciones de acceso a personas, en función del impacto que tendría sobre la zona el robo o el deterioro de los equipos y, sobre todo, de la información. Por esa razón, es obvio que el área o las habitaciones en las que se encuentren los servidores tendrán la máxima protección dentro del conjunto de espacios en los que se concentre el hardware.

En la siguiente unidad se verán con mayor detalle los diferentes sistemas de control de acceso a instalaciones físicas.

caso **práctico** inicial

Las restricciones de acceso de personas serán más o menos fuertes en relación a la importancia de los datos que se custodian, del valor de los equipos y del impacto que supondría para la organización la pérdida de material o de información.

↑ Cartel de aviso de zona vigilada por vídeo.

El control de acceso de personas se puede realizar con sistemas muy diversos. Hay incluso compañías que ocupan edificios completos con el sistema informático distribuido por plantas y que usan uniformes de distinto color para el personal que puede tener acceso a cada planta. Pero también puede hacerse mediante tarjetas magnéticas que permitan el acceso a una o varias zonas determinadas, **vídeo vigilancia, tele vigilancia, vigilantes jurados, biometría.** Prácticamente todo lo relacionado con el control de acceso tiene una vertiente preventiva, pero en caso de incidencias también tomará la vertiente correctiva. Por ejemplo, un vigilante delante de un monitor puede impedir el acceso de una persona a una zona que no le está permitida, pero en caso de que se pase ese control y se produzca un ataque, esa persona podría ser identificada mediante las grabaciones de la cámara.

Alarma contra intrusos

En todo momento debemos tener claro que el fin primordial de la protección tanto física como lógica de un sistema de información son los datos. La entrada de intrusos en un espacio protegido en el que se encuentra información esencial para la organización, es un evento probable, y en cierto modo frecuente, que hace inútiles todas las medidas de protección del software y del hardware. Es, por tanto, importante la instalación de alarmas para detectar la presencia de personas no autorizadas en las áreas significativas.

Existen varios modelos de alarmas y en todas ellas se pueden instalar más o menos componentes. En esencia, un **sistema de alarma** consta de:

- **Un módulo central.** Se trata de una consola electrónica que controla el funcionamiento del resto de los componentes y los coordina. Permite un retardo en el aviso de alarma para dar un tiempo de entrada y desactivación del sistema a personas autorizadas. En el módulo central puede contener la **consola de activación** y desactivación por voz o introducción de contraseña, aunque puede ser independiente y tener asociado un mando a distancia. Si la alarma está conectada a una central de alarmas externa a la organización, el módulo enviará la señal a la central cuando se produzca una anomalía que haga sospechar de una intrusión.

↑ Consola de activación y desactivación de dos niveles: un nivel para toda el área protegida y otro para una subárea.

- **Detectores.** Disponen de sensores que detectan variaciones –generalmente del volumen o la temperatura– del espacio físico que abarcan. Los más modernos disponen de cámara que al mismo tiempo que detecta una intrusión, registra y envía las imágenes obtenidas a la central de alarmas interna o externa. Los sensores pueden ser infrarrojos, microondas y por frecuencias de sonido (en este caso normalmente se emplean para detectar la rotura de cristales). En zonas exteriores es común utilizar detectores con sensores de ultrasonidos.
- **Sistema de cableado.** Si los componentes no fueran inalámbricos, aunque la mayoría de los sistemas de alarma disponen hoy día de tecnología inalámbrica.
- **Baterías autónomas o de emergencia** en cada dispositivo. Funcionan todo el tiempo o utilizan los dispositivos conectados a la corriente eléctrica cuando se produce un corte de fluido.
- **Contactos magnéticos.** Se colocan en puertas y ventanas. Constan de dos piezas magnéticas que, si se separan, significa que la puerta o la ventana se ha abierto. Tras la espera de unos segundos para que la persona autorizada pueda proceder a la desconexión, saltaría la alarma.
- **Avisador telefónico.** En los modernos sistemas de alarma, existe un dispositivo que envía una señal a uno o varios números de teléfono predeterminados, bien sea mediante un mensaje de voz o mediante una señal acústica.
- **Pulsadores de emergencia.** Son botones que se colocan en lugares resguardados de la vista de personas extrañas, normalmente bajo mesas y mostradores, para activar la alarma en el caso de que se detecte la presencia de alguna persona extraña en una zona restringida.
- **La alarma** propiamente dicha. Básicamente consiste en un dispositivo acústico que emite una fuerte señal de sirena cuando se produce una intrusión, aunque suele estar acompañado de otro dispositivo que produce señales luminosas. Si la alarma es interior, la señal luminosa sirve para alertar a personas sordas; si es exterior, para localizar el lugar donde se ha producido la alarma sonora. En exteriores, la alarma acústica y en su caso la sonora están insertadas en una carcasa protegida de los elementos meteorológicos y en un lugar bien visible y poco accesible físicamente para evitar daños intencionados.

caso **práctico** inicial

La distribución de detectores y su ubicación en el espacio físico dependen de cuáles son las áreas sensibles con riesgo de intrusión. En todo caso, en una zona activable puede haber varios detectores, y existirán tantas zonas activables como sean necesarias sin entorpecer el trabajo normal de las personas en una organización.

↑ Detector volumétrico.

saber más

En las organizaciones de cierta relevancia como puede ser un importante Data Center existe un panel de control que monitoriza las distintas alarmas: incendios, temperatura, gases, líquidos, intrusos..., y que indica qué tipo de alarma se ha producido y en qué punto del edificio, además de activar los mecanismos de seguridad asociados a cada tipo de alarma.

↑ Módulo central y dispositivos de un kit básico distribuido por la empresa Securitas Direct, para uso doméstico o empresarial.

↑ Kit básico creado por Honeywell, que incluye detector de humos, de líquidos y de gases.

ACTIVIDADES

1. ¿Qué protege la seguridad lógica?
2. ¿Y la seguridad física?
3. En el caso poco probable de que una organización tuviese que decidirse por la seguridad activa o por la seguridad pasiva, ¿cuál de las dos consideras que debería elegir? Razona tu respuesta.
4. ¿Por qué crees que es importante adoptar medidas de seguridad pasiva si ya se han implantado todas las medidas posibles de seguridad activa?
5. El control de acceso de personas al recinto de un sistema de información es una medida de seguridad:
   a) Física.
   b) Lógica.
6. El control de acceso de personas es principalmente una medida de seguridad:
   a) Activa.
   b) Pasiva.
7. Si una empresa tiene un sistema de vídeo vigilancia mediante circuito cerrado de televisión, podríamos considerar este sistema como una medida de seguridad activa, puesto que persigue prevenir la entrada indiscriminada de personas a determinados recintos.
   a) ¿En qué casos podría considerarse que la medida es correctiva?
   b) ¿Podría considerarse la vigilancia mediante circuito cerrado de televisión como una medida mixta activa-pasiva? Razona la respuesta.
8. Una organización mantiene un potente sistema de seguridad lógica que impide el acceso telemático de intrusos a la información. ¿Puede entonces considerarse un sistema de información seguro?
9. Marca la opción u opciones que consideres acertadas. Un seguro contra incendios pertenecería a la seguridad:
   a) Física.
   b) Lógica.
   c) Activa.
   d) Pasiva.
   e) Ninguna de ellas.
10. ¿Qué diferencia hay entre sensores y detectores?
11. ¿Cómo funcionan los contactos magnéticos y dónde se colocan? Si no has visto ninguno, busca en internet y haz un dibujo o esquema aproximado de su forma.
12. Busca en internet algún kit de alarma de alguna empresa de seguridad. Verás que consta de varios módulos. Después, responde a estas preguntas:
    a) ¿Tienen que instalarse todos los módulos del kit para que el sistema funcione?
    b) ¿Hay unos módulos básicos imprescindibles?
    c) ¿Pueden agregarse módulos al kit básico?
13. Investiga:
    a) ¿Qué es un detector volumétrico?
    b) ¿Qué es lo que mide?
    c) ¿Cómo funciona?
    d) ¿Qué puede detectar que haga que se active la alarma?
    e) ¿Puede hacer saltar la alarma contra intrusos un detector volumétrico si en la estancia entran pájaros u otros animales de pequeño tamaño?
    f) ¿Qué tipo de detector aconsejarías para un patio de acceso a unas oficinas si en el patio hay normalmente un perro guardián?

2.2. Instalación eléctrica

Si prácticamente todo el hardware funciona mediante corriente eléctrica, es natural considerarlo como un punto importante a tener en cuenta al hablar de seguridad.

Podemos ver la red eléctrica desde dos puntos de vista: la **externa,** que pertenece a la compañía proveedora de electricidad, y la **interna,** que es propiedad de la empresa. Sobre la externa poco puede hacerse en cuestión de seguridad, excepto ocultar el cableado visible o fácil de alcanzar en la fachada del edificio y que se convertiría en un punto vulnerable si alguna mano malintencionada quisiese cortar el suministro. Para cubrir y proteger esa parte externa se necesitan los permisos de la compañía de electricidad.

caso **práctico** inicial

La persona encargada de la instalación y mantenimiento de equipos informáticos debe tener en cuenta el estado de la instalación eléctrica, y en caso de encontrar fallos de seguridad en la misma, pedir que se proceda a su revisión y reparación por un especialista en electricidad.

↑ Revisión de una instalación eléctrica.

saber más

Normalización

UNE (**U**na **N**orma **E**spañola). Conjunto de normas elaboradas por distintos Comités Técnicos de Normalización (CTN) y aprobadas dentro de la estructura de la Agencia Española de Normalización y Acreditación (AENOR).

EN (**E**uropean **N**orms). Conjunto de normas desarrolladas y aprobadas dentro de la Unión Europea en la estructura del Comité Europeo de Normalización (CEN).

UNE-EN. Adaptación española de las normas europeas.

El texto de las normas españolas no puede copiarse ni distribuirse gratuitamente.

En cuanto a la parte interna, la instalación eléctrica debe contratarse con la potencia suficiente para hacer funcionar todo el sistema sin riesgo de cortes internos de suministro por exceso de consumo, estar montada con elementos homologados y cumplir con las normas españolas y europeas (UNE y UNE-EN).

Por otra parte, **el personal** es un elemento del sistema de información y es muy importante tenerlo en cuenta al establecer medidas de seguridad. La instalación de tomas de tierra protege de descargas a las personas aunque haga saltar los magneto-térmicos y los diferenciales.

Pero… ¿qué ocurre si saltan esos elementos ya sea por exceso de consumo en un momento concreto o porque se ha producido un cortocircuito? La zona de la instalación que se viese afectada dejaría de funcionar, lo que podría poner en peligro la integridad de la información.

caso **práctico** inicial

La toma de tierra evita el riesgo de electrocución de personas y de avería de equipos. Es obligatoria su instalación, según el Reglamento electrotécnico para baja tensión (RD 842/2002).

saber más

Algunas normas españolas y europeas sobre seguridad de materiales eléctricos y protección de personas frente a la electricidad.

UNE 20314
UNE 20324
UNE 204001
UNE 20572
UNE 21720
UNE 21720
UNE 21737
UNE-EN 5010
UNE-EN 60832
UNE-EN 60855
UNE-EN 60900
UNE-EN 61032
UNE-ENV 50166

Buscador de normas AENOR

http://www.aenor.es/desarrollo/normalizacion/normas/ buscador normas.asp

La solución está, por una parte, en tener suficientes sectores acotados de corriente eléctrica para que un accidente afecte al menor número posible de elementos. Por otra parte, se pueden instalar otros dispositivos y mecanismos que sirvan como recursos provisionales hasta que la avería pueda ser subsanada, tales como **grupos electrógenos** y **sistemas de alimentación ininterrumpida,** además de una instalación de **luces de emergencia.**

Un **grupo electrógeno** es un generador de corriente eléctrica, independiente de la red eléctrica que se tiene contratada con alguna compañía. Funcionan con combustible y generan la energía eléctrica necesaria para paliar las deficiencias o los cortes en situaciones determinadas. Son imprescindibles, por ejemplo, en los hospitales para suministrar energía a los quirófanos, equipos informáticos y material quirúrgico de emergencia cuando se producen cortes de fluido eléctrico.

← Grupo electrógeno SDMO.

Los **sistemas de alimentación ininterrumpida** (SAI; en inglés, UPS) tendrán consideración especial y se tratarán con detalle en la siguiente unidad.

ACTIVIDADES

14. Explica la importancia que tiene la instalación eléctrica en la seguridad de un sistema informático.

15. ¿Es posible que el hardware funcione sin corriente eléctrica? Razona tu respuesta.

16. Estamos trabajando con nuestro ordenador y sufrimos un corte de electricidad. ¿Perdemos información? Razona tu respuesta.

17. ¿Es importante el número de ordenadores que tengamos para trabajar en una oficina a la hora de contratar la potencia de la corriente eléctrica? ¿Por qué?

18. ¿Por qué son importantes las luces de emergencia en un corte de luz?

19. Investiga sobre las luces de emergencia: ¿Por qué funcionan cuando no hay corriente eléctrica? ¿Cuánto tiempo se pueden mantener encendidas sin corriente eléctrica? ¿Qué ocurre si se encienden cuando hay corriente y se apagan cuando no la hay?

20. Busca en internet algunas normas AENOR relativas a seguridad en instalaciones eléctricas y explica de qué temas en concreto tratan.

21. ¿Es recomendable acotar por sectores la corriente eléctrica? ¿Por qué?

22. En un importante sistema de información, ¿siempre que se produce un corte de luz se debería poner en funcionamiento el grupo electrógeno?

23. ¿El electricista que viene a revisar la instalación eléctrica es un elemento del sistema de información? ¿Por qué?

24. En cuestión de seguridad, ¿para qué necesitamos los permisos de la compañía de electricidad?

25. ¿El grupo electrógeno funciona con electricidad?

2.3. Temperatura

El funcionamiento idóneo de los ordenadores es a baja temperatura, y la ideal se encuentra entre 15 y 25 °C, aunque trabajan sin dificultad entre los 10 y los 32 °C. Los terminales están siendo usados la mayor parte del tiempo por el personal encargado de ellos, en tanto que los servidores no requieren una presencia humana constante. Debe considerarse un sistema de climatización de las zonas de ordenadores que sea agradable para las personas sin poner en riesgo el buen funcionamiento de los equipos.

En las salas frías de los **centros de cálculo,** o en inglés *data centers*, la temperatura debe estar «pensada para ellos», es decir, para los servidores y otros equipos informáticos y electrónicos de alto nivel que allí se alojan, y no para las personas, y la temperatura adecuada oscila en torno a los 22 °C.

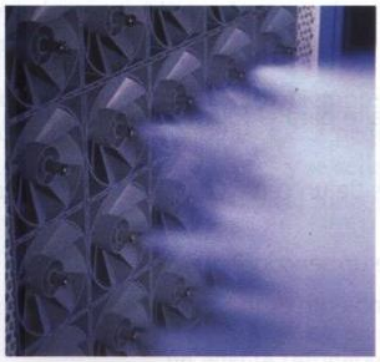
caso **práctico** inicial

La temperatura de 22 a 28 °C es agradable para las personas y no perjudica el funcionamiento de un ordenador normal.

↑ Sala fría de un centro de cálculo.

2.4. Aire y humedad ambiente

La **humedad relativa del aire** que asegura un funcionamiento óptimo de ordenadores y servidores es del 40 al 50 %. Las personas aportan humedad al aire mientras que los equipos electrónicos e informáticos no. Con este fundamento puede ser necesaria la instalación de humidificadores o deshumidificadores de aire en las zonas que lo requieran, o bien sistemas mixtos que humedezcan o sequen el aire hasta conseguir el grado de humedad relativa necesario para el buen funcionamiento de los equipos.



↑ Humidificador de aire de la compañía Luwa.

Las **partículas de polvo** son un gran enemigo de los ordenadores. Con el tiempo se incrustan en los disipadores y cubren los circuitos, tapando las vías necesarias de refrigeración, lo que hace que los componentes -principalmente el microprocesador- se calienten y se deterioren o se fundan. Otras veces, esas mismas partículas pueden provocar cortocircuitos si son conductoras de electricidad.

Para permitir la aireación de los equipos es conveniente un sistema de ventilación natural, si bien el aire natural lleva consigo partículas, como polen y pelos de animales. Un aire limpio puede conseguirse mediante purificadores de aire con filtro contra polvo y otras partículas. Hay quien asegura que el humo del tabaco también perjudica el funcionamiento de los ordenadores, pues, al igual que recubre de suciedad las pantallas y paredes, del mismo modo se adhiere a los discos, lectores láser y circuitos electrónicos, al ser absorbido directamente por los disipadores.

En zonas muy sensibles, como pueden ser los CPD (centros de procesamiento de datos), se hace necesario el aislamiento integral de la sala contra el polvo, fibras y otras partículas, como veremos más adelante al tratar de estos centros de computación.

La pureza del aire se puede controlar mediante la instalación de **detectores de gases,** que detectan y miden el monóxido de carbono, el oxígeno, el metano, el sulfuro de hidrógeno y otros gases.

ACTIVIDADES

26. Investiga. ¿Cuál es la temperatura ambiente ideal para un ser humano?

27. ¿Crees que la presencia de personas en una habitación afecta a la humedad relativa del aire?

28. Investiga qué tipos de desgaste sufren los ordenadores en climas con temperaturas extremas.

29. ¿Es aconsejable instalar un aparato de aire acondicionado en una zona con muchos ordenadores?

30. ¿Qué es un centro de cálculo?

31. Investiga. ¿Hay un tiempo límite para permanecer dentro de una sala fría de un centro de cálculo?

32. ¿Puede producir el polvo un cortocircuito? Razona tu respuesta.

33. ¿Cómo afecta el humo del tabaco a tu ordenador?

34. ¿Qué mide un detector de gases?

35. ¿Por qué es tan importante la humedad relativa del aire para el funcionamiento de un equipo informático? Busca información adicional al respecto.

36. Investiga si las personas que trabajan en las salas frías de un centro de cálculo necesitan algún tipo de indumentaria especial.

37. ¿Es necesaria la presencia humana para que funcione un servidor?

38. En una sala llena de ordenadores, ¿la temperatura ambiente es mayor que en una sala sin ordenadores? Razona tu respuesta.

2.5. Agua

El agua es otro de los grandes enemigos del hardware. Una inundación provocada por la rotura de tuberías en el interior del edificio o debido a la entrada de agua de lluvia, tendría consecuencias nefastas sobre equipos informáticos y periféricos. Los baños y salidas de agua deben situarse a distancia de las salas que alojen hardware o contar con sistemas de desviación y absorción del agua en caso de escapes accidentales y roturas. Los elementos del hardware deberán estar alejados de las ventanas y no apoyarse directamente en el suelo. Asimismo existen detectores de líquidos que pueden instalarse en el suelo o en las paredes y techos para detectar fugas de agua de la misma planta o de la superior.

caso **práctico** inicial

Se debe estudiar el riesgo de inundaciones por averías en la fontanería o por entrada de agua de lluvia. De cualquier modo, el hardware es más seguro situado sobre superficies que en caso de inundaciones lo protejan del agua.

2.6. Sistema contra incendios

Las medidas de seguridad pasiva contra incendios comprenden principalmente la instalación de barreras contra la propagación del fuego, la existencia de vías de evacuación de personas con la señalización correspondiente y los sistemas de extinción.

La seguridad activa contará con todas las medidas necesarias para evitar incendios fortuitos o provocados y con los sistemas de detección de humo, llamas y calor.

La mayor parte de los incendios que se producen en las áreas de ordenadores se deben a problemas con el sistema eléctrico, del que ya hemos hablado anteriormente.

El problema que el incendio causa sobre el hardware no es únicamente el fuego, ya que aunque algunos materiales se quemen sin llama, provocan un calor que deteriora gravemente circuitos y soportes. El humo es el tercer factor a tener en cuenta, porque ensucia y puede dañar el hardware.

Barreras murales

Los **muros cortafuegos** separan edificios o zonas distintas de un mismo edificio. Su objetivo es impedir durante un periodo más o menos largo de tiempo que el incendio se propague a sus áreas colindantes, reduciendo los daños y el riesgo para las personas. En las separaciones entre edificios, se construyen a la vez que estos y van desde los cimientos hasta sobrepasar la cubierta. Las placas cortafuegos pueden adosarse a muros y pilares de hormigón o metálicos. Están construidas con materiales ignífugos, no inflamables y de gran resistencia al calor y, en relación a su grosor, pueden detener el paso del fuego hasta varias horas, el tiempo necesario para que pueda ser extinguido.

A pesar de la construcción de muros cortafuegos, siempre quedan pequeñas zonas de conexión entre paredes, huecos y rendijas. Estas pequeñas áreas servirían de punto de contagio del fuego a zonas colindantes y se sellan mediante proyección de masillas y siliconas intumescentes resistentes al fuego.

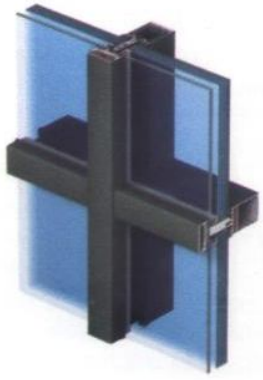
saber más

Las barreras cortafuegos están construidas con materiales ignífugos y de alta resistencia al calor, como la lana de roca o la cola de silicato, combinados en capas hasta obtener el espesor de seguridad deseado.

vocabulario

Intumescente

Según el diccionario de la Real Academia Española, significa «que se va hinchando».



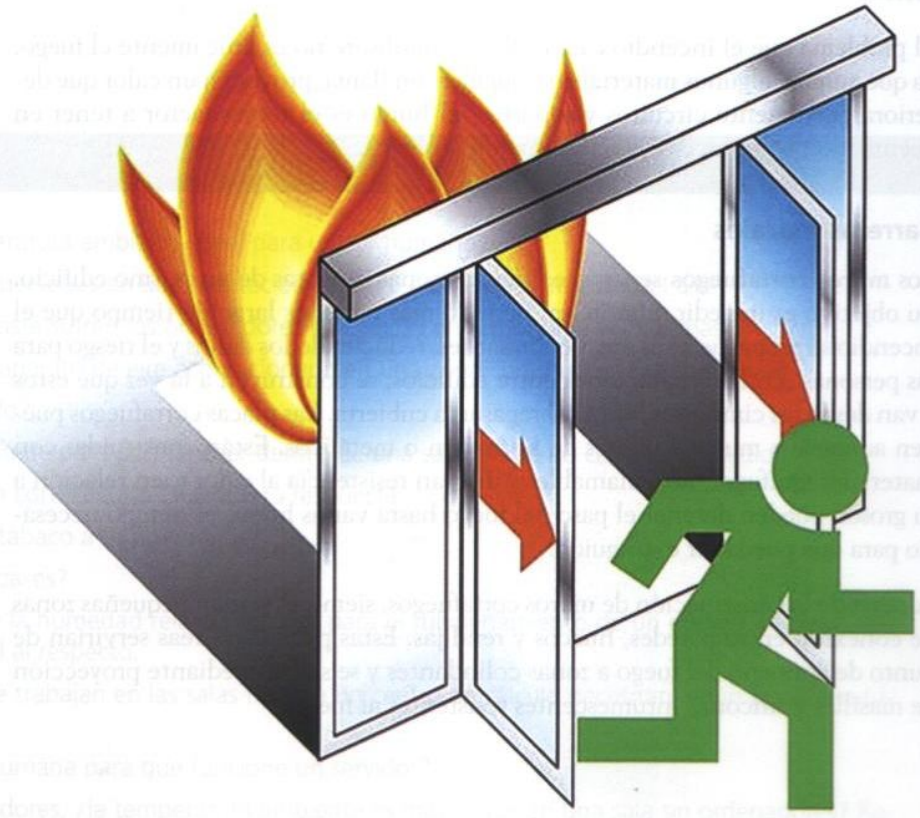
→ CW 50-FP EI60, un muro cortina que incorpora un agente refrigerante que extiende el factor tiempo de 30 a 60 minutos de resistencia al fuego.

Puertas y compuertas cortafuegos

Estos elementos deben cumplir, en cuanto a superación de pruebas de resistencia al fuego, lo establecido por las normas UNE-EN-1634 (puertas) y UNE-EN-1366 (compuertas), ambas del año 2000.

Las **puertas cortafuegos** constituyen una medida pasiva indispensable en la limitación de daños por incendio, y su uso está cada día más extendido –aunque aún no suele ser obligatorio– incluso en la construcción actual de edificios destinados a viviendas. Impiden la propagación no solo del fuego a zonas colindantes, sino también de humo y gases tóxicos y deben proteger las vías de evacuación.

Existen de varios tipos: basculantes, de guillotina, correderas, batientes, de persiana… y todas ellas pueden estar fabricadas con madera, metal y vidrio, aunque las más eficaces son las metálicas, que suelen consistir en dos chapas de acero en cuyo interior se encuentra una tercera capa de lana de roca. Dependiendo de su capacidad de resistencia al fuego, se clasifican en DF-30, DF-60…, donde el número corresponde a la cantidad de minutos que resistirían sin quemarse.



↑ Señalización de puerta cortafuegos en vía de evacuación.

Las **compuertas cortafuegos** se colocan en las salidas de los conductos de ventilación y aire acondicionado para cerrarse de forma manual o automática en caso de incendio e impedir que el fuego, el humo y los gases se propaguen a otras secciones.

Detectores de incendios

Los **detectores de incendios** son dispositivos que se instalan normalmente en el techo o en la parte más alta de los muros de las habitaciones, que son los puntos hacia los que se desplaza el humo, evitando las esquinas, a las que el humo llega más tarde que al resto de la superficie. Se deben instalar tantos puntos de detección de humo como posibles focos de riesgo de incendio, teniendo en cuenta que el detector convencional detecta el humo a una distancia no superior a seis o siete metros. Todos ellos estarán enlazados con una central de alarma que mostrará cuál ha sido el detector que se ha activado. Cuando un detector percibe aumentos considerables de temperatura, presencia de humo o partículas de combustión en el aire, se activa la alarma contra incendios.

Existen detectores mixtos, como el óptico-térmico o el óptico-térmico-químico.

Los **detectores de incendios** pueden ser:

- **Ópticos.** Dotados de tecnología fotoeléctrica que genera un haz de rayos luminosos. Cuando el humo penetra en el detector de humos, se produce un oscurecimiento del haz de luz y se activa la señal de peligro. El más moderno de los sistemas fotoeléctricos funciona mediante rayos láser y es hasta cien veces más rápido que los sistemas ópticos simples.

↑ Detector óptico de humos Zeta.

- **Iónicos.** Perciben las partículas procedentes de la combustión de materiales. Al penetrar el humo en las rendijas del detector, disminuye la ionización del aire, con lo que se corta la pequeña corriente eléctrica que se produce entre sus dos electrodos, lo que activa la señal acústica que avisa del peligro de incendio. Funcionan con una cámara de americio 241, un elemento radiactivo que bajo un normal funcionamiento no representa riesgo para las personas pero que necesita revisiones periódicas.

saber más

Normas a seguir en las instalaciones contra incendios:

- Norma básica de la edificación NBE CPI-96 sobre condiciones de protección contra incendios en los edificios.
- Real Decreto 1942/1993, de 5 de noviembre, por el que se aprueba el reglamento de instalaciones de protección contra incendios.
- Normas UNE 23110.

saber más

VESDA es una patente desarrollada por Xtralis que tiene capacidad para detectar la densidad del humo y determinar en qué fase se está produciendo un incendio, desde un estado de humo aún no perceptible hasta la de incendio de alta temperatura.

saber más

El humo puede producirse incluso si no hay fuego. El humo es uno de los componentes que más daño causa en equipos informáticos. Existen dispositivos especiales para la absorción y evacuación del humo en caso de incendio con o sin llama.

- **De temperatura o térmicos.** Programados para avisar de los cambios bruscos de temperatura en el recinto o para que disparen la alarma a partir de un número de grados.

↑ Detector de temperatura EST.

saber más

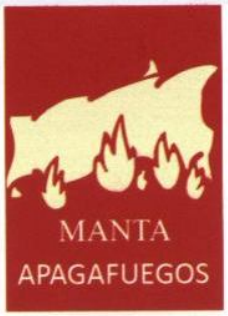
No se debe confundir el **detector por extracción de humo** con el **extractor de humos** para caso de incendios. Este último es una medida de seguridad pasiva que mantiene el aire con un cierto punto de respirabilidad cuando se ha producido un incendio. El detector por extracción de humos es una medida preventiva y corresponde, por tanto, a la seguridad activa.

- **Por extracción de humo.** Son dispositivos que extraen aire de manera continua por una serie de conductos. Cuando el aire está enrarecido a partir de un patrón de aire predeterminado, se produce una alarma. Es uno de los extractores más costosos por el tipo de instalación que necesita para su funcionamiento.

Extintores

Existen varias clases de extintores en consideración a su peso y al tipo de carga que contengan. En cuanto al peso, los hay portátiles desde 1 kg hasta los de 250 kg, dotados de ruedas para su desplazamiento.

Pero la cuestión principal es conseguir el tipo de extintor conveniente a cada espacio físico y que cumpla el Reglamento de aparatos a presión y el conjunto de normas europeas UNE- 23, en materia de extinción de incendios. El fuego de un incendio se clasifica en categorías, dependiendo del material combustible afectado. Los tipos no están estandarizados a nivel mundial, y existen ligeras variaciones de un país a otro en cuanto a su denominación, simbología y material combustible al que afectan:



↑ Señalización de manta apagafuegos.

↑ Pulsador de emergencia.

- **Tipo A.** El fuego que se produce sobre material combustible sólido, tal como la madera, el papel o el plástico, que al arder forma brasas.
- **Tipo B.** El que quemaría líquidos altamente inflamables, como grasas, aceites, gasolina, alcohol, etc.
- **Tipo C.** Sobre gases inflamables como butano, gas natural, propano, etc.
- **Tipo D.** El que quemaría metales especiales combustibles como el sodio, el magnesio o el potasio, que arden a alta temperatura.
- **Riesgo de electrocución.** Anteriormente llamado tipo E, que afecta a materiales que conducen, producen o almacenan corriente eléctrica.

Para cada tipo de fuego existe un tipo de agente extintor adecuado y otros contraindicados.

Siguiendo las recomendaciones del RD 1942/1993, del Ministerio de Industria y Energía, los agentes extintores adecuados e inadecuados para cada tipo de fuego se muestran en la siguiente tabla, con estas consideraciones:

(1) Los niveles de adecuación que están marcados con (1) podrían considerarse **Adecuados** en lugar de **Aceptables** si el fuego tiene una profundidad inferior a 5 milímetros.

(2) Los niveles que están marcados con un (2) no pueden utilizarse para extinguir incendios en donde hay presencia de aparatos bajo tensión eléctrica. El resto de agentes extintores no marcados con (2) podrían utilizarse en este caso siempre que hayan superado el ensayo dieléctrico normalizado según la norma UNE-23.110.

Por tanto, en espacios físicos donde haya equipamiento informático o electrónico o eléctrico están excluidos los extintores por agua o espuma, y son recomendables los de anhídrido carbónico (CO_2). Los halones (hidrocarburos halogenados), como agentes extintores, se desaconsejaron en el Protocolo de Montreal porque dañan la capa de ozono.

caso práctico inicial

En una sala con equipamiento electrónico y con importante flujo de corriente eléctrica es aconsejable el uso de extintores con CO_2 o de agua nebulizada.

	CLASE DE FUEGO – (UNE 23.010)			
	A (Sólidos)	B (Líquidos)	C (Gases)	D (Metales)
Agua pulverizada	Muy adecuado (2)	Aceptable		
Agua a chorro	Adecuado (2)			
Polvo BC convencional		Muy adecuado	Adecuado	
Polvo ABC polivalente	Adecuado	Adecuado	Adecuado	
Polvo específico metales	Adecuado			Adecuado
Espuma física	Adecuado (2)	Adecuado		
Anhídrido carbónico	Aceptable (1)	Aceptable		
Hidrocarburos halogenados	Aceptable (1)	Adecuado		

Vías de evacuación

Las vías de evacuación y las salidas de emergencia para casos de incendio deberán estar debidamente señalizadas y constarán en el plan de emergencias de la organización.

saber más

Algunas normas europeas en señalización contra incendios y vías de evacuación

- UNE 23033-81: Seguridad contra incendios. Señalización.
- UNE 23034-88: Seguridad contra incendios. Señalización de seguridad. Vías de evacuación.
- UNE 23-035-95: Seguridad contra incendios. Señalización fotoluminiscente. Parte 1.

Sistemas mixtos de detección y extinción de incendios

Son sistemas automáticos que ponen en marcha el proceso de extinción cuando se ha producido la alarma –mediante pulsadores manuales o de forma automática– de un peligro de incendio o de un incendio ya iniciado.

1. Un sensor de temperatura, de gases, de llamas o de humo, detecta el conato de incendio y emite una señal acústica y otra electrónica dirigida a un equipo de control.
2. Un equipo de control recibe la señal del elemento que la envía, comprueba que corresponde a una alarma de incendio y verifica el lugar en el que se ha producido.
3. El equipo de control activa el procedimiento de evacuación de personas y de extinción del incendio en la zona en la que se ha producido la alarma.
4. El sistema de extinción se pone en marcha vaciando de manera automática los extintores adecuados sobre la zona afectada.
5. El equipo de control verifica en cada momento el estado del incendio.

2.7. Seguros

La contratación de uno o varios seguros de riesgos compensará económicamente o minimizará las pérdidas por desastres ocurridos en la organización, como incendios, inundaciones, robo, fallos eléctricos, polvo en el ambiente, etc.

ACTIVIDADES

39. El personal de una empresa es un elemento del sistema de información al que se desea dotar de seguridad en el ámbito físico. Existen unas medidas de protección pasiva adicionales para personas, como pueden ser las mantas de fibra de vidrio, o mantas apagafuegos. Investiga de qué están fabricadas y por qué pueden proteger a las personas durante un incendio.

40. ¿Un soporte con ruedas para la CPU mantendría el ordenador a salvo en caso de un escape de agua?

41. Los muros cortafuegos, ¿son una medida de seguridad activa o pasiva contra incendios?

42. ¿Dónde se colocan las compuertas cortafuegos?

43. ¿Un sensor de humos es lo mismo que un detector de humos? ¿Por qué?

44. ¿Qué tipo de extintor sería adecuado para una sala con ordenadores?

45. Haz una pequeña labor de investigación: averigua si los componentes de los extintores dañan la capa de ozono.

46. Explica la diferencia entre detección y extinción.

47. ¿Un equipo de control avisa del lugar donde se ha producido un incendio?

48. Investiga. ¿Qué es el botón de emergencia contra incendios?

49. El sistema de extinción, ¿puede ser manual o automático?

50. ¿Los extintores deben cumplir algún tipo de reglamento?

51. Averigua qué tipo de controles deben hacerse en los extintores y con qué periodicidad.

52. Trabajas en una oficina, y tu jefe escuchó hace cinco años algo sobre la obligación de tener extintores y compró dos en la ferretería donde trabaja un amigo suyo. Dicho extintor nunca ha pasado una revisión. ¿Estamos incumpliendo alguna normativa?

53. ¿Funcionaría un detector de humos colocado a un metro del suelo? Razona tu respuesta.

54. Investiga y redacta un texto sobre el sistema contra incendios HI FOG, desarrollado por la compañía Marioff. ¿En qué consiste dicha tecnología? ¿Puede aplicarse a salas de datos y salas de ordenadores? ¿Es un sistema contra incendios antiguo o moderno? ¿Puede considerarse un sistema ecológico?

3. El entorno físico de un centro de proceso de datos (CPD)

Un CPD (centro de proceso de datos) consiste en uno o varios locales, una planta o un edificio completo que alberga el sistema principal de redes, ordenadores y recursos asociados para procesar toda la información de una empresa u organismo.

Otros nombres que se dan a un centro de proceso de datos son **centro de cálculo** y en inglés ***data center***, término utilizado cada vez con más frecuencia en España.

El objetivo principal de un CPD es proteger la **integridad, confidencialidad** y **disponibilidad** de la información. En este cometido velarán por lo dispuesto en la LOPD (Ley Orgánica de Protección de Datos de carácter personal), publicada en 1999, y por la Agencia de Protección de Datos.

↑ Vista del exterior de un *data center* de Google.

En lo que respecta al entorno físico, contarán con todas las medidas de seguridad que se han enumerado en esta unidad, y otras adicionales que exponemos a continuación.

3.1. Seguridad física redundante

Los CPD más importantes del mundo duplican la seguridad en aquellos elementos con más riesgo de fallos, como por ejemplo:

- Electricidad. Dos o más acometidas de red eléctrica de compañías proveedoras diferentes, para evitar que un apagón producido en una de ellas pueda comprometer la seguridad de los equipos electrónicos e informáticos si el tiempo de desconexión eléctrica superase la capacidad de los sistemas de alimentación ininterrumpida y de los grupos electrógenos. También se debe contar con una línea de corriente independiente para las áreas más críticas del CPD, de modo que no se produzcan interferencias por el uso de la corriente en otros locales.
- Detección y extinción de fuego.
- Doble cableado de fibra óptica.
- Climatización (temperatura, humedad y filtrado de aire).
- Dos o más proveedores de servicios de internet.
- CPD de respaldo. Otro edificio con información duplicada.

caso práctico inicial

La seguridad física de un *data center* o CPD es una seguridad extrema. En otras organizaciones y negocios se utilizarán las medidas de seguridad que correspondan a la importancia de la información que contienen, a los equipos instalados y al impacto que produciría la pérdida de hardware, de software o de información.

saber más

CPD de respaldo

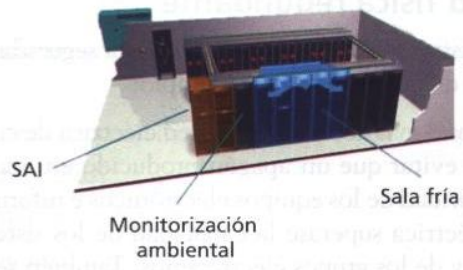
Algunos importantes centros de procesamiento de datos cuentan, como medida de seguridad, con dobles edificios en distintas áreas geográficas. En cada uno de ellos se mantiene idéntica información y en caso de un ataque que devastase uno de ellos, se podría activar el otro en pocas horas.

3.2. Control de acceso

- Guardias de seguridad 24 horas al día.
- Control de acceso perimetral y a zonas interiores.
- Cámaras de reconocimiento de matrículas de vehículos.
- Vigilancia en circuito cerrado de televisión.
- Puertas blindadas en las áreas más críticas.
- Sistemas biométricos (se verán con detalle en la siguiente unidad).
- Control de acceso personal o electrónico al CPD y nuevo control en las distintas dependencias para que ninguna persona pueda acceder a una zona para la que no tiene permiso.

3.3. Estructura

- Suelos con alta capacidad de carga.
- Dobles suelos para evitar riesgos de electrocución y de inundación.
- Construcción **antisísmica** en zonas con riesgo de terremotos.
- Paredes con tratamiento ignífugo y antipolvo.
- Aislamiento térmico en muros y ventanas.
- Sala fría. También denominada «pecera» y «nevera», es la zona más protegida de todo el centro de cálculo. En ella están los servidores, que son los elementos más protegidos de todo el sistema de información de un CPD. Esta sala deberá tener una temperatura constante recomendada de 22,3 °C y estar completamente aislada de contaminación por polvo y partículas. Normalmente, el acceso de personas es muy limitado y según algunos reglamentos tienen obligación de ponerse batas, gorros y zapatillas reglamentarias para no traspasar al aire fibras de la ropa ni cabellos.



↑ Esquema de un CPD con sala fría, con los sistemas de monitorización ambiental y de alimentación ininterrumpida.

ACTIVIDADES

55. Explica la importancia que tiene la seguridad física redundante en un *data center*.

56. Investiga para obtener más información acerca de qué es y qué contiene la sala fría de un *data center*.

PRÁCTICA PROFESIONAL

SPOF

Deriva de las siglas en inglés de ***S**ingle **P**oint **O**f **F**ailure* (punto único de fallo), y en el campo de la seguridad informática se refiere a un subsistema que, en caso de fallar, ocasionará un fallo general o parcial del sistema, que ponga en peligro la disponibilidad, la confidencialidad o la integridad de la información.

↑ La presencia de mecanismos de seguridad en el espacio físico de un sistema de información constituye una garantía para los datos, pero al mismo tiempo pueden constituir un problema si no están bien instalados, configurados o mantenidos.

OBJETIVOS

- Determinar qué elementos de la seguridad en el entorno físico pueden ser SPOF.
- Reflexionar sobre los fallos que pueden producirse en cada sistema de seguridad en el entorno físico.
- Analizar la repercusión que puede tener sobre la información el fallo en un sistema de seguridad.

Resuelve

1. A continuación hay una lista de elementos y mecanismos de seguridad física del edificio. Suponiendo que están instalados en una empresa, de cada uno de ellos indica:

a) Si puede ser un SPOF.

b) Un ejemplo de un posible fallo del elemento.

c) Qué incidencia podría tener sobre la información del sistema un fallo en el elemento en cuestión.

PRÁCTICA PROFESIONAL

Mecanismo	¿Es un SPOF?	Posible fallo del mecanismo	Repercusión del fallo en el sistema
Alarma contra intrusos			
Instalación eléctrica			
Sistema de control de la temperatura			
Sistema de control del aire y humedad del ambiente			
Detector de líquidos			
Barrera mural			
Puerta cortafuegos			
Compuerta cortafuegos			
Detector iónico de incendios			
Señalización de vías de evacuación			
Seguros de robo e incendio			
Extintor de incendios			

MUNDO LABORAL

Explosión en data center derriba miles de sitios web

Noticias24. Decenas de miles de sitios web se encuentran inoperativos por un fallo eléctrico que se produjo ayer por la tarde en uno de los data center más grandes de los EE. UU., el H1 de The Planet.com.

El fallo tuvo como origen la explosión de un transformador, que derribó tres paredes circundantes al cuarto eléctrico, y un incendio que obligó a evacuar al personal en el data center más antiguo de la compañía, ubicado en Houston, Texas.

Uno de los servidores de **Noticias24** se encuentra en el data center afectado y por ello es posible que algunas imágenes no estén disponibles para nuestros lectores.

Unos 9.000 servidores, que podrían albergar decenas de miles de sitios web, se encuentran completamente inaccesibles desde internet. Otros varios miles, ubicados en las otras instalaciones de The Planet, estarían inoperativos debido a la desconexión de los dos servidores de nombres que pertenecían a EV1Servers, empresa que fue adquirida por The Planet en 2006. Estos servidores proveen la traducción de nombres de dominio .com, .net y otros a las direcciones IP de los computadores en los que residen físicamente los *websites*.

El incendio derribó todos los *websites* alojados en las instalaciones afectadas, aunque la compañía cuenta con otros cinco data center en Dallas y Houston. Los servidores de los clientes no habrían sufrido daños, aseguraron empleados de ThePlanet que estuvieron emitiendo partes informativos hasta altas horas de la madrugada.

Portavoces de la empresa prometieron que los sitios volverían a estar en línea «tan pronto como fuera posible» aunque se negaron a dar una estimación concreta del tiempo que tomaría solventar los fallos y reparar los equipos de red afectados por el incendio. Sin embargo, dijeron que quizá podrían comenzar a verse resultados en la tarde de este domingo.

Otras compañías que dependen de ThePlanet.com, como revendedores tales como HostGator, también tienen un importante número de servidores fuera de línea.

MUNDO LABORAL

La empresa asegura que, aunque sus instalaciones de Houston cuentan con un sistema de generadores eléctricos a base de diésel en caso de fallos de energía, autoridades del departamento de bomberos les prohibieron encenderlos por los riesgos de empeorar la situación en el interior del edificio.

El fallo irritó a clientes que habían confiado en que la compañía tenía a mano los más modernos sistemas de redundancia de conectividad de red y de energía eléctrica, tal como promete su sitio web. Otros lamentaron que los servidores de nombres de dominio ns1.ev1servers.net y ns2.ev1servers.net estuvieran ubicados en el mismo edificio, dado que uno de los servidores debería suplir al otro en caso de fallos.

El «evangelista» de la compañía, Kevin Hazard, había publicado en el *blog* corporativo una serie de imágenes tomadas en uno de los data center de The Planet en Houston, aunque ignoramos si se trata del mismo DC afectado por el incendio. Hazard fotografió los cuartos eléctricos, de transferencia de energía y los generadores de respaldo ubicados en el techo de las instalaciones.

Adaptado de Noticias24. 1 de junio de 2008

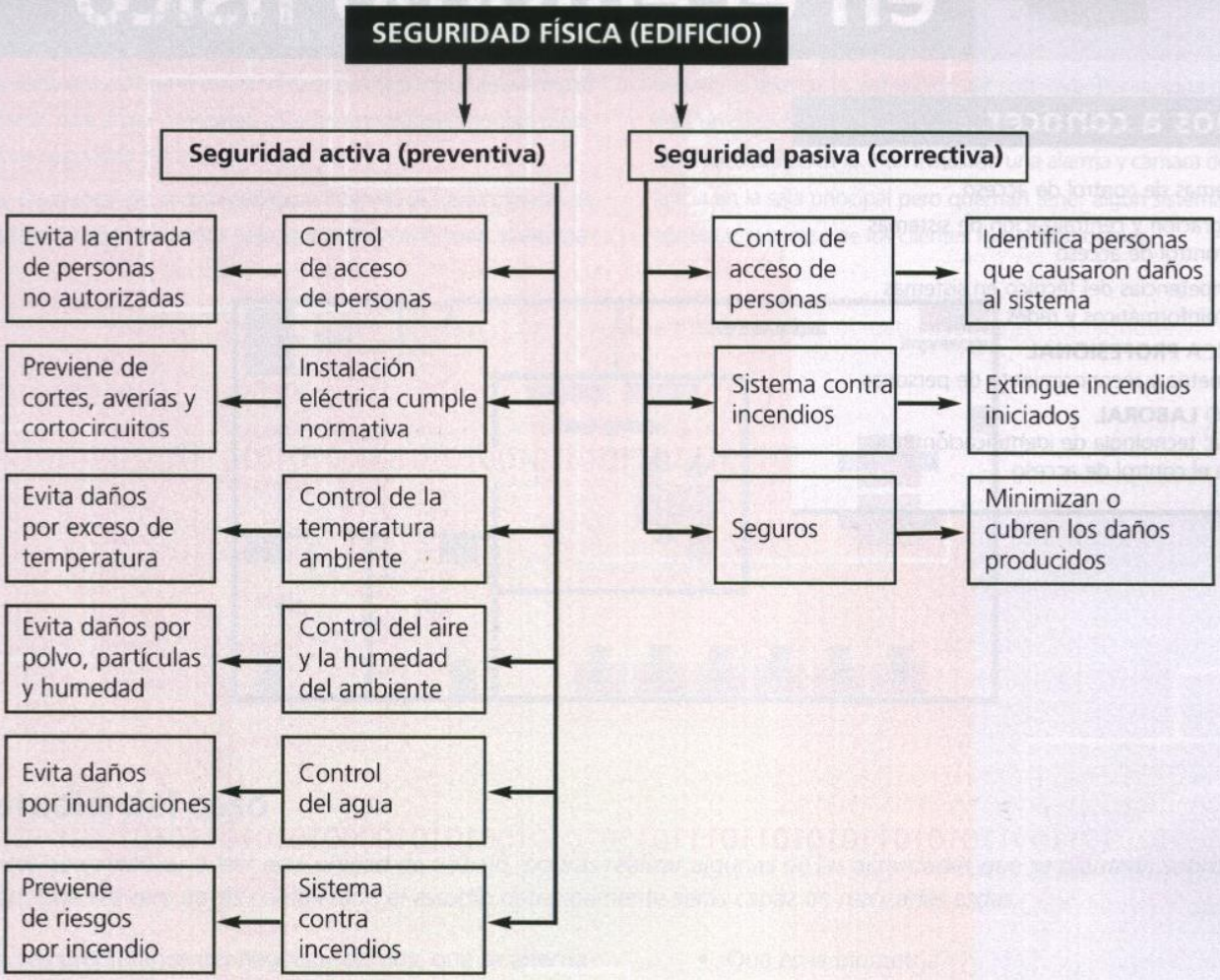
http://www.noticias24.com/tecnologia/noticia/756/explosion-en-datacenter-derriba-miles-de-sitios-web/

Actividades

Después de leer la noticia publicada por Noticias24, responde a las siguientes cuestiones:

1. ¿Dónde se produjo un importante fallo eléctrico?
2. ¿Qué fue lo que ocasionó el siniestro?
3. ¿Qué consecuencias tuvo el siniestro sobre el edificio?
4. ¿Y sobre el personal del data center?
5. ¿Qué repercusión tuvo el siniestro sobre la agencia Noticias24 que publica la noticia?
6. ¿Cuántos servidores tenía alojados el data center?
7. La empresa decía tener grupos electrógenos de emergencia, ¿por qué no pudieron utilizarlos?
8. ¿Qué sistemas redundantes parecía tener la compañía, según publicaba en su sitio web?
9. ¿Consideras que los servidores redundantes de nombres de dominio debían encontrarse en el mismo espacio físico? Razona tu respuesta.
10. ¿Crees que es posible la pérdida de clientes en una situación como la que detalla el artículo? ¿Por qué?
11. ¿Crees, a la vista de lo narrado en la noticia, que la empresa propietaria del data center dio partes del incidente que podrían no corresponder con la realidad?
12. ¿Qué importancia tienen las medidas de seguridad en el edificio sobre la disponibilidad de la información?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **La seguridad en el espacio físico de un sistema de información tiene como objetivo final:**
   a) Que el edificio no se deteriore.
   b) La protección de las personas.
   c) La protección de la información.
   d) Evitar desastres naturales.

2. **La seguridad de un edificio o un local es:**
   a) Física.
   b) Activa.
   c) Pasiva.
   d) Las tres anteriores.

3. **¿Qué activos se están protegiendo al cuidar de la seguridad física del edificio?**
   a) Las personas.
   b) La información.
   c) El hardware.
   d) Todos.

4. **El control de acceso físico al sistema es, principalmente:**
   a) Seguridad activa.
   b) Seguridad pasiva.
   c) Seguridad lógica.

Soluciones: 1c, 2d, 3d, 4a

3 Control de acceso en el entorno físico

vamos a conocer...

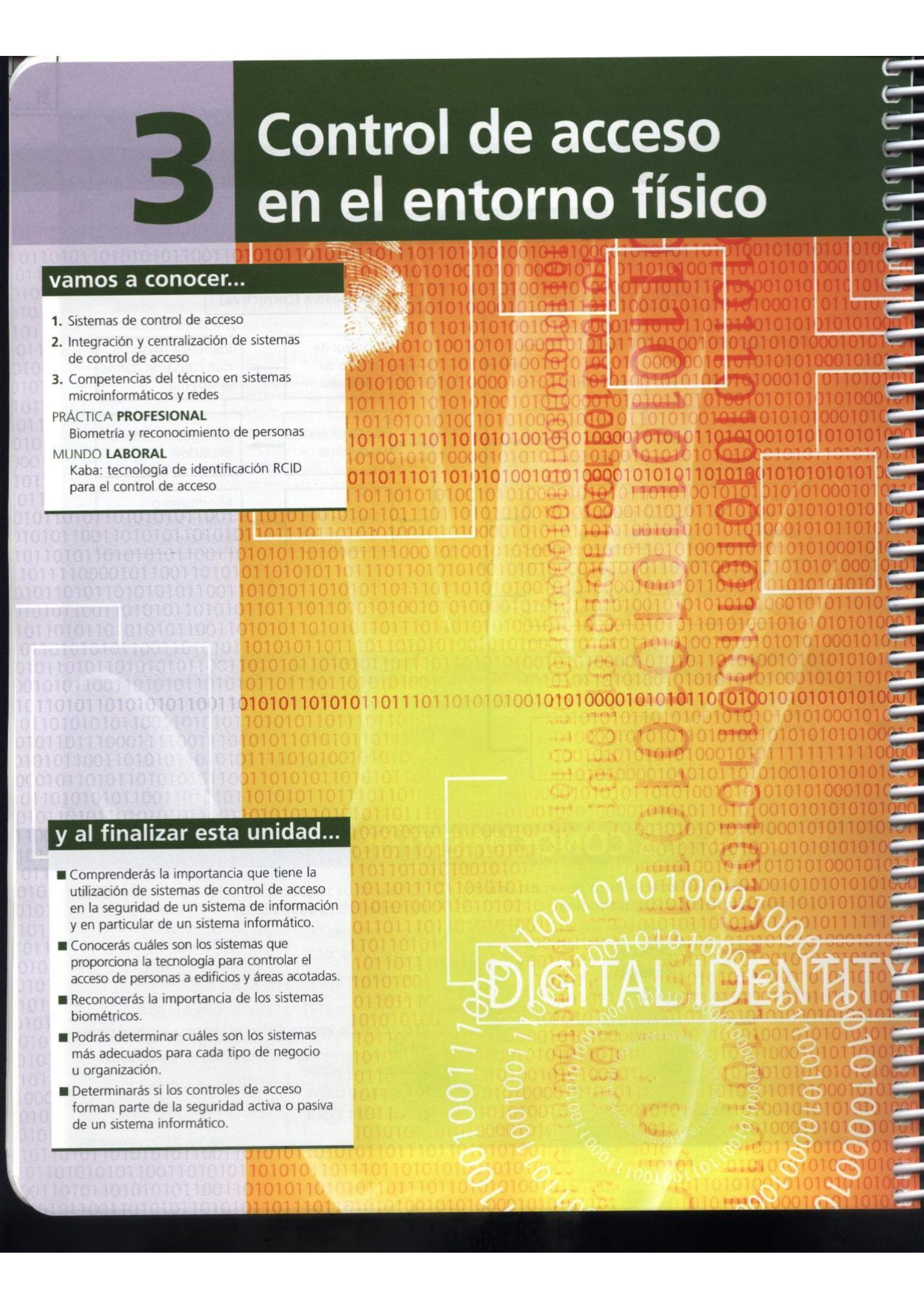
1. Sistemas de control de acceso
2. Integración y centralización de sistemas de control de acceso
3. Competencias del técnico en sistemas microinformáticos y redes

PRÁCTICA **PROFESIONAL**
Biometría y reconocimiento de personas

MUNDO **LABORAL**
Kaba: tecnología de identificación RCID para el control de acceso

y al finalizar esta unidad...

- Comprenderás la importancia que tiene la utilización de sistemas de control de acceso en la seguridad de un sistema de información y en particular de un sistema informático.
- Conocerás cuáles son los sistemas que proporciona la tecnología para controlar el acceso de personas a edificios y áreas acotadas.
- Reconocerás la importancia de los sistemas biométricos.
- Podrás determinar cuáles son los sistemas más adecuados para cada tipo de negocio u organización.
- Determinarás si los controles de acceso forman parte de la seguridad activa o pasiva de un sistema informático.

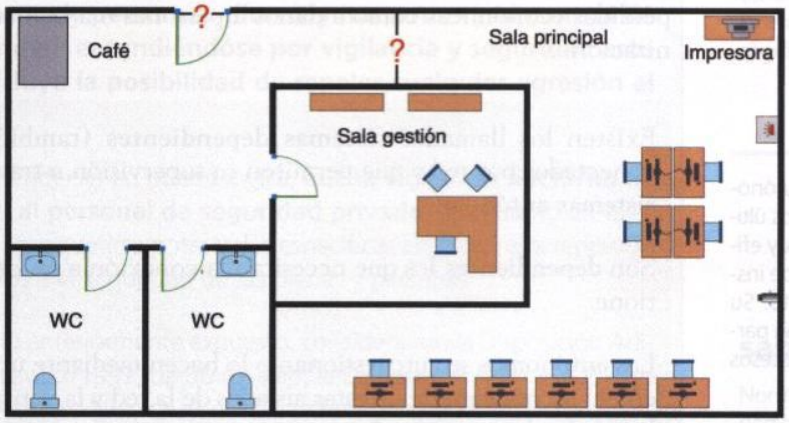


CASO **PRÁCTICO** INICIAL

situación de partida

Recuerda el local que vimos en el caso práctico inicial de la Unidad anterior, para el que solicitaron a Carlos asesoramiento sobre medidas de seguridad física.

Hoy día el local de acceso público a internet se ha terminado de construir. Ya se encuentra colocado e instalado todo el equipamiento, a falta de la instalación del software. Por la zona donde está ubicado el negocio la mayoría de clientes serán estudiantes de la Facultad cercana. Han instalado una alarma y cámara de vigilancia en la sala principal pero querrían tener algún sistema para controlar el acceso de los clientes fijos y ocasionales.



estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Los propietarios del negocio son dos, que se alternarán en horarios para la gestión y el mantenimiento, de modo que nunca habrá más de uno a la vez en el local. La empresa es nueva y de momento no tiene recursos para contratar personal, aunque una sola persona en horas punta puede sentirse desbordada mientras informa y atiende a clientes, cobra, repara pequeñas averías, registra datos en el ordenador, atiende reclamaciones, etc. Les gustaría que Carlos les proporcionara alguna información acerca de sistemas que puedan ayudarles a controlar el acceso y la gestión de clientes.
   - ¿En qué consiste el control de acceso físico?
   - ¿Existen sistemas de bajo costo que puedan ayudar a controlar el acceso de personas a pequeñas empresas?
2. Le han preguntado a Carlos sobre algo que han oído de sistemas biométricos.
   - ¿Qué es la biometría?
   - ¿Se puede utilizar la biometría como control de acceso?
   - ¿Habría algún sistema biométrico que se adaptara a las necesidades y economía del negocio?
3. En cuanto al lugar físico en el que se podría colocar el sistema en caso de que optasen por esa solución:
   - ¿Sería conveniente instalarlo en la puerta de acceso principal o a la larga resultaría más eficaz en el pasillo que da entrada a la sala principal?
4. Los dueños del negocio están verdaderamente interesados por conocer todo lo relativo al control de acceso.
   - En el fondo, ¿qué es lo que se protege cuando se instalan medidas de seguridad en los accesos?
   - ¿Se está protegiendo la información?
   - El control de acceso, ¿es una medida de seguridad activa o de seguridad pasiva?

1. Sistemas de control de acceso

En esta unidad continuamos estudiando la seguridad en el entorno físico, entendido como el espacio donde se encuentra el sistema de información (locales y edificios), y veremos qué mecanismos de seguridad física tienen relación con el control de acceso, algunos de ellos utilizables también en la protección directa del equipamiento hardware.

Naturalmente, los dispositivos –tipos, categorías o número– que se utilicen para controlar la entrada de personas a un edificio o a algunas de sus áreas dependerán del nivel de seguridad que requiera un sistema de información y de la cuantificación del impacto de una amenaza sobre sus activos, tanto en lo relativo a pérdidas económicas como a daños a personas o a la imagen social de la organización.

saber más

Se llama **sistema autónomo convertible** el que, siendo autónomo, también tiene la posibilidad de ser conectado a otro dispositivo gestor, como un PC o una central de control.

saber más

La instalación de sistemas autónomos se ha incrementado en los últimos años ya que resultan muy eficientes y reducen los costes de instalación y de mantenimiento. Su inconveniente: que no forman parte de un control central de accesos y movimientos de personas.

Existen los llamados **sistemas dependientes** (también llamados *on-line*, conectados por red y que permiten su supervisión a través de internet) y los **sistemas autónomos.**

Son **dependientes** los que necesitan la conexión a un ordenador que los gestione.

Los **autónomos** se autogestionan o lo hacen mediante un dispositivo adjunto, con el inconveniente de estar aislados de la red y la ventaja de que se reducen los costes de conexión.

A los sistemas autónomos que permiten ser configurados para su conexión a un ordenador que controla sus funciones, se les denomina **sistemas autónomos convertibles.** La conexión a un PC o central de control puede realizarse de forma cableada o inalámbrica.

caso **práctico** inicial

El control de acceso físico es una medida de seguridad activa que previene de peligros que en último extremo podrían afectar al núcleo de cualquier sistema de información: los datos.

Además de los dispositivos y sistemas mecánicos, electrónicos o biométricos, están las personas que se ocupan del control de los accesos y de la vigilancia, que tienen unas funciones establecidas por ley, diferentes si se trata de personal de vigilancia privada (externo a la organización) o de la plantilla de la empresa.

1.1. Personal de vigilancia y control

La vigilancia y el control de seguridad pueden asignarse a personal auxiliar de la plantilla de la organización, a vigilantes de seguridad privados u optar por un sistema mixto de vigilancia entre el personal propio de la empresa y externo.

El Ministerio del Interior publicó en julio de 2009 un **informe orientativo y no vinculante** sobre las funciones y tareas del personal de seguridad privada, atendiendo a la petición de información de una empresa.

El contenido de dicho informe aclara las dudas que puede suscitar la interpretación de la legislación correspondiente en cuanto a la distribución de tareas entre el personal auxiliar de la propia empresa dedicado al control o la vigilancia y el personal de seguridad privada.

A continuación, presentamos parte de dicho informe del Ministerio del Interior:

En principio, y como criterio general, puede señalarse que la correcta aplicación de la legislación de seguridad privada pasaría por **reservar al personal de seguridad privada estrictamente las funciones de vigilancia y seguridad activa de bienes y personas –diurna y nocturna– y el control de sistemas de seguridad; entendiéndose por vigilancia y seguridad activa aquella que incluye la posibilidad de repeler cualquier agresión al bien que se vigila.**

Asimismo, ha de entenderse, en buena lógica, que **la vigilancia nocturna ha de estar reservada al personal de seguridad privada,** por cuanto en tales circunstancias podrían requerirse potestades específicas en orden a la represión de posibles agresiones a la seguridad de los bienes y personas.

Teniendo en cuenta lo anteriormente expuesto, considerando la Disposición Adicional Tercera de la Ley 23/1992, de 30 de julio, la Disposición Adicional Primera del Real Decreto 2364/1994, de 9 de diciembre, y las concretas funciones que corresponden al personal de seguridad privada –en particular los artículos 71, 72, 76 y 77 del Reglamento de Seguridad Privada–, se podrían, a grandes rasgos, señalar como tareas **que corresponde realizar al personal de seguridad privada** en relación con la vigilancia y custodia de personas y bienes, las siguientes:

1) El control de accesos cuando existan mecanismos de seguridad incorporados contra la comisión de infracciones o se trate de limitar la entrada de determinadas personas.

2) El control de sistemas de seguridad contra la comisión de delitos y faltas (si los hubiera), incluyendo las siguientes actuaciones:

   a) Comprobación del estado y funcionamiento de las instalaciones de seguridad para la prevención de delitos y faltas.

   b) Vigilancia y control desde los medios técnicos que constituyen sistemas de seguridad contra delitos y faltas.

   c) Transmisión de la información a las Fuerzas y Cuerpos de Seguridad referentes a las situaciones advertidas por los mencionados sistemas de seguridad.

3) La vigilancia y seguridad de los bienes y de las personas que se encuentren en los inmuebles o establecimientos, con posibilidad de represión, incluyendo las siguientes actuaciones:

recuerda

Son diferentes las áreas de competencia del personal de seguridad de la empresa y las del personal de seguridad privada.

saber más

Normativa sobre competencias del personal de vigilancia y control:

1) Ley 23/1992, de 30 de julio, Disposición Adicional Tercera.
2) Real Decreto 2364/1994, de 9 de diciembre:
   a) Disposición Adicional Primera.
   b) Reglamento de Seguridad Privada, artículos 71, 72, 76 y 77.

a) Identificación de personas.

b) Retención de personas, si fuera absolutamente necesario, poniéndolas inmediatamente a disposición de las Fuerzas y Cuerpos de Seguridad.

c) Registros, aun cuando únicamente en supuestos de indicios de comisión de actos delictivos.

d) Expulsión de personas por incumplimiento de las normas propias del establecimiento.

e) Intervención en supuestos de actos vandálicos, atraco, intrusión, etc., y puesta en conocimiento de las Fuerzas y Cuerpos de Seguridad de tales hechos.

f) Especial atención, de carácter complementario, en la organización y control de la evacuación de visitantes.

Estas funciones deberán realizarse por vigilantes de seguridad, debidamente habilitados e integrados en empresas de seguridad, los cuales, dentro de la entidad o empresa donde presten sus servicios, **se dedicarán exclusivamente a la función de seguridad propia de su cargo, no pudiendo simultanear la misma con otras funciones** (artículo 12 de la Ley 23/1992, de 30 de julio).

Por contraposición a lo anterior, **existen una serie de funciones que, como norma general, por ser ajenas a las de seguridad privada, no deberían ser realizadas por vigilantes de seguridad,** como son las que se refieren, entre otras, a la comprobación del estado y funcionamiento de las instalaciones generales que no sean de seguridad; el control, en su caso, a través de medios técnicos de los sistemas de mantenimiento (calderas, instalaciones eléctricas, etc.) que no sean de seguridad; el control del ambiente (temperatura, humedad, etc.); el control de agentes exteriores tales como insectos, microorganismos, etc.; y el control de los sistemas antiincendios.

Tal es lo que deriva de la Disposición Adicional Tercera de la Ley 23/1992, de 30 de julio, y Primera del Real Decreto 2364/1994, de 9 de diciembre, en base a las cuales quedan fuera del ámbito de aplicación de la normativa de seguridad privada una serie de actividades que **serán realizadas por personal distinto del de seguridad privada, no integrado en empresas de seguridad y que puede ser contratado directamente por los titulares de los inmuebles**. Entre dichas actividades figuran las siguientes:

1) Las de información en los accesos, custodia y comprobación del estado y funcionamiento de las instalaciones, y de gestión auxiliar, realizadas en edificios particulares por porteros, conserjes y personal análogo.

2) En general, la comprobación y control del estado de calderas e instalaciones generales en cualesquiera clase de inmuebles, para garantizar su funcionamiento y seguridad física.

caso práctico inicial

La contratación de personal o de empresas de seguridad privada para el control y la vigilancia es uno de los métodos más costosos en lo relativo a seguridad física y suelen emplearse en grandes empresas.

3) El control de tránsito en zonas reservadas o de circulación restringida en el interior de fábricas, plantas de producción de energía, grandes centros de procesos de datos y similares.

4) Las tareas de recepción, comprobación de visitantes y orientación de los mismos, así como las de control de entradas, documentos o carnés privados, en cualquier clase de edificios o inmuebles.

Dichas actividades, al no ser de seguridad privada, **deben ser realizadas por personal distinto del de seguridad privada y ello, fundamentalmente, porque el personal de seguridad privada, por imperativo legal y reglamentario, no puede dedicarse a otras funciones que no sean las propias de seguridad que tiene legal y reglamentariamente atribuidas.**

Por su parte, el artículo 70 del Reglamento de Seguridad Privada, en la redacción dada al mismo por el Real Decreto 1123/2001, de 19 de octubre, dispone lo siguiente:

> *«1. Los vigilantes, dentro de la entidad o empresa donde presten sus servicios, se dedicarán exclusivamente a la función de seguridad propia de su cargo, no pudiendo simultanear la misma con otras misiones.*
>
> *No se considerará excluida de la función de seguridad, propia de los vigilantes, la realización de actividades complementarias, directamente relacionadas con aquella e imprescindibles para su efectividad.*
>
> *Las funciones de escolta privado, vigilante de explosivos y detective privado son incompatibles entre sí y con las demás funciones de personal de seguridad privada, aun en los supuestos de habilitación múltiple. Tampoco podrá compatibilizar sus funciones de seguridad privada, salvo los jefes de seguridad, con el ejercicio de otra actividad dentro de la empresa en la que realicen sus servicios».*

Respecto al apartado primero del artículo transcrito, esta Secretaría General Técnica ha venido considerando que el mismo no se refiere tanto a un supuesto de incompatibilidad legal para el desempeño de dos puestos de trabajo, como a la exclusividad en el desarrollo de las funciones que se tienen atribuidas mientras se están materialmente desempeñando.

Efectivamente, se establece que los vigilantes –cabe entender también que sus especialidades de escoltas privados y de vigilantes de explosivos y sustancias peligrosas–, dentro de la entidad o empresa donde presten sus servicios (esto es, dentro de la empresa usuaria de los servicios de seguridad), se dedicarán exclusivamente a la seguridad propia de su cargo, no pudiendo simultanear la misma con otras misiones. Ello significa que, **durante el tiempo de prestación de servicios para el que haya sido contratado el vigilante de seguridad por la empresa o entidad usuaria, no puede desempeñar en la misma otras funciones –de cualquier naturaleza– que no sean las propias de vigilancia y seguridad que le corresponden.**

↑ Placa de vigilante de seguridad privada.

En este sentido, cabe interpretar que la vigente normativa de seguridad privada lo que pretende es garantizar que no se produzca menoscabo o disminución de la eficacia de las funciones específicas de vigilancia, seguridad y protección que los vigilantes de seguridad tienen encomendadas. De ahí que se prohíba la prestación simultánea (ejercicio en el mismo periodo de tiempo de dos actividades) de funciones de seguridad privada y otras distintas a estas.

Tras la modificación efectuada por el Real Decreto 1123/2001, de 19 de octubre, y con el fin de contribuir a paliar el intrusismo en el sector de la seguridad privada, se introdujo el siguiente párrafo en el artículo 70 del Reglamento de Seguridad Privada: «*No se considerará excluida de la función de seguridad, propia de los vigilantes, la realización de actividades complementarias, directamente relacionadas con aquella e imprescindibles para su efectividad*».

Pues bien, puesto que la norma exige que se trate de actuaciones «*directamente relacionadas con aquella (la función de seguridad) e imprescindibles para su efectividad*», podrían considerarse comprendidas entre tales actuaciones las de comprobación de daños personales y materiales producidos, la persecución de delincuentes sorprendidos en flagrante delito, la prestación de auxilio a posibles víctimas, la colaboración con las Fuerzas y Cuerpos de Seguridad o con los equipos de emergencia, la evacuación de heridos, etc.

En **conclusión,** sin perjuicio de que pueda admitirse una cierta discrecionalidad en cuanto a determinados puestos de trabajo que, consistentes en la custodia ordinaria relacionada básicamente con las normas de funcionamiento del establecimiento, pudieran ser asignados a personal auxiliar o propio de los establecimientos o a personal de seguridad privada, en atención a determinadas circunstancias, puede decirse que **los aspectos diferenciadores de uno y otro personal se fundamentan básicamente en tres parámetros:**

1. La naturaleza de las actividades que realizan que, en el caso de las excluidas del ámbito de aplicación de la Ley 23/1992, de 30 de julio, y el Reglamento de Seguridad Privada, aprobado por el Real Decreto 2364/1994, de 9 de diciembre, no van encaminadas a la prevención de delitos y faltas.

2. La no exigencia de que el personal al que se refiere la Disposición Adicional Primera del Real Decreto 2364/1994, de 9 de diciembre, esté integrado en empresas de seguridad, requisito que, sin embargo, sí se exige para los vigilantes de seguridad.

3. Las circunstancias en que deben prestarse los servicios que, en el caso de los vigilantes de seguridad, habrán de desempeñarse en el interior de los edificios e inmuebles, portando el uniforme y los distintivos reglamentarios, así como, en su caso, las armas previstas en la normativa de seguridad privada.

Puede consultarse el informe completo en:

http://www.mir.es/SGACAVT/respuestas/seg_privada/Personal_Seg._Privada/i3459-07-09.htm

ACTIVIDADES

1. ¿Cuántos tipos de sistemas de control de acceso conoces?
2. ¿Cómo se denominan los sistemas autónomos que permiten ser configurados para su conexión a un ordenador?
3. ¿Qué tiene que ver el control de acceso al edificio con la seguridad informática?
4. Las tareas y funciones del personal de seguridad privada, ¿tienen algún tipo de reglamentación?
5. Las tareas de información y orientación de visitas son competencia de:
   a) Personal de la empresa.
   b) Personal de vigilancia privada.
6. El control de accesos cuando existan mecanismos de seguridad incorporados contra la comisión de infracciones o se trate de limitar la entrada de determinadas personas corresponde a:
   a) Personal de la empresa.
   b) Personal de vigilancia privada.

1.2. Teclados

Los teclados básicos abren la puerta si se introduce la contraseña correcta que sería común a todos los usuarios y que, por seguridad, debería cambiarse con cierta frecuencia. Disponen de una batería y de un sistema automático de cierre y apertura de la puerta, que tendrá una cerradura eléctrica. Los hay para interior y para exterior. Estos últimos son de material más resistente a las agresiones humanas y a las atmosféricas.

Si avanzamos en complejidad, tenemos los teclados que permiten ser configurados con contraseñas personalizadas para cada usuario, que pueden programarse y con capacidad para un número máximo de usuarios, dependiendo del fabricante y del precio.

Aunque no es frecuente en teclados simples, existen algunos con posibilidad de ser conectados a un ordenador que registre las entradas y las salidas identificadas y los accesos frustrados.

↑ Teclado básico de control de acceso DK-9520 Digital de la compañía Protect-on Systems Limited.

1.3. Tarjetas

Las más actuales son las **tarjetas de proximidad,** resistentes a los rayos solares y a los campos magnéticos. Su funcionamiento consiste en acercar la tarjeta al dispositivo lector, que procede a la identificación.

Con mucha menos frecuencia se utilizan a día de hoy otros lectores que exigen la introducción de **tarjetas de banda magnéticas,** ya que tanto el dispositivo como las tarjetas sufren deterioro con el uso y estas últimas, además, si se exponen al calor o a campos magnéticos.

También está decreciendo el uso de tarjetas con código de barras, que, aunque no necesitan ser introducidas en el lector –con lo cual no sufren roces–, su código impreso puede sufrir arañazos que las harían inservibles.

Si bien básicamente se trata de un sistema autónomo, muchos de ellos tienen también la posibilidad de conectarse a un ordenador que daría de alta y de baja las tarjetas y ejercería la función de control de entradas, salidas y tiempo de permanencia en una determinada estancia o edificio.

Estos lectores de tarjetas pueden permitir configurar hasta un número de usuarios que puede llegar a varios miles.

En el conjunto de tarjetas suele existir una de **borrado** que permite eliminar de la base de datos de accesos permitidos la identidad de una persona que ha dejado de tener autorización, por ejemplo, porque ya no trabaja en la empresa.

Las **tarjetas de proximidad** se basan en la tecnología de identificación por radiofrecuencia (RFID) de corto –hasta unos 15 centímetros de distancia– o de largo alcance –hasta 2 o 3 metros–. Tienen la ventaja sobre otros sistemas de que la identificación se realiza sin contacto e incluso a cierta distancia, lo que deja abierto el campo a la imaginación para su uso. Por ejemplo, el lector puede situarse en la parte interior de una puerta, lo que impide cualquier intento de vandalismo sobre el mismo.

saber más

Las tarjetas cumplen una doble misión:

Acceso. Permitir la entrada al portador de la tarjeta.

Identificación. Conocer la identidad del titular de la tarjeta.

↑ Lector de tarjetas de proximidad de la empresa Softrónica (Madrid). Junto al lector hay cuatro llaves y otra más en funda de plástico colgada del llavero.

Utilidades adicionales de las tarjetas

Algunos tipos de tarjetas pueden ser configuradas con utilidades adicionales, tales como:

- ***Antipassback* por áreas.** Cada usuario tendrá una tarjeta personalizada que le abrirá el acceso a una o varias zonas.

  Por ejemplo, dos usuarios tienen el mismo tipo de tarjeta, pero a uno de ellos le permitirá la entrada a varias estancias o áreas y a otro solamente a una.

- ***Antipassback* por tiempo.** Se puede configurar individualmente cada tarjeta para que abra determinadas puertas solamente en una franja horaria y no en otras.

  Por ejemplo, para restringir el acceso del personal de la organización fuera del horario laboral.

  También pueden hacerse tarjetas con caducidad en varias horas o varios días; por ejemplo, para entregarlas a las visitas o a técnicos externos que vienen a realizar servicios temporales.

- ***Antipassback* de acceso.** Impide que varios usuarios utilicen la misma tarjeta simultáneamente.

- **Fecha de caducidad.** Una fecha y hora a partir de la cual la tarjeta dejará de ser operativa.

  Por ejemplo, para el caso de personal contratado por un año. La tarjeta tendrá las restricciones horarias, por áreas u otras que le correspondan durante el tiempo de vigencia. A partir de entonces dejará de funcionar.

1.4 Llaves electrónicas de contacto *(touch memories)*

Una *touch memory* es una pastilla electrónica incluida dentro de una carcasa de acero inoxidable y montada en un soporte de material plástico. Es invulnerable al polvo, la suciedad, el calor, el agua, los campos magnéticos o los arañazos, a la vez que resulta cómoda de llevar, incluso colgada del llavero. También se conoce con el nombre de *iButton*.

↑ *Touch memory.*

Se utiliza poniendo en contacto la parte metálica con la equivalente del lector, que debe estar colocado junto a la puerta de acceso correspondiente.

Se le pueden aplicar las mismas configuraciones y restricciones que a las tarjetas de proximidad.

↑ Cerradura para *touch memory* con teclado.

ACTIVIDADES

7. Investiga y después responde. Los teclados para insertar un PIN o clave numérica:

a) Por sus características y fragilidad solamente pueden instalarse en el interior del edificio.

b) Existen modelos antivandalismo que también soportan bien las condiciones meteorológicas adversas.

8. Cada vez con más frecuencia se utilizan teclados para acceder incluso a las comunidades de vecinos. ¿Sería técnicamente posible que se dispusiese una clave distinta para cada piso de la comunidad?

9. Investiga. ¿Cuántos euros puede costar un teclado sencillo?

10. Y un lector de tarjetas de proximidad, ¿a partir de qué precio se puede encontrar?

11. ¿De qué tipo son las tarjetas que utilizan actualmente los cajeros automáticos de los bancos y cajas de ahorro?

12. Trabajas en una empresa donde se acaba de instalar un sistema de acceso por tarjetas, y tu jefe te solicita que prepares las tarjetas de acceso para cada empleado. A continuación tienes un listado del personal, indica qué tipo de utilidades adicionales deberán tener en su tarjeta: personal de limpieza, personal de vigilancia, trabajadores con horario de oficina, personal de mantenimiento.

13. Tienes que coger un avión para trasladarte a una oficina que tiene tu empresa en otra ciudad. En el control del aeropuerto, debes pasar por el escáner. Investiga si tendrás algún problema con tu *touch memory*.

14. ¿Una tarjeta magnética tiene más durabilidad que una tarjeta por aproximación? Explica tu respuesta.

15. En cuanto a la forma de usarse, ¿qué diferencia existe entre una *touch memory* y una tarjeta de aproximación?

16. Investiga. ¿Qué es una tarjeta neutra?

1.5. Sistemas biométricos

La biometría es el estudio de métodos que permiten reconocer a seres humanos basándose en factores genéticos o en determinados rasgos físicos o de conducta.

Aplicada a los sistemas de información, permite la autenticación de personas utilizando tecnologías electrónicas que usan fórmulas matemáticas complejas para asegurar, con un margen de error nulo o insignificante, que la persona que solicita su entrada a un recurso o a un espacio físico, es quien dice ser.

caso práctico inicial

La biometría es el estudio de métodos para reconocimiento de seres humanos por sus rasgos físicos o conductuales. Aplicado a las TIC, es un sistema perfectamente idóneo para la identificación y el control de acceso físico y lógico.

En la tecnología de la información podemos hablar de características físicas que identifican a una persona, tales como el iris, las huellas dactilares, la palma de la mano o los rasgos faciales. Pero también pueden identificarse personas basándose no en sus rasgos físicos, sino en sus hábitos o su comportamiento. Como ejemplos podemos citar la forma de andar, la firma o la escritura manual. La voz es una característica física pero también tiene una parte de comportamiento, en cuanto a las inflexiones de voz utilizadas en situaciones distintas.

Una característica física de indudable fiabilidad para la identificación de una persona es su ADN, si las muestras recogidas no han sido contaminadas.

↑ Antigua China. Huellas digitales en sellos de arcilla.

Orígenes de la biometría

Los actuales sistemas de medición biométrica utilizan las más altas tecnologías, pero se vienen utilizando desde hace cientos de años para identificar a las personas por sus características físicas únicas. Basta recordar las huellas dactilares en los documentos legales de identidad o las huellas de la planta del pie de los recién nacidos en los hospitales.

China, ya en el siglo XIV, es el primer país del que se tiene noción que utilizase la biometría como método de identificación infantil, mediante estampado de las huellas de la palma de la mano.

Se conoce que en la antigua Babilonia y en Persia se firmaban tablillas de arcilla o documentos de papiro mediante huellas dactilares.

En Occidente comenzó a utilizarse en el siglo XIX. Un oficial de la policía francesa, **Alphonse Bertillon,** ideó un modo de identificar a delincuentes. Al ser fichados se les tomaban medidas del contorno de la cabeza, piernas, brazos y dedos, estatura, color de ojos y del cabello, localización de cicatrices, lunares y otras marcas individuales del cuerpo. Si el delincuente reincidía, se hacían las comprobaciones en la ficha para tener la seguridad de que se trataba de la misma persona.

↑ Alphonse Bertillon.

Bertillon fue el creador de esa nueva ciencia llamada **antropometría** y el sistema se adoptó rápidamente en el resto de Europa y en Estados Unidos a partir de 1884. Hasta entonces solamente se habían utilizado en Europa sistemas de identificación visual.

Sin embargo, el sistema de Bertillon no era del todo infalible. Existía la remota posibilidad de que dos personas tuviesen las mismas medidas físicas e incluso señales parecidas y localizadas en el mismo punto del cuerpo.

↑ Identificación de dos individuos por comparación de rasgos a diferentes edades.

En 1892, el investigador de múltiples campos, médico y antropólogo británico **Francis Galton,** propuso el sistema de identificación mediante las **huellas dactilares,** dando lugar a la ciencia llamada **dactiloscopia,** basada en la unicidad del dibujo que forman las líneas en las yemas de los dedos de cada persona. Ya anteriormente se había utilizado la impresión de huellas dactilares en la firma de documentos mercantiles y algunos estudiosos, como Henry Faulds, habían apuntado a que estas huellas eran irrepetibles en distintas personas, pero es Galton quien profundiza en el estudio y publica un libro titulado *Fingerprints* en el que asegura que las huellas dactilares son únicas e invariables a lo largo de la vida de una persona.

El incremento de la seguridad con los sistemas de acceso biométricos

Los métodos de identificación personal para el control de acceso que hemos ido estudiando en esta unidad se basan en:

1. Algo que conoces. Es el caso de las contraseñas o palabras clave de acceso.

2. Algo que posees. Por ejemplo, una tarjeta magnética codificada.

Ambos métodos tienen sus inconvenientes, como el no recordar una contraseña o poseer una tarjeta u otro objeto de identificación pero no tenerlo disponible en el momento necesario, además del riesgo de suplantación de personalidad en caso de pérdida o robo de esa información o ese objeto.

↑ Sir Francis Galton.

En la actualidad las tecnologías de la información y la comunicación nos mantienen en contacto casi constante con recursos para los que se tiene o no permiso de acceso. Con el desarrollo de tecnologías biométricas, se ha dado un paso importante en el control de acceso, al agregar una nueva connotación a la identificación:

3. Una característica personal, como las huellas dactilares o el iris. Tienen la ventaja de que «la clave se lleva encima» y no dependen de la memoria. Al mismo tiempo, si se utilizan como referencia identificativa características determinantes de la identidad, como puede ser la huella dactilar, la fiabilidad del control se incrementa hasta acercarse al 100 %.

↑ Sistema de acceso combinado de huella dactilar y contraseña.

Si se combinan dos o más métodos, se consigue un nivel aún más alto de seguridad. Por ejemplo, para entrar en un recinto puede ser obligatorio pasar la palma de la mano por un detector y también introducir una contraseña.

Otro ejemplo de sistema combinado sería el de los cajeros automáticos, en los que un lector comprueba la banda magnética de la tarjeta y se solicita además la introducción de una contraseña. El ordenador verifica que la contraseña corresponde a la que está registrada para la banda magnética de esa tarjeta.

Indicadores biométricos

Para que un control de acceso con tecnología biométrica sea fiable debe crearse en torno a características humanas que tengan los siguientes indicadores:

- **Universalidad.** Todos los individuos poseen esa característica.
- **Unicidad.** La característica es distinta en cada individuo.
- **Permanencia.** No se modifica en el tiempo ni a corto ni a largo plazo.
- **Cuantificación.** Puede medirse con cualquier sistema (numérico, físico, matemático...).

Características exigibles a un sistema biométrico

- **Efectividad.** Su uso debe hacerse cómodo y rápido para los usuarios.
- **Aceptabilidad.** No debe provocar rechazo de las personas para someterse al reconocimiento ni puede ser peligroso para la salud o la integridad física.
- **Fiabilidad.** Ha de ser robusto, en el sentido de que sus resultados sean al máximo fiables y que no pueda ser trucado o utilizado de manera fraudulenta.

Funcionamiento de un sistema biométrico

El reconocimiento biométrico personal puede utilizarse de dos maneras distintas:

- **Identificación.** Una vez obtenidas las características biométricas de una persona, se introducen en una base de datos y se lleva a cabo una búsqueda para determinar a qué persona pertenecen. Es un proceso que puede utilizarse, por ejemplo, en las investigaciones policiales cuando se ha obtenido una prueba que contiene ADN del presunto autor de un delito. Si existe una base de datos de ADN y el de esa persona está recogido con anterioridad, se comparará la muestra con la base de datos y se conseguirá su identificación.
- **Verificación**. No se realiza una búsqueda como en el caso anterior, sino que se utiliza para verificar que una persona en cuestión es la que dice ser. Es el caso, por ejemplo, de la utilización de las huellas dactilares en un lector para permitir el acceso a una persona que tiene permiso de entrada. La persona en cuestión aportaría su identificación mediante nombre de usuario o contraseña y a continuación pasaría el dedo por un lector de huellas dactilares. Se efectúa la comprobación directa de que ese nombre o esa contraseña corresponden a sus huellas y se le permite o se le deniega el acceso.

Nivel de exigencia

Un sistema biométrico no es infalible. Podría darse el caso de un lector de huellas dactilares o uno del iris ocular de una persona autentificada para acceder al edificio o al sistema y no aceptarlo porque el nivel de exigencia que se ha marcado para ese dispositivo es muy alto.

Si en cambio el nivel de exigencia es bajo, se producirán menos falsos rechazos a la vez que aumentará el número de falsas aceptaciones (usuarios no autentificados a los que el dispositivo permite la entrada).

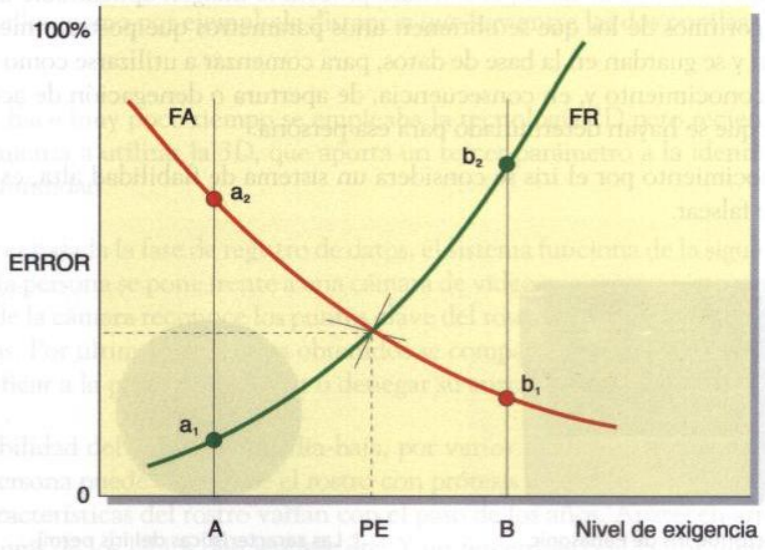
En la siguiente figura puede apreciarse la gráfica del nivel de exigencia relacionada con el porcentaje de error en falsas aceptaciones (FA) y falsos rechazos (FR).

El punto en el que se cruzan ambas líneas indica el punto de equilibrio deseable (PE).

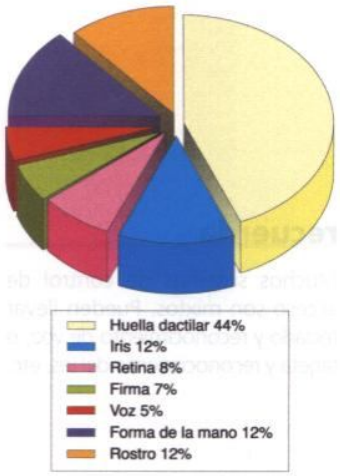
Puedes comprender mejor la gráfica si te fijas en la línea A que corta en un punto la curva FR y por otro la curva FA.

El punto A corresponde a un nivel de exigencia bajo, lo que arroja un número alto de falsas aceptaciones (a2) y bajo de falsos rechazos (a1).

Si avanzamos al punto B, en el que el nivel de exigencia al dispositivo se ha incrementado, entonces disminuye el número de falsas aceptaciones (b1) a cambio de un aumento considerable de falsos rechazos (b2).



↑ Curvas de falsas aceptaciones (FA) y falsos rechazos (FR) en función del nivel de exigencia del dispositivo biométrico.



↑ Proporción de uso de sistemas de reconocimiento biométricos a nivel mundial.

La fiabilidad de los sistemas biométricos es un tema que se sigue estudiando con la idea de conseguir un punto de equilibrio en el que el error sea muy próximo a cero, tanto para las falsas aceptaciones como para los falsos rechazos. Actualmente se admiten como buenos si dan una tasa de falsas aceptaciones inferior al 0,1 %, y de falsos rechazos, inferior al 2 %.

recuerda

Muchos sistemas de control de acceso son mixtos. Pueden llevar teclado y reconocimiento de voz, o tarjeta y reconocimiento del iris, etc.

Sistemas biométricos para el control de acceso a espacios físicos

La moderna biometría está diseñando constantemente sistemas de acceso biométrico a espacios físicos y a la información digital. Se aplica sobre patrones de las facciones, la retina, el termograma del rostro, la geometría de la mano, la voz y otros. A continuación relacionamos algunos de los sistemas más utilizados basándonos en patrones anatómicos. Los más sofisticados permiten comprobar si la identificación se realiza con un órgano vivo.

Iris

El iris es la parte que otorga color a los ojos y es inalterable a lo largo de la vida.

El lector identificador de iris se coloca próximo a los accesos. Puede ir sobre la pared o con un pie. En todo caso, los más cómodos tienen la altura regulable para adaptarla a personas de mayor y menor estatura.

Al realizarse la toma de datos, el software procesa la imagen aplicándole una serie de algoritmos de los que se obtienen unos parámetros que posteriormente se codifican y se guardan en la base de datos, para comenzar a utilizarse como medida de reconocimiento y, en consecuencia, de apertura o denegación de acceso a las áreas que se hayan determinado para esa persona.

El reconocimiento por el iris se considera un sistema de fiabilidad alta, es decir, difícil de falsear.

↑ Lector de iris de Panasonic.

↑ Las características del iris permiten que se considere un elemento anatómico único y diferenciable sobre el resto de seres humanos.

Manos

Uno de los sistemas más fiables de identificación por las manos consiste en captar el entramado de las venas que discurren por las palmas. La captación se hace desde un dispositivo que emite rayos casi-infrarrojos que al reflejarse en las manos, a causa de una propiedad de la hemoglobina, hace que en la imagen obtenida las venas se muestren de color negro. Del entramado se realiza una imagen digital y se conserva en una base de datos, que servirá para la posterior identificación y permiso de acceso de la persona registrada.

Fujitsu es el creador del sistema *Palm Secure* de identificación por las palmas de las manos. En sus investigaciones demuestra que no hay un entramado de venas igual a otro –ni siquiera en gemelos idénticos– y que el mismo patrón se mantiene a lo largo de la vida, únicamente ampliado con el crecimiento. Una vez tomadas y archivadas las muestras de reconocimiento, el control de acceso se lleva a cabo colocando la mano a unos centímetros del escáner lector.

Este sistema de identificación se considera de fiabilidad alta.

↑ Sistema *Palm Secure*, creado por Fujitsu.
FA < 0,00008%
FR = 0,01%

Reconocimiento facial

Los sistemas biométricos electrónicos basados en los rasgos faciales se basan en la colocación de puntos sobre la imagen del rostro y en la medición de las distancias entre ellos, como por ejemplo la distancia que hay entre las dos pupilas de un sujeto.

Hasta hace muy poco tiempo se empleaba la tecnología 2D pero recientemente se comienza a utilizar la 3D, que aporta un tercer parámetro a la identificación: la profundidad.

Una vez pasada la fase de registro de datos, el sistema funciona de la siguiente manera: la persona se pone frente a una cámara de vídeo que capta su imagen, el software de la cámara reconoce los puntos clave del rostro y hace el cálculo de las distancias. Por último, los valores obtenidos se comparan con la base de datos para identificar a la persona y admitir o denegar su entrada o salida.

La fiabilidad del sistema es media-baja, por varios motivos. Uno de ellos es que una persona puede disfrazarse el rostro con prótesis y otros añadidos. Otro es que las características del rostro varían con el paso de los años. Aparecen arrugas, las comisuras de los labios descienden, etc. Y un tercero sería el factor iluminación, pues según el foco de luz se producen sombras en el rostro que pueden confundir al sistema.

↑ Imagen de un vídeo que muestra un sistema de biometría facial desarrollado por la Universidad Carlos III de Madrid.

caso práctico inicial

A pesar de la fiabilidad que aportan los sistemas biométricos, no tienen por qué suponer un costo excesivo para las pequeñas y medianas empresas en las que no se necesita gran cantidad de puntos de control de acceso.

↑ Cerradura biométrica de huella dactilar con manivela y teclado.

Huellas dactilares

Desde que en 1892 Francis Galton propusiera la identificación de personas por sus huellas dactilares, este método ha sido el más utilizado en el mundo.

Aplicado a las tecnologías de la información y la comunicación, facilita la tarea de identificar y comparar huellas con bases de datos sin tener que emplear el reconocimiento visual.

↑ Cerradura dactilar de *TS Biometrics*.

El sistema empleado para extraer el patrón de las huellas dactilares de una persona es similar al que se utiliza para el iris ocular. La identificación posterior, al contrario que en la del iris, se realiza por contacto del dedo identificador sobre la superficie lectora del dispositivo.

En control de acceso electrónico basado en las huellas dactilares se emplea para la apertura de puertas y para el control de entradas, salidas y permanencia. De los sistemas biométricos que hemos visto, es el más empleado incluso en los hogares y pequeñas oficinas, entre otros motivos porque su coste no es muy elevado.

Este sistema es de fiabilidad media.

ACTIVIDADES

17. Busca en internet información sobre la tecnología Palm Secure y coméntala en clase.

18. ¿Un DNI digital puede suplantar nuestra identidad y nuestra personalidad jurídica?

19. Explica las ventajas de la autenticación biométrica.

20. ¿Cuál crees que es el principal riesgo que se deriva de los sistemas biométricos?

21. ¿Crees que la biometría evita el fraude? Razona tu respuesta.

22. ¿Cuál fue el primer país en utilizar la identificación de recién nacidos mediante la impresión en papel de los pies y las manos?

23. Investiga en internet sobre el carnet de identificación del recién nacido.

24. Investiga qué es el Eurodac.

25. Si es posible, visionad la película *Minority Report* y debatirla en el aula.

26. Anualmente se celebra en Londres la Feria de la Biometría en la que se exhiben las últimas novedades tecnológicas en torno a la identificación a través de rasgos biométricos.

La página del evento es www.biometrics.elsevier.com. Entra en esa página y contesta:

a) ¿En qué año ha sido la última edición de la Feria?

b) ¿Qué principales empresas *(main sponsors)* la patrocinaron?

↑ Imagen animada de la página principal de Biometrics.

(Continuación)

27. A la izquierda de la siguiente tabla hay un conjunto de características personales, físicas, fisiológicas o conductuales. En la parte superior están los indicadores biométricos. Marca en cada casilla qué indicadores cumple cada una de las características mostradas, suponiendo que se habla de personas adultas.

	Universalidad	Unicidad	Permanencia	Cuantificación
Estatura				
Color del cabello				
Peso				
Color del esmalte				
ADN				
Huella palmar				
Forma de andar				
Forma de la nariz				
Iris				
Huella dactilar				
Calor corporal				
Distancia entre pupilas				

28. Una vez completada la tabla anterior, podrás reconocer qué características humanas cumplen con los indicadores que requiere un control de acceso biométrico.

29. La siguiente tabla muestra en su parte de arriba tres grupos de sistemas de control:

a) Aquellos cuyo soporte es un objeto físico, como tarjetas, llaves mecánicas o electrónicas, etc.

b) Los que se utilizan introduciendo una contraseña o un PIN.

c) Los que usan características físicas, fisiológicas o conductuales de las personas.

A la izquierda hay una lista de sucesos o características que cada grupo tendrá o no, desde el punto de vista del usuario (persona que se somete al control de acceso). Marca en la tabla con una X si un grupo de arriba es susceptible o no de los eventos que se relacionan en la parte de la izquierda.

Por ejemplo, una característica biométrica, ¿es algo secreto para otras personas? ¿Es posible adivinar una clave? ¿Se puede compartir una tarjeta? ¿Puede ser robada una llave?

	Objeto físico		Clave conocida		Característica biométrica	
	Sí	No	Sí	No	Sí	No
Pérdida						
Olvido						
Robo						
Compartir						
Adivinar						
Secreto						

saber más

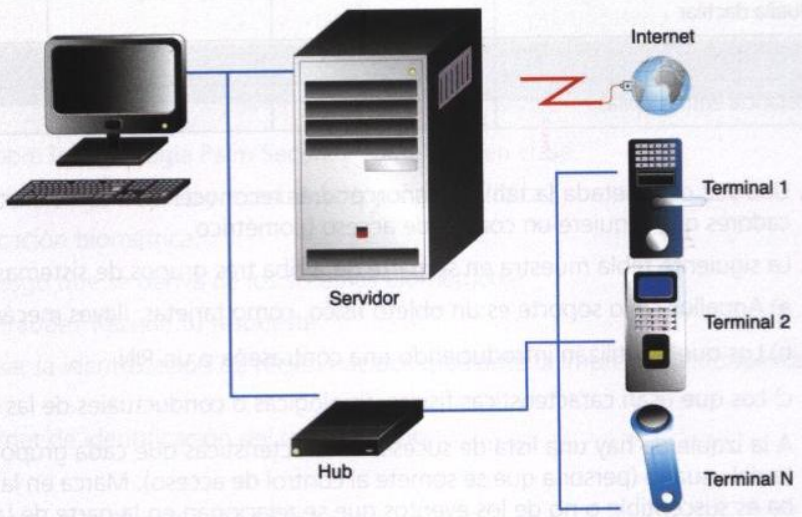
Algunas empresas que crean o distribuyen en España sistemas de control de acceso físico, incluso software de gestión:

- Bytech (www.by.com.es/). Ver sistema IMBY.
- Fermax (www.fermax.es).
- Grupo SDI (www.sisdid.com).
- CTS (www.controltime.net/).
- Inditar (www.inditar.com).
- Kimaldi (www.kimaldi.com/).
- Aike (www.aike.com/).
- Bodet (www.bodet.es). Ver sistema Kelux.
- MMSistemas (www.mmsistemas.es).

2. Integración y centralización de sistemas de control de acceso

Además de los sistemas que se han mostrado en esta unidad, existen otros como molinetes, tornos, portillos, lector de matrículas de vehículos, etc. Los diferentes sistemas de control de acceso, tanto si son dependientes como autónomos convertibles, pueden centralizarse en un potente ordenador al que estarán conectados y que gestiona esos recursos mediante un software dedicado. El software suele ser un paquete de aplicaciones integradas que proporciona todas las utilidades necesarias para la gestión y el control de accesos: puntos de control, altas, bajas y modificación de datos de usuarios, configuración de tarjetas y otros elementos de control de usuarios, creación de privilegios, identificación, confección de nóminas en función del registro de horas trabajadas, ausencias o retrasos, control de alarmas, etc.

La decisión de integrar o no los distintos sistemas en una unidad de control, depende de las necesidades de cada negocio y de la rentabilidad que le proporcione, teniendo en cuenta el coste de la centralización y el incremento o ahorro en gastos de personal.



↑ Conexión TCP/IP a través de Hub.

3. Competencias del técnico en sistemas microinformáticos y redes

El estudio de necesidades de cada caso en particular, el presupuesto y la instalación de los sistemas de control de acceso son realizados por las empresas que los distribuyen o por profesionales de la electrónica.

La persona que se ocupe de la instalación y mantenimiento del sistema informático y de las redes ha de tener conocimiento de cuáles son las medidas de seguridad que protegen el entorno físico, tanto las que se vieron en la unidad anterior como las relativas al control de acceso, y en la medida de lo posible, asesorar sobre la conveniencia o no de instalar algunos de estos sistemas.

PRÁCTICA PROFESIONAL

Biometría y reconocimiento de personas

Una vez terminado el aprendizaje de esta unidad y realizadas todas las actividades, se debe tener una idea muy clara de lo que es el control de acceso a un edificio, un local o cualquier espacio físico en donde se lleve a cabo la actividad de una empresa o institución. Habremos visto que cualquier empresa, por pequeña que sea, puede adoptar sistemas de control de acceso y de vigilancia sin que le suponga un coste inasumible, porque hay sistemas bastante económicos. Y también sabremos que el control de acceso tiene repercusión indirecta –y a veces muy directa– sobre la seguridad informática y la protección de la información. Esta práctica profesional será de investigación, análisis y crítica.

OBJETIVOS

- Averiguar cuál es el único sistema biométrico que puede utilizarse a distancia, es decir, cuando la persona no está presente.
- Considerar si los sistemas de control de acceso, y en particular la biometría, suponen una mayor garantía de seguridad sobre personas y bienes en relación a otros sistemas.
- Considerar qué requisitos deben cumplir los sistemas de control de acceso, y en particular los biométricos, para que se garantice la libertad individual y el derecho a la privacidad.
- Ofrecer un punto de vista personal (o de grupo) sobre la incidencia de los actuales métodos de vigilancia y control sobre la libertad de las personas.

INSTRUCCIONES

Primera parte

Busca vídeos en Youtube con la palabra clave «biometría» o «acceso biométrico».

Sugerencias: http://www.youtube.com/watch?v=NT0GVSNgVr8

http://www.youtube.com/watch?v=ZTcOPyrpF_Y

http://www.youtube.com/watch?v=0Gg7YkEH-9o&NR=1

En los vídeos encontrarás parte del contenido de esta unidad, y otros sistemas, pero ante todo podrás ver en funcionamiento algunos de los que se han desarrollado aquí.

Toma nota de aquello que te suscite un mayor interés o curiosidad.

PRÁCTICA PROFESIONAL

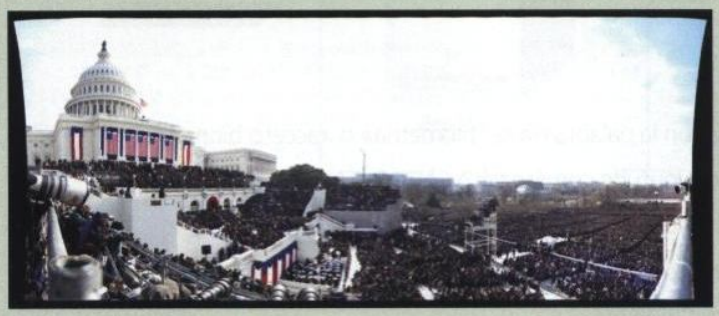
Segunda parte

No se trata de un sistema biométrico, pero lo agregamos como algo novedoso y que tiene que ver con el reconocimiento de personas. En la página web www.gigapan.org se exponen fotografías panorámicas con una extrema definición, tal que utilizando el ratón podemos acercarnos a personas lejanas y apreciar perfectamente sus rasgos, o reconocer matrículas de vehículos, etc.

Sugerencia: puedes ver la fotografía que se encuentra en esta dirección:

http://gigapan.org/viewGigapanFullscreen.php?auth=033ef14483ee899496648c2b4b06233c

Si lo prefieres, una vez abierta la página de Gigapan, escribe **Obama President** en el recuadro de búsqueda. Una vez localizada la imagen del capitolio, individualiza personas y trata de encontrar al presidente Obama.



Tercera parte

Lee algún artículo publicado en internet u otro medio en el que se hable de **libertad y seguridad.**

Sugerencia: «Seguridad contra libertad», de Andrés Aberasturi, publicado en *La Opinión de Málaga* el 21 de noviembre de 2009.

Ver http://www.laopiniondemalaga.es/opinion/2009/11/21/seguridad-libertad/303833.html

Resuelve

1. Individualmente o en grupo, estudia la documentación sugerida y realiza un informe que contenga al menos las cuestiones que se fijan en los objetivos.

MUNDO LABORAL

Kaba: tecnología de identificación RCID para el control de acceso

Durante la última edición de la *Feria Internacional Security Essen,* celebrada el pasado mes de octubre en esta ciudad alemana, Kaba ha sido galardonada con el *Security Innovation Gold Award* por su innovadora tecnología de identificación RCID. Esta solución, capaz de compatibilizar la máxima seguridad en accesos con la total comodidad de los usuarios, subraya el papel desempeñado por la compañía de origen suizo como líder tecnológico dentro del sector de la seguridad.

El sueño del futuro se ha hecho realidad

Durante los últimos tres años, un equipo de investigadores de Kaba, dirigido por el Dr. Andreas Häberli, director de desarrollo, ha estado trabajado en nuestros laboratorios de Wetzikon (Suiza) en una de las tecnologías más revolucionarias que se han desarrollado en los últimos años y que, sin duda alguna, marcará el futuro de los sistemas de cierre: la innovadora tecnología de identificación RCID *(Resistive Capacitive Identification).*

Esta tecnología es la consecución de un viejo sueño para muchos investigadores. Como reconoce el propio Häberli, «*nosotros no hemos inventado la idea de transmitir datos a través del cuerpo humano*». Ya en los años 60, algunos inventores andaban dándole vueltas; incluso, a mediados de los 90, miembros del Instituto Tecnológico de Massachusetts consiguieron algún resultado en esa línea. Pero hasta ahora, ninguna patente había demostrado ser comercialmente viable. (...)

Tecnología RCID, la protección más segura

Utilizando la carga electrostática natural del cuerpo humano, la tecnología de identificación RCID hace posible que solo con que una persona toque una superficie de metal receptiva de electrodos, como, por ejemplo, la manivela de una cerradura, se pueda comprobar la autorización de acceso de esa persona.

De acuerdo con esta concepción del método de identificación, creo conveniente hacer dos importantes consideraciones:

Primera. A diferencia de los sistemas basados en radiofrecuencia (RFID), podemos decir que la nueva tecnología Kaba RCID tiene una selectividad inherente, en otras palabras, que consigue un importante incremento de la seguridad frente a intercepciones casuales. Al utilizar la carga electrostática del propio cuerpo, esta tecnología RCID hace un uso muy eficiente de la energía, reduciendo al mínimo los aportes externos de energía y contribuyendo así a un mayor confort para los usuarios.

Segunda. Por otro lado, lo que también diferencia a la nueva tecnología RCID de los sistemas RFID –el Bluetooth, por ejemplo– es su prevención ante radiaciones durante los procesos de transmisión de información. Si siempre que se hace uso de la electrónica, surgen dudas respecto a su tolerancia por parte del cuerpo humano y a su posible efecto *electrosmog* (contaminación electromagnética por radiaciones nocivas para la salud: jaquecas, insomnio, dificultades de concentración...), en el caso de la tecnología RCID, el cuerpo no sufre carga alguna. Y es que la fuerza electrostática que utiliza para la transmisión de señales, es millones de veces menor que la que se produce en acciones tan cotidianas como el cepillado del cabello o las conversaciones con teléfono móvil.

Por lo tanto, la innovadora tecnología desarrollada por Kaba permite un alto nivel de seguridad en el control de acceso y el máximo confort para el usuario, pero garantiza también un método seguro para este.

MUNDO LABORAL

Kaba TouchGo, marcando el camino del mañana

En definitiva, estamos hablando de una tecnología que aportará muchas ventajas en el futuro y que, sin duda alguna, marcará la evolución de los sistemas y dispositivos de control de acceso. Una tecnología que por futurista que pueda parecer, es ya una realidad. De hecho, los primeros productos dotados de esta tecnología llegarán al mercado en el verano de 2009. Su nombre: Kaba TouchGo.

Con estas nuevas soluciones, Kaba consolida, una vez más, su posición mundial como pionera y líder en la innovación de sistemas de cierre, y demuestra cómo convertir la alta tecnología en aplicaciones prácticas para la vida diaria.

La primera aplicación de la tecnología Kaba RCID fue presentada por primera vez al público en el Salón del Automóvil de Ginebra, de 2007, como parte del prototipo de coche *Rinspeed eXasis*.

El vehículo –apodado el «coche de cristal», por su aspecto totalmente transparente– podía reconocer si una persona estaba autorizada para ponerlo en marcha, sin necesidad de hacer uso de una llave, solo mediante el tacto. Lo que parecía imposible se hacía realidad gracias a un dispositivo que transportaba la autorización de acceso y que la persona podía llevar en un bolsillo o a modo de pulsera, y a la innovadora tecnología de identificación desarrollada por Kaba. La solución, además de garantizar un acceso seguro al vehículo, permitía que las funciones y mandos de este se adaptasen de manera automática a las preferencias de cada uno de los conductores autorizados.

En cuanto a la comercialización de productos basados en la tecnología Kaba RCID, está previsto que para el verano de 2009 la compañía de origen suizo lance al mercado Kaba TouchGo, la primera gama de sistemas de cierre RCID.

Adaptado de KABA – Sala de prensa

http://www.kaba.es/Sala-de-prensa/Prensa/Notas-de-prensa/25818_243812/tecnologia-de-identificacion-rcid-generico.html

Actividades

Después de leer la noticia publicada por Kaba, responde a las siguientes cuestiones:

1. ¿Cómo se llama la tecnología desarrollada por Kaba y cuáles son las siglas en inglés de esta tecnología?

2. ¿Se puede utilizar esta tecnología para el control de acceso?

3. ¿En qué aspecto biométrico se basa?

4. ¿Qué aspectos no negativos sobre la salud señala Kaba sobre su sistema?

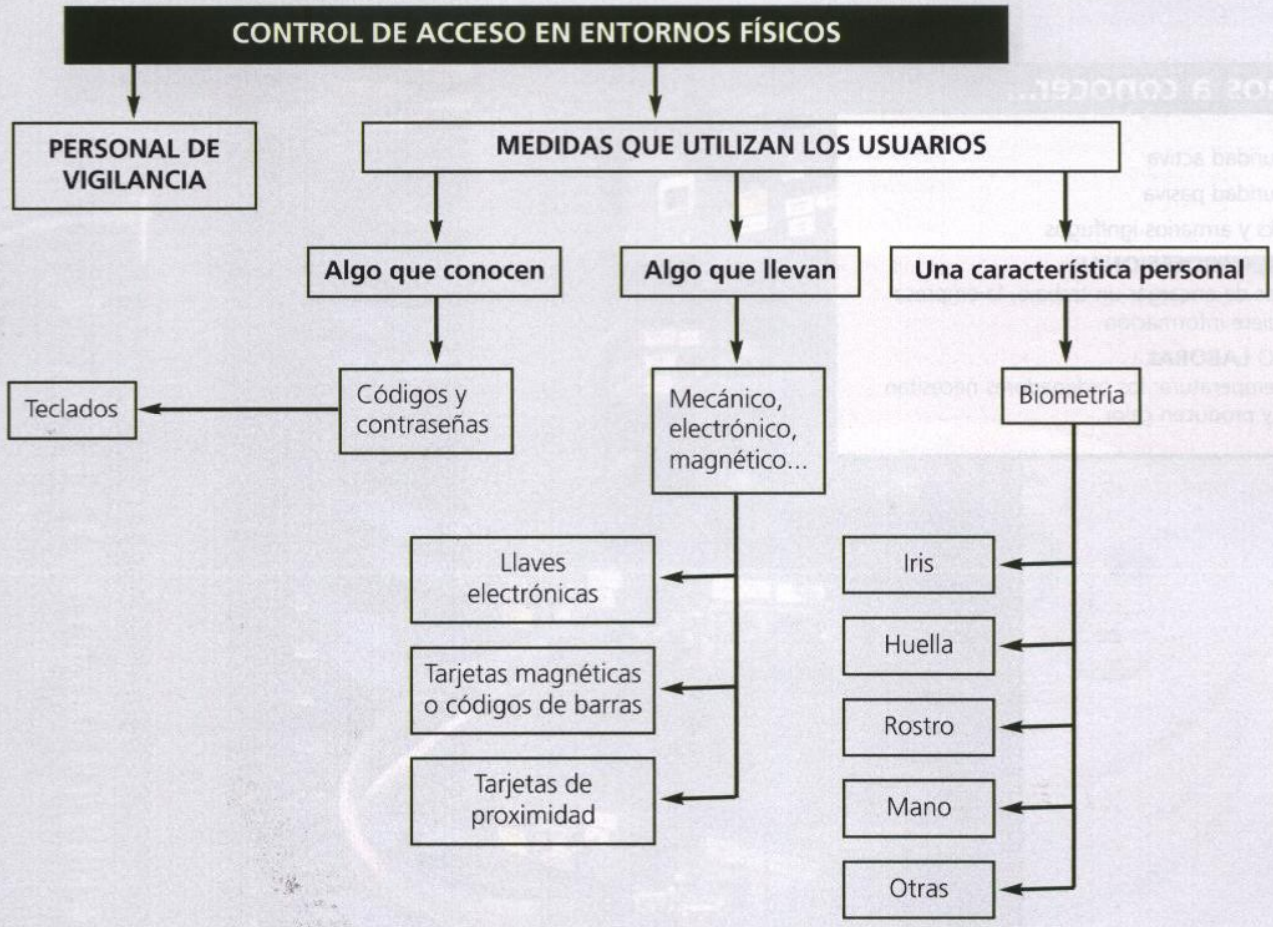
5. ¿Se utilizan las huellas dactilares o las de la palma de la mano para la identificación y el acceso?

6. ¿Qué premio ha obtenido la compañía por esta tecnología?

7. ¿En qué país está su sede central?

8. Cuando la noticia fue publicada por Kaba, estaba previsto sacar al mercado esta tecnología bajo el nombre Kaba TouchGo. Comprueba si a fecha actual existen aplicaciones en el mercado basadas en este sistema.

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **En seguridad informática, el control de acceso al entorno físico tiene como objetivo final:**
   a) La protección de las instalaciones.
   b) La protección de las personas.
   c) La protección de la información.
   d) El reconocimiento de intrusos.

2. **Un sistema autónomo convertible:**
   a) Puede conectarse a un PC.
   b) Va conectado a un PC que lo gestiona.
   c) No puede conectarse a un PC.
   d) Ninguna de las anteriores respuestas.

3. **¿Qué lector no es biométrico?**
   a) De tarjetas de proximidad.
   b) De la forma de la mano.
   c) De la huella palmar.
   d) De firma.

4. **El personal de vigilancia:**
   a) Es un sistema autónomo.
   b) Es un sistema autónomo convertible.
   c) Es un sistema biométrico.
   d) No es un sistema tecnológico.

Soluciones: 1c, 2a, 3a, 4d

4 Seguridad del hardware

vamos a conocer...

1. Seguridad activa
2. Seguridad pasiva
3. *Racks* y armarios ignífugos

PRÁCTICA **PROFESIONAL**
Antes de encargar un trabajo, la empresa requiere información

MUNDO **LABORAL**
La temperatura: los ordenadores necesitan frío y producen calor

y al finalizar esta unidad...

- Comprenderás la importancia de mantener una alimentación eléctrica de forma ininterrumpida.
- Conocerás las diferencias de aplicación y resultados entre SAI, regleta y grupo electrógeno.
- Conocerás distintos modos de monitorizar el hardware, tanto mediante el método software como mediante el método hardware.
- Apreciarás la importancia de la utilización de componentes homologados y de buena calidad para la conducción eléctrica y protección general del hardware.
- Sabrás qué son los mecanismos de tolerancia a fallos.
- Conocerás los métodos más interesantes de renovación de equipos y de contar con equipos de sustitución para emergencias.

CASO **PRÁCTICO** INICIAL

situación de partida

Estás en el mundo laboral. Tienes la oportunidad de montar una empresa pero te surgen dudas. Sabes que tu empresa dará servicio a través de internet las 24 horas del día los 365 días del año y no puedes permitir que se corte la comunicación.

Tendrás sistemas sensibles que deben ser monitorizados y la seguridad de los empleados y los equipos es la máxima en tu empresa.

↑ El sistema requiere un ajuste fino y debe funcionar a la perfección. La seguridad no puede fallar.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Como todo empresario, esperas que sea un proyecto a largo plazo, por lo que te planteas una estrategia para la adquisición, mantenimiento y renovación de equipos.

- ¿Cómo piensas lograr que todo el sistema funcione siempre al margen de los problemas, cada día más comunes, de corte de suministro?
- ¿Quién se encarga de controlar, y con qué software, el funcionamiento de los equipos?
- Sabes que vas a hacer una instalación limpia y bien mantenida, pero ¿cómo piensas lograrlo?
- ¿Cuál será tu política de renovación de equipos y plan de actuación frente a averías?

1. Seguridad activa

En esta unidad trataremos todos los aspectos importantes en la **seguridad del hardware.**

Dedicaremos nuestro esfuerzo a **proteger** nuestro **sistema,** porque proteger el hardware implica mantener a salvo los **datos** con los que trabajamos.

Tendremos en cuenta la protección frente a **terremotos** y **tormentas eléctricas,** aprenderemos a realizar un **mantenimiento** adecuado y protegeremos todos los sistemas frente a **cortes de electricidad,** tanto breves como prolongados, en función de los requisitos de nuestra instalación.

Podremos **renovar** los equipos gracias a una eficiente **gestión financiera** y estaremos al tanto de su funcionamiento con los sistemas de **monitorización del hardware.**

Comenzaremos por los sistemas, componentes y herramientas que aseguran de forma activa nuestro hardware.

1.1. SAI

saber más

Las siglas en inglés para SAI son **UPS** ***(Uninterruptible Power Supply).***

Los **sistemas de alimentación ininterrumpida,** también llamados SAI, constituyen un elemento básico en la protección de nuestro hardware y, por extensión, de los datos almacenados en él.

A pesar de lo que su nombre nos pueda sugerir, estos dispositivos no sirven para seguir trabajando durante un corte de electricidad prolongado, sino que nos permiten **guardar** con seguridad los **datos** si falla el suministro eléctrico.

↑ **LAPC 700VA 405W**

Este SAI es ideal para ordenadores domésticos o de pequeñas oficinas. Tiene ocho tomas, de las cuales cuatro poseen batería de respaldo más protección contra sobretensiones y las otras cuatro solamente tienen protección contra sobretensiones. Además cuenta con protección contra sobretensiones en redes Ethernet 10/100 Base-T. Ofrece una protección de hasta 58 minutos de autonomía.

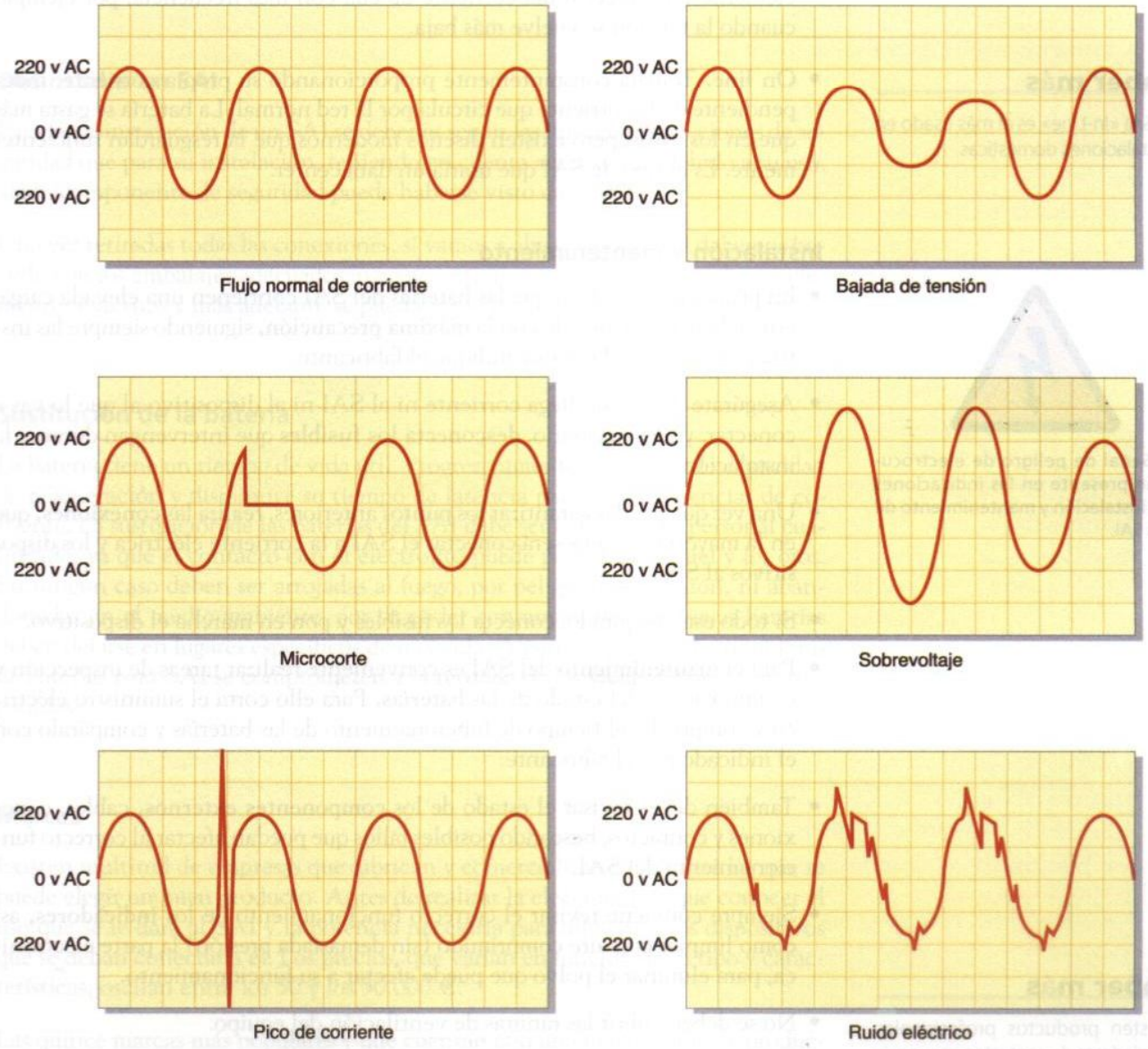
Problemas que soluciona un SAI

Como se comentó antes, los SAI no sirven para seguir trabajando de forma normal cuando haya un corte de electricidad prolongado, sino que suministran energía al ordenador u otro periférico durante un tiempo limitado para poder salvar los datos necesarios y apagar con seguridad nuestros sistemas.

Los problemas que solucionan los SAI son muy variados, desde el comentado **corte de electricidad** (denominado **interferencia en la red eléctrica o microcorte** si dura aproximadamente un segundo) hasta el **sobrevoltaje,** es decir, un voltaje mayor que el máximo previsto para el buen funcionamiento de los dispositivos, así como bajadas de tensión, ruido eléctrico y picos de corriente.

saber más

Se llama **ruido eléctrico** a las fluctuaciones en la línea normal de la corriente eléctrica que se producen por la interferencia de dispositivos electrónicos. Si la corriente eléctrica se ve alterada por un fuerte ruido eléctrico puede causar daños a equipos y componentes.



Los SAI, además, protegen contra **descargas de rayos** y **variaciones de frecuencia.**

Principales tipos de SAI

Existen varias topologías de SAI, aunque podríamos agruparlos en tres grandes grupos: **Standby, Interactivos** y **On line.**

- **Standby.** Suelen utilizarse en ordenadores personales. Cuando existe corriente eléctrica, hay una línea directa –no obstante con algunos filtros– que pasa a través del SAI hasta la conexión con el ordenador (u otro elemento que se desee proteger), con lo que apenas corrige las imperfecciones del suministro eléctrico.
- **Interactivo.** Es un SAI de tipo medio, que se suele utilizar para ordenadores personales o pequeños servidores. Ofrece más protección que el de tipo Standby pero la batería suele durar menos tiempo que en aquellos, porque el elemento a proteger toma corriente de ella con más frecuencia, por ejemplo cuando la tensión se vuelve más baja.
- **On line.** Trabaja constantemente proporcionando su propia corriente, independiente de la corriente que circula por la red normal. La batería se gasta más que en los otros, pero existen diseños modernos que la resguardan suficientemente. Es el tipo de SAI que usaría un data center.

saber más

SAI de tipo Standby

Solamente cuando las imperfecciones superan la cota que el SAI tiene programada o cuando se ha producido un corte de fluido, se desactiva esa línea directa y se desvía la toma de corriente hacia la batería, que se habrá ido cargando de forma automática cuando el SAI ha recibido electricidad por la red.

saber más

El SAI «In-Line» es el más usado en instalaciones domésticas.

Instalación y mantenimiento

↑ Señal de peligro de electrocución presente en las indicaciones de instalación y mantenimiento de los SAI.

- En primer lugar, y dado que las baterías del SAI contienen una elevada carga, este deberá ser manejado con la **máxima precaución,** siguiendo siempre las instrucciones particulares que indique el fabricante.
- Asegúrate de que no llega corriente ni al SAI ni al dispositivo al que lo vas a conectar, y si es necesario, **desconecta los fusibles** que intervengan durante la instalación.
- Una vez que puedas garantizar los puntos anteriores, realiza las **conexiones,** que en la mayoría de casos será conectar el SAI a la corriente eléctrica y los dispositivos al SAI.
- Si todo está asegurado, conecta los fusibles y pon en marcha el dispositivo.
- Para el **mantenimiento** del SAI es conveniente realizar tareas de inspección y comprobación del estado de las **baterías.** Para ello corta el suministro eléctrico y comprueba el tiempo de funcionamiento de las baterías y compáralo con el indicado por el fabricante.
- También debes revisar el estado de los **componentes externos,** cables, conexiones y contactos, buscando posibles fallos que puedan afectar al correcto funcionamiento del SAI.
- Siempre conviene revisar el correcto funcionamiento de los **indicadores,** así como limpiar con aire comprimido (sin demasiada presión) la parte electrónica, para eliminar el polvo que puede afectar a su funcionamiento.
- No se deben cubrir las ranuras de ventilación del equipo.
- Puedes comprobar, además, los valores eléctricos del SAI, tanto con dispositivos externos, como el osciloscopio, como mediante software, que requerirá la instalación de los *drivers* adecuados.

saber más

Existen productos profesionales limpiadores de contactos para equipos eléctricos y electrónicos. No dejan residuos ni conducen electricidad.

Configurar un SAI

La mayoría de los SAI para uso doméstico no requieren una configuración aparte de las conexiones explicadas anteriormente.

Algunos modelos incluyen **software y drivers** para la monitorización del adecuado funcionamiento del sistema, y además los hay que permiten la conexión mediante **USB** del SAI al ordenador, y a través de una interfaz se pueden configurar los **tiempos de uso** de la batería antes del apagado seguro, así como las **alarmas** establecidas para diversos eventos.

Debes tener en cuenta que cada fabricante da sus propias instrucciones de instalación y configuración para cada equipo específico, y siempre se han de **seguir** estas **instrucciones.**

Desinstalar un SAI

Para la desinstalación de un SAI se deberán seguir las mismas instrucciones de seguridad que para su instalación, teniendo en cuenta además que, debido a su uso, algún componente de seguridad puede haberse visto dañado.

Una vez retiradas todas las conexiones, si vamos a almacenar el SAI debemos hacerlo con los embalajes adecuados, para garantizar que no se vea afectado por elementos externos y más adelante se pueda instalar sin riesgos mayores.

Sustitución de la batería

La batería tiene un tiempo de vida útil. Progresivamente va perdiendo capacidad de regeneración y disminuye su tiempo de latencia para cubrir ausencias de corriente. La sustitución de las baterías del SAI debe ser realizada por personal cualificado, ya que el contacto con el electrolito puede perjudicar la piel y los ojos. En ningún caso deben ser arrojadas al fuego, por peligro de explosión, ni abandonadas en el medio ambiente, por su poder contaminante. Las viejas baterías deben dejarse en lugares específicos de recogida. Algunas empresas distribuidoras de baterías para SAI se comprometen a la retirada de las viejas cuando sean sustituidas.

Marcas

Existen multitud de empresas que fabrican y comercializan SAI, entre las que se puede elegir un buen producto. Antes de realizar la elección, hay que conocer el uso que se le dará al SAI y la potencia necesaria para alimentar los dispositivos que se deban conectar a él. Los precios, que varían en función de su tipo y características, oscilan entre los 50 y los 50.000 €.

Las quince marcas más populares y que cuentan con una mayor gama de productos de alimentación ininterrumpida de venta en España son, en este orden: APC, Merlin Gerin, Riello, Zigor, Hewlett Packard, Apple, Energizer, Trust, Belkin, MGE, Sony, Unitec, Soyntec, Enelecsys y Cegasa.

ACTIVIDADES

1. ¿Qué es un SAI?

a) Sistema alimentación inmediata.

b) Sistema alimentación interactivo.

c) Sistema alimentación ininterrumpida.

d) Sistema automático informático.

2. Un SAI permite seguir trabajando con normalidad durante un apagón, sea cual sea la duración:

a) Sí.

b) No.

3. Marca los problemas que creas que soluciona un SAI:

a) Breve corte de suministro.

b) Gran corte de suministro.

c) Calentamiento excesivo de la CPU.

d) Sobrevoltaje.

e) Reduce el ruido que emite el dispositivo.

4. Para realizar un correcto mantenimiento es necesario:

a) Nada, el SAI no requiere mantenimiento.

b) Revisar las baterías.

c) Limpiar los conectores.

5. ¿Qué topología de SAI se prefiere por sus buenas prestaciones y su bajo costo para ordenadores personales?

a) Standby.

b) Interactivo.

c) On line.

6. Indica el orden de los pasos necesarios para instalar y configurar correctamente un SAI:

- Instalar los *drivers*.
- Tomar precauciones previas.
- Configurar las opciones deseadas.
- Realizar las conexiones necesarias.
- Leer las instrucciones propias del fabricante.

7. Busca en internet algunas marcas que fabriquen SAI. Enuméralas.

8. ¿Qué topología de SAI se suele utilizar en un *data center?*

a) Standby.

b) Interactivo.

c) Online.

1.2. Regletas protectoras

Las regletas protectoras son, en la mayoría de los casos, una solución barata al problema de las **subidas de tensión.**

No son comparables a los SAI ya que no protegen de los cortes de suministro, pero pueden ser útiles para proteger nuestro hardware, por un módico precio, de la acción de rayos, bajadas y subidas de tensión o ruido eléctrico. Pueden incluir un interruptor general y un mando a distancia para apagarlas y ahorrar la energía que consumen los equipos en estado de reposo.

↑ Supresor de sobrevoltaje Trust Surge Guard Deluxe PW-3700.

1.3. Grupos electrógenos

En la unidad 2 vimos un avance de lo que son los grupos electrógenos, que ahora vamos a ampliar. Se llama grupo electrógeno la maquinaria que **genera electricidad** mediante un **motor de combustión interna.**

↑ Generador diésel monofásico de baja potencia ID-TEK 5500.

Este tipo de maquinaria se emplea en lugares donde es vital poder seguir trabajando sean cuales sean las condiciones. Es habitual conectar a los grupos electrógenos los **sistemas críticos** de hospitales y todos los **sistemas de seguridad** que, en caso de un corte de suministro prolongado, deben seguir funcionando.

Es fácil encontrar grupos electrógenos dando apoyo a **servidores** y **centros de datos** en prácticamente cualquier empresa mediana-grande. En caso de un corte en el suministro eléctrico, los SAI garantizarán el correcto apagado y salvado de datos en los ordenadores personales, y el grupo electrógeno garantizará que se pueda seguir accediendo a recursos vitales.

La mayoría de grupos electrógenos poseen varios **tipos de arranque,** principalmente **manual** y **automático.** Configurar adecuadamente el arranque automático, mediante las conexiones necesarias, permite que en el momento en que el sistema detecte un fallo, este se encienda y comience a dar corriente.

caso **práctico** inicial

Los problemas de falta prolongada de suministro se evitan si se cuenta con un grupo electrógeno debidamente instalado y revisado.

Elementos que forman un grupo electrógeno

De forma genérica podemos decir que un grupo electrógeno cuenta con los siguientes elementos:

- **Motor.** Será el encargado de generar energía mecánica. Suelen encontrarse en dos versiones, diésel y gasolina, pero el primero es el más utilizado.
- **Alternador.** Se encarga de transformar la energía mecánica del motor en corriente eléctrica.
- **Tubo de escape.** Al usar un motor de combustión, se generan gases que son expulsados al exterior a través del tubo de escape.
- **Depósito.** Es el lugar donde se almacena el combustible.
- **Reguladores e indicadores.** El grupo electrógeno permite regular las revoluciones por minuto del motor, lo que hará que varíe la potencia obtenida.
- **Chasis y protecciones.** Todo el grupo electrógeno va instalado sobre un chasis que, según el tamaño, permitirá su transporte con mayor comodidad. Cuenta también con numerosas protecciones que permiten su uso en exterior e interior con la adecuada seguridad.

saber más

Cuando coloques un grupo electrógeno en una zona interior, debes tener muy en cuenta la ventilación del lugar, haciendo las instalaciones necesarias que garanticen la seguridad.

Además, a los grupos electrógenos se les pueden instalar elementos adicionales que permiten su funcionamiento de forma ininterrumpida, como por ejemplo una bomba que suministre combustible de forma continua.

En lugares donde se alcancen temperaturas muy bajas se les podrá acoplar un dispositivo calefactor, que ayudará en el arranque del grupo electrógeno.

ACTIVIDADES

9. Ya se ha comentado en esta unidad que los grupos electrógenos tienen diversas aplicaciones, desde centros de datos hasta hospitales. Haz un trabajo de investigación con algún compañero o compañera e indica en qué otros lugares es necesario un grupo electrógeno y por qué. Infórmate de marcas y modelos, combustible usado y fiabilidad del mismo.

10. Consulta en alguna tienda especializada o busca en internet para encontrar el precio de una regleta protectora. Escribe a continuación tu respuesta y compara las características y precio de tu regleta con la de tus compañeros.

11. Elige la opción u opciones que creas más adecuadas:

a) La regleta protectora cubre las mismas necesidades que un SAI.

b) La regleta protectora ofrece protección contra las subidas de tensión.

c) La regleta protectora ofrece protección contra breves cortes de suministro.

d) El SAI hace el trabajo de la regleta protectora además de otras funciones.

12. Elige la opción u opciones correctas. El grupo electrógeno:

a) Genera corriente eléctrica mediante un motor de combustión externa.

b) Genera corriente eléctrica a través de un motor eólico.

c) Genera corriente eléctrica usando un motor de fusión.

d) Genera corriente eléctrica a través de un motor de combustión interna.

13. ¿Qué elementos de una instalación informática conectarías a un grupo electrógeno?

14. Indica al menos tres elementos comunes en todos los grupos electrógenos y uno opcional.

1.4. Monitorización del hardware

La monitorización del hardware se usa para **comprobar** el correcto **funcionamiento** del sistema y detección de errores en los componentes físicos, como la temperatura de la CPU y otros componentes o la velocidad de giro de los ventiladores.

Para ello usaremos diferentes medios, tanto de software como de hardware.

Método hardware

Se puede comprobar el funcionamiento de un componente midiendo las **magnitudes eléctricas** de los elementos que forman parte del sistema.

En algunos casos puede resultar una tarea complicada, pero en otros, como la fuente de alimentación, será sencillo y la mejor forma de comprobar que todo funciona correctamente.

Para estas tareas usaremos un **polímetro.** Este es un instrumento que nos permite conocer las corrientes de un determinado dispositivo. La mayoría de los modelos incluyen una rueda que permite seleccionar la magnitud que vamos a medir.

Para medir, por ejemplo, la corriente continua de una fuente de alimentación, usaremos la opción DCV.

En muchos casos, además, podremos usar la vista como elemento para el reconocimiento de problemas de hardware.

Piezas en mal estado (por ejemplo, quemadas), mal instaladas o la suciedad, son causa de problemas en el hardware que difícilmente serán detectados mediante software, pero se verán a simple vista con una atenta mirada.

Método software

La monitorización del hardware a través de programas es el método más utilizado. Cada vez los programas son más completos y ofrecen información importante que puede ser de utilidad no solo en la detección de errores, sino a la hora de comprobar el rendimiento de nuestro ordenador para un determinado programa o sistema operativo en concreto.

Prácticamente cualquier software analiza el uso de la **CPU,** la memoria **RAM** disponible, consumida y libre restante, el **disco duro** y el uso que hacemos de él, así como de la **tarjeta gráfica** y las características de los **buses** de nuestro PC.

Para realizar tareas de monitorización específicas siempre es deseable usar un software destinado a tal fin. Por norma general, un usuario final podrá adquirir **licencias de software** a un módico precio o utilizar versiones gratuitas.

Como **ejemplo** usaremos capturas usando el software **Everest Home Edition,** propiedad de la empresa **Lavalys.** Podéis encontrar toda la información sobre sus productos de software en la web www.lavalys.com

↑ Polímetro.

saber más

Además del polímetro digital, pueden utilizarse otros tipos de medición: polímetro analógico, voltímetro.

caso **práctico** inicial

El software de monitorización del hardware permite detectar el mal funcionamiento de los componentes de un equipo informático, como por ejemplo la velocidad del ventilador de la CPU, indicada por un exceso de temperatura de la misma.

saber más

Utilizando software de monitorización del hardware, normalmente se muestran constantemente los valores instantáneos de las temperaturas de los sensores hardware y el uso de CPU y memoria RAM.

El resto de indicadores se actualizan con menor frecuencia.

↑ Panel lateral del programa Everest.

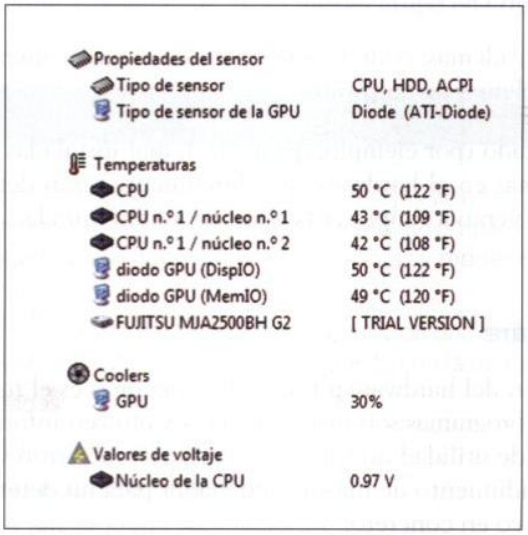
↑ Everest. Paquetes disponibles de la versión trial para 30 días.

saber más

Otros programas para monitorizar el hardware:

- HWMonitor.
- Hardware Sensors Monitor.
- Hardware Monitor (licencia gratuita).
- Notebook Hardware Monitor (para notebook).
- Hardware Monitor (para Mac).

Una característica común en este tipo de programas es la ventana de entrada, que generalmente muestra un resumen y da acceso a las distintas secciones para ver la información con más detalle.



↑ Valores mostrados por el sensor para el equipo monitorizado.

saber más

Algunos sistemas operativos contienen herramientas de monitorización del hardware con sensores de temperatura y usos de CPU, red y discos duros.

Las opciones más utilizadas son las referentes a la **placa base** (procesador, placa base, memoria, BIOS, etc.) y el **almacenamiento** (discos lógicos, discos físicos, discos ópticos, ATA, SMART, etc.).

La utilización de un método software para la monitorización presenta una ventaja, pues se puede ejecutar en un segundo plano y acudir al programa cuando sea necesario, sin requerir una especial atención, y obtener datos en **tiempo real** sobre el estado del sistema.

Además, suelen contar con una **herramienta de informes** que genera un documento con toda la información recabada por el programa, muy útil a la hora de realizar una auditoría sobre seguridad del hardware.

1.5. Cableado

En los apartados referentes a SAI y regletas protectoras hemos podido comprobar la importancia de la correcta conexión de nuestros dispositivos a la red eléctrica, ya sea directamente o a través de estos sistemas de alimentación.

No cabe duda de que es vital para la seguridad de los equipos y de las personas que las conexiones se realicen bien y con materiales en perfecto estado y de buena calidad, para de esta forma poder garantizar la duración de los mismos.

Se debe evitar el sobrecalentamiento de los componentes así como conectar demasiados dispositivos a una misma toma para evitar accidentes, cortocircuitos, etcétera.

Tendremos en cuenta el tipo de enchufe al que conectaremos nuestro equipo, si es de baja potencia deberemos prestar especial atención, ya que puede que sus componentes no resistan la conexión de varios equipos.

No se recomienda utilizar cables diseñados para otro uso, ni realizar empalmes de cables que no cumplan con las normas de seguridad.

↑ Cable de alimentación genérico.

ACTIVIDADES

15. Instala el programa del ejemplo del epígrafe 1.4 (Everest Home Edition) o un equivalente y monitoriza el hardware de tu ordenador. Compara con tus compañeros los resultados obtenidos y extraed conclusiones sobre qué hardware ofrece un mayor rendimiento.

saber más

Algunos programas para el control del hardware tienen como inconveniente el fácil acceso a la información sin ser administrador del sistema.

saber más

Uno de los *gadgets* de Windows Sidebar muestra en cada instante el uso de la CPU y de la memoria RAM.

caso **práctico** inicial

El primer paso para garantizar una instalación limpia y bien mantenida es la conexión correcta de los dispositivos a la red eléctrica y utilizar, como mínimo, las medidas más elementales de monitorización y seguridad del hardware, en función de las necesidades reales de la empresa u hogar.

1.6. Fijación de componentes físicos

saber más

Los ventiladores y el disco duro son las principales fuentes de ruido del ordenador.

Hay muchos motivos por los que resulta conveniente fijar de forma correcta los componentes físicos de un ordenador.

En primer lugar, el propio equipo produce **vibraciones** que pueden afectar al hardware. El **disco duro,** un lector de **CD/DVD** o el **ventilador** de la fuente de alimentación son componentes que contienen partes móviles que, al funcionar, traspasan parte de esa energía al resto de piezas.

Además, existen **conexiones** de gran tamaño, como puede ser el conector VGA del monitor, que realizan presión sobre la tarjeta gráfica, llegando con el tiempo a deteriorarla y descolocarla de su posición inicial.

Es del todo deseable evitar estas situaciones ya que provocan un **mal funcionamiento** del equipo y que el ambiente de trabajo no sea el idóneo debido al **ruido** que producen.

Aparte de los inconvenientes propios que presentan los ordenadores por el diseño de sus componentes, se debe contemplar la posibilidad de **factores externos** que requieran una atención especial.

↑ *Rack* antisísmico.

Tal es el caso de los **terremotos.** En zonas de mayor actividad sísmica conviene **anclar** los equipos de forma segura, instalándolos en **armarios especiales** o simplemente encajándolos en zócalos atornillados sobre soportes de goma que absorban vibraciones.

Se debe tener en cuenta a la hora de fijar un equipo que cualquier lugar no es válido, y que hay que dejar libre la zona de **ventilación.** Los armarios y escritorios empotrados que no están diseñados específicamente para contener ordenadores suelen obviar este detalle, algo que puede ser muy perjudicial para nuestro PC.

↑ Cable y llaves Kensington.

Si nuestro ordenador va a instalarse de cara al público o en un lugar con gran afluencia de personas, debemos saber que el equipo es susceptible de ser **robado,** por lo que también deben tomarse precauciones al respecto.

Existe un tipo de cerradura, presente en prácticamente cualquier equipo portátil y ordenadores de alto coste, llamada cerradura Kensington o **conector de seguridad Kensington.** Este tipo de cerraduras se anclan al ordenador y se conectan mediante un cable de acero a un lugar fijo, como por ejemplo la pata de una mesa. A pesar de no ser un elemento definitivo en la protección antirrobo, sí tiene al menos efectos disuasorios.

1.7. Otros componentes

↑ Filtros contra el polvo de tamaños estándar, que se instalan en las rejillas de la carcasa de los ordenadores.

Cuando hablamos de componentes refiriéndonos a la seguridad hardware, estamos hablando de muchos de los elementos nombrados hasta ahora.

Las llaves Kensington, los tornillos y los soportes especiales son solo el comienzo de una larga lista de productos diseñados para proteger la parte más física de nuestros equipos.

- **Carcasas.** Las carcasas son el recubrimiento de las interioridades de todo sistema. Los diseños varían según los gustos, desde las más austeras hasta las de último diseño en ***modding,*** pero todas cumplen su cometido de proteger lo que guardan en su interior.

- **Maletín de transporte.** Son maletines o mochilas con acorchamientos que absorben impactos y garantizan la seguridad del hardware durante el transporte. Son utilizados principalmente con ordenadores portátiles, aunque existen versiones para torres y semitorres.
- **Refrigeración líquida.** Aunque suele estar ligada al *modding* y a los equipos de alto rendimiento, la refrigeración líquida supone un elemento más de seguridad puesto que garantiza una baja temperatura en nuestro ordenador y evita posibles problemas derivados de un sobrecalentamiento.
- **Protector de pantalla.** Probablemente el gran olvidado. Es un sistema software que evita la congelación de imágenes –y posterior deterioro– de los monitores.
- **Teclado resistente al agua.** No siempre las condiciones de trabajo son las deseadas. Por este motivo existen teclados resistentes al agua y a las salpicaduras, que se pueden lavar.

Estos son solo algunos ejemplos de la amplia gama de componentes al alcance de los profesionales y usuarios finales.

saber más

Modding

Se denomina así la modificación estética o de comportamiento de un ordenador o un periférico, por ejemplo, decorándolo con diseños gráficos personalizados.

saber más

El teclado es uno de los periféricos más vulnerables a derrames de líquido y entrada de polvo, grasa y partículas. Los teclados de silicona son una solución económica y lavable.

ACTIVIDADES

16. El polímetro es:

a) Un instrumento software para medir el hardware.

b) Un instrumento hardware para controlar el software.

c) Un instrumento hardware para medir el hardware.

d) Un instrumento software para controlar el software.

17. Nombra al menos un problema hardware que no puede ser detectado mediante software.

18. Busca y recopila información sobre empresas que fabriquen software para la monitorización del hardware. Encuentra al menos una que ofrezca software gratuito o de evaluación gratuita por un periodo de tiempo limitado.

19. Utiliza la empresa que hayas seleccionado de la actividad 18 y que ofrezca software gratuito para descargarlo. Anota los puntos que cubre la información. Compáralo con el software de tus compañeros y compañeras de clase. ¿Qué empresa ofrece un software más completo?

20. Si alguien compra un ordenador portátil en Europa y viaja al Caribe, ¿podrá conectarlo a la corriente eléctrica directamente? En caso negativo, ¿qué necesitará?

21. Analiza el lugar donde está tu ordenador de casa. ¿Crees que es el mejor sitio? ¿Por qué?

22. Busca algún componente de seguridad que creas interesante y coméntalo con tus compañeros.

23. ¿Ves útil usar un salvapantallas? ¿Tienes activado el de casa?

2. Seguridad pasiva

Como es sabido, por más medidas que se tomen para asegurar un bien, no todas las vulnerabilidades pueden cubrirse por completo, lo que deja abierta la posibilidad de un ataque al sistema hardware y su consiguiente deterioro o pérdida. Cuando esto ocurre entrarían en acción las medidas de seguridad pasiva, que reducirían o anularían el impacto del ataque.

A continuación estudiaremos las medidas pasivas de protección del hardware que se emplean con mayor frecuencia.

2.1. Mecanismos de tolerancia a fallos

saber más

La redundancia lleva años siendo usada por los militares para alcanzar un alto nivel de confianza.

Definimos la tolerancia a fallos como la capacidad de los sistemas de seguir funcionando a pesar de la avería de alguno de sus componentes.

Se suele dotar con este tipo de mecanismo a equipos vitales de los que se espera un funcionamiento continuo y sin fallos. No es habitual encontrarlos en ordenadores de usuarios finales debido al alto coste económico que conllevan, ya que estos sistemas necesitan componentes duplicados. A esta duplicidad de componentes la llamaremos **redundancia.**

saber más

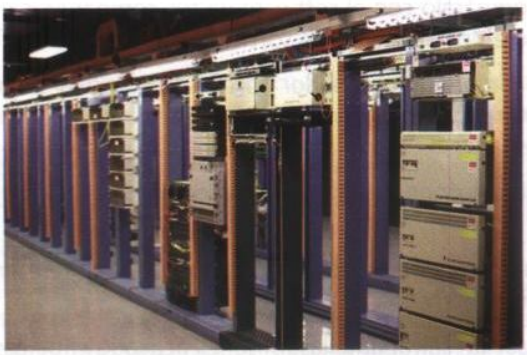
La redundancia de tarjetas de red en los servidores asegura el funcionamiento de la red en caso de fallo o avería de una de ellas. Además distribuye la carga en momentos de máximas peticiones.

La redundancia puede ser de dos tipos, **estática** y **dinámica.**

- **Redundancia estática.** Los componentes duplicados siempre están activos y funcionando.
- **Redundancia dinámica.** Es el propio componente redundante, mediante otros sistemas, el que detecta el fallo y comienza a funcionar.

Actualmente, todos los servidores cuentan con multitud de CPU y módulos de memoria RAM que trabajan en conjunto para satisfacer las necesidades de demanda del servidor. Todas las piezas de este tipo de equipos pueden ser cambiadas «en caliente», es decir, no es necesario apagar el equipo para realizar las tareas de mantenimiento y sustitución de piezas.

Además de lo comentado hasta ahora, es habitual encontrar sistemas con discos duros, fuentes de alimentación y tarjetas de red redundantes.



↑ *Racks* dentro de un *data center* en San Antonio, Texas.

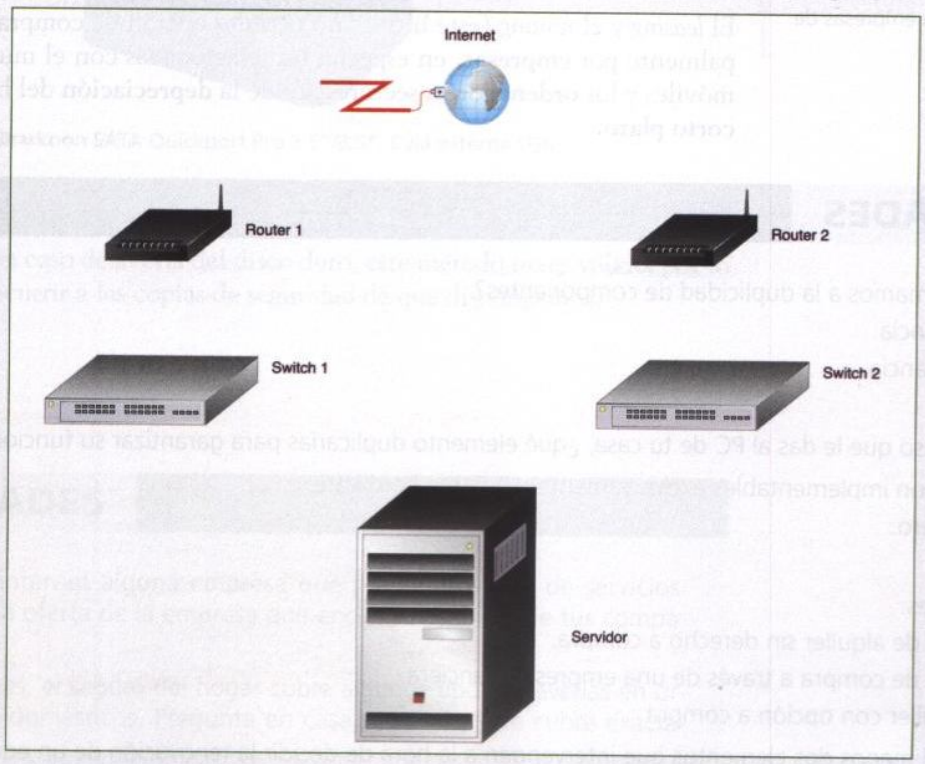
- **Discos duros.** Se usan **RAID** ***(Redundant Array of Independient Disk)*** que en español significa **grupo redundante de discos independientes.** Son un conjunto de discos físicamente independientes, pero que trabajan como un solo disco a un nivel lógico. Los datos almacenados se copian en los distintos discos, proporcionando una redundancia que protege frente a fallos en alguno de ellos. Se pueden encontrar implementaciones de RAID tanto de software como de hardware. Se verá con mayor profundidad en la unidad 8.
- **Fuentes de alimentación.** Es normal encontrar un mínimo de dos fuentes redundantes en los servidores. Se conectan a sistemas eléctricos que garantizan el suministro eléctrico en caso de fallo en alguna de las fuentes.
- **Tarjetas de red.** También usamos un mínimo de dos. Trabajan en conjunto para satisfacer picos de peticiones en los servidores y así garantizar el correcto funcionamiento. En caso de que alguna falle, las restantes siguen realizando su función mientras se soluciona el problema.

↑ Fuente de alimentación redundante TC-iSTAR.

En caso de que sea necesario, se pueden construir sistemas de red redundantes, con *switches* conectados entre sí y *routers* interconectados para garantizar que si uno cae la comunicación no se pierda.

ACTIVIDADES

24. ¿Cómo conectarías a internet un servidor con dos tarjetas de red, si dispones de dos *routers* y dos *switches*, para garantizar que aunque falle un componente el servidor seguirá conectado a la red? Conecta los elementos.



2.2. Renovación de equipos

Pasado un tiempo desde la adquisición de nuestros equipos, llega la decisión sobre la **renovación.**

No se trata de decidir si cambiar un equipo que no funciona por otro que sí, ya que ese caso de renovación o sustitución, tiene fácil solución. Si necesitamos el equipo, debemos cambiarlo.

Se trata más bien de valorar la **obsolescencia** de nuestro sistema, que sigue funcionando, aunque se prevé que en poco tiempo deje de hacerlo o al menos deje de hacerlo en las condiciones adecuadas.

Se deben tener en cuenta diversos factores, entre ellos si el equipo a sustituir está convenientemente **amortizado,** el **coste** del nuevo equipo, los costes de **instalación** y adecuación del resto de componentes al nuevo hardware y los gastos, en caso necesario, para la **actualización** del software para el nuevo equipo.

saber más

El *leasing* suele incluir una cláusula que obliga al cliente a permitir inspecciones del bien por parte del propietario.

Además, en ambientes tecnológicos, se puede tener la certeza de que en poco tiempo surgirá un nuevo hardware, y tal vez este cubra mejor nuestras necesidades.

Una buena forma de solucionar el problema de la renovación de equipos, así como el de la financiación de la adquisición de los mismos, es el ***leasing.***

El *leasing* es un tipo de alquiler en el que se paga a un arrendador una cantidad fija durante un tiempo determinado. Pasado ese tiempo tenemos una opción de compra sobre el bien que tendrá un precio al que se le descuenta lo ya pagado mensualmente por el alquiler.

caso **práctico** inicial

El *leasing* informático puede ser una opción interesante de renovación de equipos para empresas de todo tipo.

Usando este sistema de **arrendamiento financiero,** la renovación y mantenimiento de los sistemas queda de parte del propietario –el arrendador–, que dispone de los medios económicos necesarios para llevar a cabo la renovación necesaria.

El *leasing* y el *renting* (este último no permite opción de compra) se usan principalmente por **empresas,** en especial las relacionadas con el mundo de los automóviles y los **ordenadores,** sectores donde la **depreciación** del bien tiene lugar a **corto plazo.**

ACTIVIDADES

25. ¿Cómo llamamos a la duplicidad de componentes?
- a) Abundancia.
- b) Redundancia.
- c) *Leasing.*

26. Según el uso que le das al PC de tu casa, ¿qué elemento duplicarías para garantizar su funcionamiento?

27. Los RAID son implementables exclusivamente mediante hardware:
- a) Verdadero.
- b) Falso.

28. El *leasing* es:
- a) Un tipo de alquiler sin derecho a compra.
- b) Un tipo de compra a través de una empresa financiera.
- c) Un alquiler con opción a compra.

29. Nombra al menos dos elementos que intervengan a la hora de decidir la renovación de un equipo.

2.3. Equipos de sustitución

Una empresa dedicada al mundo de la informática, o un ejecutivo cuyo trabajo depende del ordenador, no pueden permitirse parar su actividad por una avería.

La posibilidad de contar con un equipo de sustitución, es decir, un ordenador para utilizar en caso de que falle el nuestro, suele estar cubierta por alguna empresa externa a la que contratamos dicho servicio por una cuota mensual o anual; probablemente, la propia empresa aseguradora o la empresa que gestione el mantenimiento del sistema.

Sería muy costoso, tanto a nivel económico como de desaprovechamiento del material, tener un ordenador guardado esperando una avería, por eso se suele recurrir a este tipo de servicios.

En caso de avería, la empresa proporciona un equipo mientras este es reparado, además de algún tipo de carcasa o sistema para el montaje del disco duro de nuestro ordenador, de forma que se pueda seguir trabajando con nuestros datos sin recurrir a la actualización posterior una vez sea reparado el ordenador.

↑ Sharkoon SATA Quickport Pro 2.5"/3.5". Caja externa USB.

Sobra decir que en caso de avería del disco duro, este método no es válido, por lo que deberemos recurrir a las copias de seguridad de que dispongamos.

caso **práctico** inicial

Contar con un equipo de sustitución inmediata para caso de averías es una buena medida que permite traspasar el disco duro al nuevo equipo sin pérdidas de información ni de tiempo. El sistema probablemente más adecuado de sustitución sea el que proporcionan empresas especializadas o aseguradoras.

recuerda

Un equipo de sustitución se hace necesario cuando el trabajo no pueda aplazarse o se necesite un equipo permanentemente disponible.

ACTIVIDADES

30. Busca en internet alguna empresa que preste este tipo de servicios. Compara la oferta de la empresa que encuentres con la de tus compañeros.

31. En ocasiones, el seguro del hogar cubre algunos tipos de averías en ordenadores domésticos. Pregunta en casa si es así y qué cubre exactamente.

3. *Racks* y armarios ignífugos

Todo lo aprendido hasta el momento está enfocado a la seguridad del hardware, a cómo proteger nuestro sistema en las diversas situaciones que pueden darse y a evitar la pérdida de datos y tiempo de trabajo.

saber más

19 pulgadas equivalen a 48,26 centímetros.

Teniendo en cuenta estas bases, surgen algunos aspectos que tratar. Ese es el caso de los ***racks***, diseñados para almacenar todo tipo de material informático, electrónico y de telecomunicaciones. Tienen unas medidas estándar de **19 pulgadas** de ancho.

Los *racks* suponen una medida de seguridad más, puesto que sirven para organizar de forma adecuada los dispositivos, lo que disminuye el riesgo de cortocircuitos a causa de un cableado mal instalado, y favorecen la colocación en zonas seguras y bien protegidas por sistemas antiincendios (ya lo vimos en la unidad 2) y con protecciones antisísmicas.

Sirven, además, para proporcionar la adecuada refrigeración de los sistemas y son aislantes acústicos.

↑ *Rack* HP 5642.

↑ SAI de la marca HP para racks.

Asimismo, pueden colocarse en armarios ignífugos, lo que brinda aún más seguridad.

Los **armarios ignífugos** están equipados con sistemas que los protegen del fuego. Además, están fabricados con materiales aislantes. Esta definición no varía para los armarios ignífugos con aplicación en el mundo de la informática, y algunos armarios *rack* ya cuentan con estos sistemas.

↑ Caja fuerte ignífuga de la marca FireKing para conservar copias de seguridad y documentos digitales, capaz de soportar hasta una hora temperaturas de 1.700 °C.

PRÁCTICA PROFESIONAL

Antes de encargar un trabajo, la empresa requiere información

Te han encomendado un trabajo para una clínica médica de tu localidad. Disponen de varias salas de consulta con un ordenador cada una de ellas, además de una sala de gestión que cuenta con varios servidores y periféricos. Acaban de adquirir la mayor parte del hardware debido al envejecimiento prematuro del anterior por una mala gestión de su seguridad.

El gerente de la clínica tiene especial interés en la conservación de los equipos por dos motivos: el primero, reducir los costes de renovación, y el segundo, porque de ello depende en buena parte la custodia de la información y, por tanto, la imagen de la clínica.

En vuestro primer contacto, el gerente no tiene muy claro qué desea hacer, por eso ha solicitado tu presencia a fin de obtener asesoramiento y poder tomar decisiones. Primero le has dado una serie de nociones generales para mantener el hardware de que dispone la clínica y a continuación, basándose en los conceptos que te ha oído mencionar, te hace una serie de preguntas que deberás responderle adecuadamente. No vale un SÍ o un NO por respuesta, sino una corta, clara y concisa explicación a cada una de esas dudas.

Resuelve

Estas son las preguntas que te hace el gerente de la clínica:

1. ¿Es muy complicado instalar un SAI?
2. Para que el SAI se mantenga en buen estado, ¿qué precauciones hay que tomar?
3. ¿Cuáles son las principales diferencias entre un SAI y una regleta protectora?
4. ¿Cómo funciona un grupo electrógeno?
5. ¿Cuáles son las ventajas de la monitorización del hardware mediante software?
6. ¿Tiene alguna desventaja?
7. ¿Para qué se usan los sistemas antivibraciones?
8. ¿Qué es un conector Kensington?
9. ¿Para qué me recomendarías la duplicidad en las tarjetas de red de los servidores?
10. Me has hablado de *leasing* y de *renting* y había pensado que cualquiera de las dos podría ser una buena solución para esta empresa, pero no tengo muy claro si para los ordenadores debería usar *leasing* o *renting*, ya que no tengo clara la diferencia entre uno y otro. ¿Podrías darme una pequeña explicación?
11. ¿Para qué sirve un *rack*?
12. Con vistas a su adaptación a la sala de servidores, ¿hay *racks* de diferentes anchuras o tienen una medida de ancho estándar?
13. En la sala de gestión trabajan permanentemente dos personas. ¿Puede un *rack* ayudar a mantener un buen ambiente de trabajo para las personas que trabajan en su proximidad?

Una vez que has aclarado las dudas que tenía, el gerente decide que debe estudiar detenidamente las posibles soluciones y que en el plazo de una semana volverá a llamarte para llevar a cabo las que considere más convenientes y factibles.

MUNDO LABORAL

La temperatura: los ordenadores necesitan frío y producen calor

La temperatura, como hemos estudiado, afecta directamente al mantenimiento del hardware.

Por otra parte, los grandes centros de datos emiten a la atmósfera demasiado calor, lo que se considera una forma de contaminación, mientras que para enfriar el hardware se necesita mucha energía. Poco a poco se van encontrando soluciones ecológicas tanto al enfriamiento del hardware como al calor que este emite.

Una de las soluciones la ha encontrado una empresa finlandesa, **Helsingin Energia,** que aprovechará el calor generado por un centro de datos instalado en un viejo refugio antiaéreo para dotar de calefacción a unas 500 viviendas de gran tamaño de Helsinki.

Otra solución la está desarrollando **Google,** que ha creado una patente denominada ***Water-Based Data Center,*** que consiste básicamente en instalar grandes centros de datos en medio del océano. La solución ecológica que proporcionarían estos centros de datos es doble: por una parte se abastecerían de la energía generada por el movimiento marino (olas y corrientes) y, por otra, utilizarían el agua del mar para enfriar miles de ordenadores.

Y ya que mencionamos a Google, puede visitarse el vídeo de Youtube **http://www.youtube.com/watch?v=zRwPSFpLX8I,** en el que se muestra uno de sus centros de datos, la forma como tienen distribuidos los servidores dentro de sus instalaciones y cuáles son las medidas de seguridad del hardware que utilizan. En el vídeo se explica que un centro ecológico no solo es bueno para el medio ambiente sino también para la economía empresarial, puesto que reduce costes.

El mundo empresarial invierte en el desarrollo de nuevas tecnologías para mejorar la seguridad del hardware y frenar el deterioro del medio ambiente.

Actividades

1. Es invierno y hace frío. Un instituto que aún no tiene puesta la calefacción cuenta con varias aulas normales y dos aulas con 30 ordenadores cada una.

a) ¿Dónde se encontrarán mejor las personas, en las aulas normales o en las aulas de informática?

b) ¿Consideras que el calor generado por los ordenadores en el aula de informática es un sistema aceptable de calefacción?

c) En general, ¿podría utilizarse el calor generado por los ordenadores como energía alternativa para proporcionar calor a un espacio?

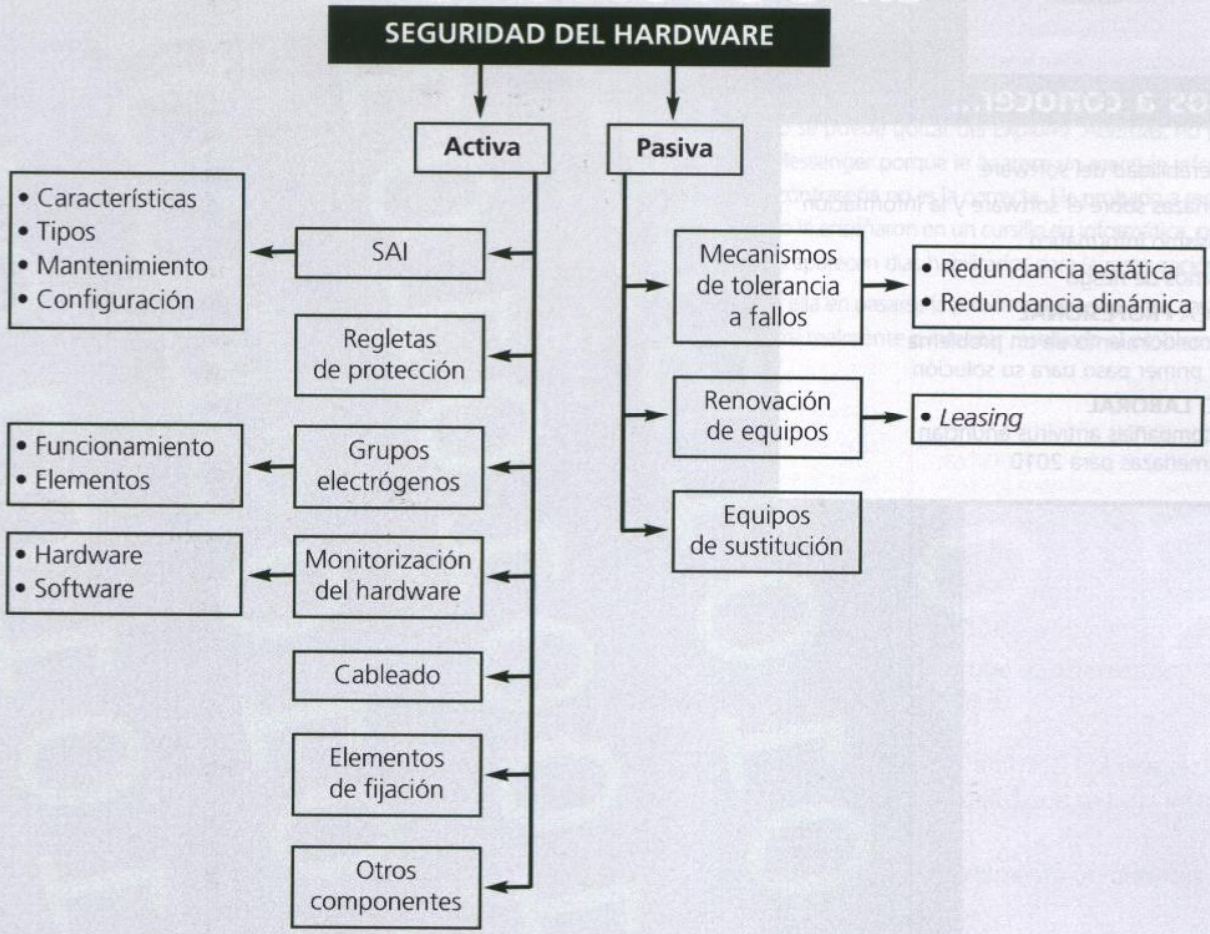
d) ¿Qué empresas conoces que hayan utilizado el calor de centros de datos para generar calefacción a las viviendas?

2. Recientemente saltó a la opinión pública una interesante noticia. Google planea trasladar sus centros de datos a Islandia.

a) ¿Por qué crees que esta noticia es verosímil?

b) ¿Qué particularidad tiene Islandia para atraer la atención de Google?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **La seguridad del hardware es:**
   a) Siempre activa.
   b) Siempre pasiva.
   c) Activa y pasiva.
   d) Si se trata de hardware no puede ser ni activa ni pasiva.

2. **La diferencia principal de una regleta de protección, comparada con un SAI, es:**
   a) La regleta no soluciona los picos de tensión.
   b) La regleta no soluciona los ruidos eléctricos.
   c) La regleta no soluciona los cortes de corriente.

3. **¿Qué elemento, método o componente para la seguridad del hardware no pertenece a la seguridad activa?**
   a) Un programa de monitorización.
   b) La redundancia dinámica.
   c) El polímetro.
   d) La refrigeración líquida.

4. **De las siguientes opciones, una o varias son ciertas. Márcalas:**
   a) La desprotección del hardware puede perjudicar a las personas.
   b) Puede perjudicar a los datos.
   c) Puede perjudicar a la economía de la empresa.

Soluciones: 1c, 2c, 3b, 4a, 4b, 4c

5 Amenazas al software

vamos a conocer...

1. Vulnerabilidad del software
2. Amenazas sobre el software y la información
3. Intrusismo informático
4. Entornos de riesgo

PRÁCTICA **PROFESIONAL**
El reconocimiento de un problema es el primer paso para su solución

MUNDO **LABORAL**
Las compañías antivirus anuncian las amenazas para 2010

y al finalizar esta unidad...

- Sabrás a qué factores se debe la vulnerabilidad del software.
- Podrás diferenciar las distintas amenazas que se distribuyen en código malware.
- Conocerás en qué se basa la ingeniería social.
- Distinguirás por sus métodos y peligrosidad a los distintos tipos de intrusos informáticos.
- Conocerás los tipos de herramientas que utilizan los *hackers*.
- Podrás ampliar tu conocimiento sobre los entornos que constituyen un riesgo para el software.

CASO **PRÁCTICO** INICIAL

situación de partida

Julia recibe una llamada telefónica de su amiga Luisa para ver si puede echarle una mano con los problemas que tiene con su ordenador de sobremesa. El portátil con Linux le va bien, pero lo utiliza poco, solamente hace en él algunos trabajos aislados y navega por internet. No tiene ningún antivirus instalado porque le han dicho que en ese sistema operativo no es necesario.

Necesita urgentemente arreglar el de sobremesa, que es donde tiene juegos bajados, ve películas, se conecta a su red social y se comunica con el trabajo. El problema que tiene en el de sobremesa es que va demasiado lento desde que la semana pasada instaló un antivirus que descargó de internet. Ha aparecido una nueva barra de herramientas que no se puede quitar del Explorer. Además, no puede conectarse al Messenger porque le aparece un mensaje informándole de que la contraseña no es la correcta. Ha probado a restaurar el sistema, como le enseñaron en un cursillo de informática, pero en el calendario no aparecen días habilitados para la restauración.

Julia queda con ella en pasarse la próxima semana por su casa para ver lo que ocurre realmente e intentar resolverle el problema.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

Julia no podrá resolver nada hasta que no vaya a casa de su amiga con su «botiquín de primeros auxilios», como llama a sus herramientas y discos de diagnóstico y reparación, pero mientras toma el café de media tarde, se queda pensando en lo que le ha contado Luisa, mezclando recuerdos de noches de estudio juntas, de aventuras y ocurrencias de su amiga. ¡Qué buena chica es y qué desastre para los ordenadores!, piensa Julia.

1. Luisa afirma que con Linux no corre riesgo de que entren virus en su portátil.
   - ¿Los equipos bajo Linux son invulnerables al software malicioso?
2. Es cierto que Linux, junto con Mac, están considerados los sistemas más seguros. Son potentes y fiables pero últimamente se empieza a hablar de ataques a ordenadores con estos sistemas.
   - ¿A qué se debe la irrupción de malware en dos sistemas considerados siempre invulnerables a código malicioso?
3. «El problema ha comenzado después de descargar un antivirus por internet», le ha comentado Luisa.
   - ¿Es posible que junto al antivirus hubiese algún virus, gusano o troyano oculto que se haya instalado en el equipo?
   - ¿Se habrá descargado realmente un antivirus o un falso antivirus?
4. Luisa es de esas amigas que te reenvían todas las cadenas graciosas, cariñosas o alarmantes que recibe por e-mail.
   - ¿Es una potencial colaboradora con los coleccionistas de direcciones e-mail para enviar *spam?*
5. El equipo se bloquea, va lento, tiene una nueva barra de herramientas en Explorer, no permite la restauración y además no puede usar su Messenger.
   - ¿Puede haber sido infectado con un software malicioso?
   - ¿Pueden haberle robado la contraseña del Messenger?
   - ¿Es posible que haya sido víctima de una intrusión informática?
6. Usa el ordenador, que ahora está averiado, para comunicarse con el trabajo.
   - ¿Las actividades de Luisa podrían repercutir negativamente en la seguridad informática de la empresa para la que trabaja?

1. Vulnerabilidad del software

saber más

«Cada programa tiene al menos dos propósitos: uno, para el que fue escrito; otro, para el que no lo fue».

Epigrams in Programming
Alan Jay Perlis
Yale University

Entendemos por software el conjunto de aplicaciones o programas que hacen posible llevar a cabo las tareas encomendadas al ordenador. Una de estas aplicaciones es el sistema operativo, el paquete de programas más importante, puesto que administra todos los recursos, archivos y tareas. Además está dotado de una serie de utilidades que proveen al ordenador de servicios especiales como la corrección automática de errores del sistema operativo, la instalación de actualizaciones, la aplicación de parches de seguridad o la dotación de controladores para periféricos. Las utilidades adicionales de un sistema operativo dependen de su implementación: Linux, Windows, Mac, etc.

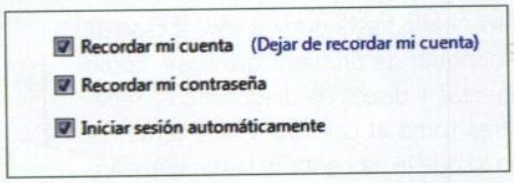
1.1. Origen de la vulnerabilidad del software

recuerda

Ningún programa está libre de manifestar, tarde o temprano, alguna vulnerabilidad. Esto incluye a los programas de seguridad del software.

¿Qué hace que una aplicación o un sistema operativo sean vulnerables? En algunas ocasiones es debido a una mala instalación o configuración del programa por parte de los usuarios o administradores, pero en la mayor parte de los casos se trata de errores de programación que dejan puertas abiertas a la entrada de intrusos.

Errores de instalación o configuración. Pueden deberse a una deficiente documentación del software, a una falta de formación o a negligencias de las personas que lo instalan y configuran. En último término, y con menor frecuencia, podría tratarse de una configuración defectuosa deliberada.



↑ Recordar cuentas y contraseñas puede entrañar riesgos de intrusión.

saber más

El ***bug*** de software, llamado en español «agujero de seguridad», es un error de programación que produce vulnerabilidades en el sistema. Algunos programas, cuando se produce un error, piden al usuario que lo notifique para detectar el código que lo produce y proceder a su rectificación (parche).

Errores de programación. Se les suele llamar *bugs*, del inglés ***bug*** (insecto). Un buen programa puede estar bien diseñado y aun así resultar vulnerable. Por ejemplo, puede ocurrir que una aplicación que funciona correctamente guarde en un registro los nombres de usuario y contraseñas sin codificar, lo que no deja de ser un error de programación que permitiría a un intruso captar esa información y utilizarla en beneficio propio y en detrimento de la seguridad de la organización.

```
<?php
if(!($conexion=mysql_connect("localhost","usuario","contraseña");))
{
echo  "Imposible realizar la conexión.";
exit();
}
if(!(mysql_select_db("Fuente",$conexion);))
{
echo "Error al seleccionar la fuente";
exit();
```

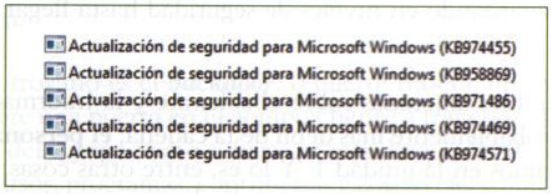
↑ Código PHP.

Retraso en la publicación de parches. Cuando los creadores de sistemas operativos y otro software detectan fallos de seguridad, proceden de inmediato a la creación de parches que ponen a disposición de los usuarios de su software. Los parches son modificaciones de la parte del código que es sensible a fallos de seguridad. Debemos tener en cuenta que cada vez con más frecuencia hay personas cuya finalidad es introducirse en sistemas ajenos para robar o dañar la información que contienen. Si se percatan de la vulnerabilidad de una aplicación antes de que haya sido reparada, habrán conseguido su primer objetivo.

caso **práctico** inicial

Sistemas operativos

Todos los sistemas operativos tienen vulnerabilidades conocidas que se reparan con parches en cuanto se descubren. A mayor número de usuarios que utilizan un sistema operativo, mayor cantidad de malware se programa para él.



↑ Parches de seguridad de Windows Vista.

Descarga de programas desde fuentes poco fiables

Existen páginas de internet que ofrecen programas comerciales, freeware o shareware que en apariencia son los mismos que se encuentran en los sitios oficiales del software correspondiente, pero que tienen código añadido que suele ser de tipo promocional de sitios web y que dan lugar a la instalación de pequeñas aplicaciones adicionales que muchas veces pasan inadvertidas a la vista del usuario. De la misma manera podrían contener fragmentos de código malicioso que pusiese en peligro las propiedades de la información.

caso **práctico** inicial

Falsos antivirus

En fuentes poco fiables es posible encontrar anuncios de antivirus gratuitos que resultan ser virus, troyanos, gusanos o programas espía (spyware), o que siendo el programa esperado, tiene agregado código malicioso que se instala junto con el programa.

1.2. Efectos de ataques a códigos vulnerables

Un ataque producido por una vulnerabilidad en el código de las aplicaciones afectará a una o más propiedades de la información segura:

- Integridad.
- Confidencialidad.
- Disponibilidad.

Pues deja las vías abiertas a posibles atacantes para:

- Obtener de forma oculta información sobre el sistema, equipos que lo componen, datos de usuarios, sistemas operativos, aplicaciones y bases de datos.
- Obtener, copiar e incluso divulgar información restringida.
- Modificar o borrar datos.
- Impedir el acceso a la información por parte de usuarios con permiso de acceso.

↑ Troyano listo para ejecutar la orden que tenga asignada.

2. Amenazas sobre el software y la información

recuerda

El ser humano se considera el eslabón más débil del sistema de información, en especial el personal que gestiona y ha de proteger los datos.

Como hemos ido viendo en las anteriores unidades, el núcleo más protegido de todo un sistema de información son sus datos. Accediendo a las bases de datos de una organización se puede obtener información privilegiada para hundirla. Dañándolos le causará igualmente un daño a veces irreparable.

Por ese motivo ese núcleo está siendo protegido desde el nivel más externo, que es el edificio, y avanzando en niveles de seguridad hasta llegar a la información misma.

saber más

El código malicioso puede afectar a:

- Ordenadores y servidores.
- PDA.
- Videoconsolas.
- Teléfonos móviles.

Existen innumerables amenazas sobre el software y la información, empezando por el eslabón probablemente más débil de la cadena, **el personal de la organización,** como ya vimos en la unidad 1. Y lo es, entre otras cosas, porque se confía en su eficacia y no siempre se tienen garantías de que esta exista, pero además porque es el elemento humano que más cerca se mueve de la información, quien la maneja y tiene la obligación de protegerla. En ocasiones las personas que se encargan de la gestión de la información de una empresa no tienen la suficiente formación. En otros casos, a pesar de tener una preparación profesional suficiente, cometen descuidos o negligencias que ponen en peligro a la organización. Esta fragilidad hace que con mucha frecuencia se utilice al personal como **intermediario** –generalmente de manera inconsciente– para atacar al núcleo del sistema de información. Se irá comprendiendo mejor a medida que se vaya desarrollando esta unidad.

Las amenazas que se ciernen sobre la información, podemos englobarlas en dos tipos: código malicioso e ingeniería social.

2.1. Código malicioso *(malware)*

En lenguaje coloquial solemos abarcar a todo el *malware* bajo el nombre de virus informáticos, si bien existen diferencias entre códigos maliciosos atendiendo al modo en que se instalan y propagan.

- **Virus.** Es un código malicioso incrustado en el código normal de un programa anfitrión. El virus se propaga de un ordenador a otro pero para ello necesita la intervención humana. Puede afectar al funcionamiento del software, del hardware y a las propiedades de la información y causar un impacto desde leve a muy grave sobre su objetivo. Hoy día las infecciones por virus son menos frecuentes que por gusanos o troyanos.

- **Gusano.** En realidad se trata de un subtipo de virus. Las principales diferencias entre el gusano y el virus son que el primero no necesita la intervención humana para propagarse, pues lo hace de forma automática, y que no necesita alojarse en un código anfitrión. Se adueñan de los servicios encargados de la transmisión de datos para tomar su control.

  Uno de los sistemas que usa el gusano para su propagación es enviarse a sí mismo, mediante correo electrónico, a los contactos que encuentra en el ordenador infectado. Muchos gusanos tienen, además, la capacidad de mutar, es decir, modificar automáticamente su propio código.

saber más

Conficker

Es un virus del tipo gusano aparecido a finales de 2008, que ataca al sistema operativo Windows hasta la versión Windows 7 beta. Se propaga a sí mismo utilizando una vulnerabilidad del servicio Windows Server.

Otros nombres para el mismo virus:

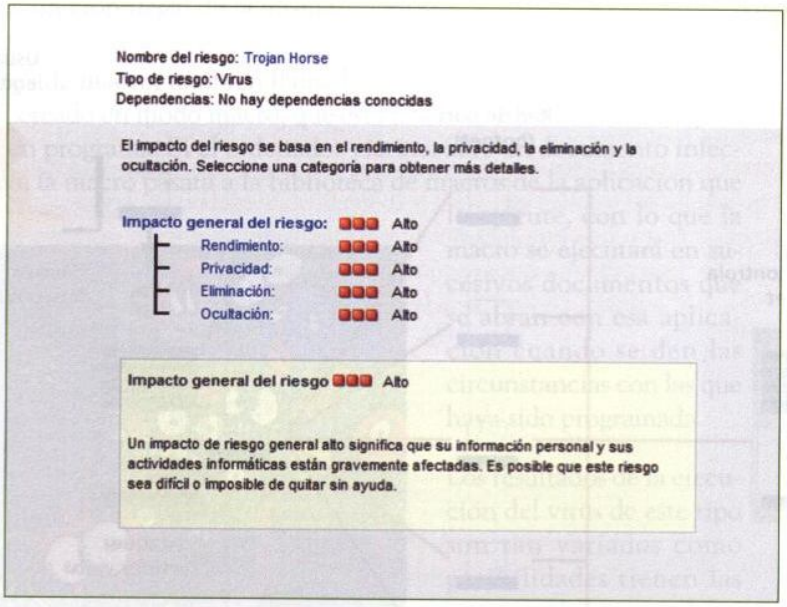
- Downup Devian.
- Downandup.
- Kido.

Uno de los gusanos más conocidos apareció en 2003 con el nombre de **Blaster;** este aprovechaba una vulnerabilidad en el servicio DCOM para enviar un mensaje al usuario del apagado inminente del equipo y realizaba una cuenta atrás, después de la cual el equipo se apagaba sin que fuera posible hacer nada por evitarlo.

- **Troyano.** También denominado caballo de Troya, debido al mito del mismo nombre mencionado en la Odisea y la Eneida en referencia a la Guerra de Troya. El troyano es un programa dañino con apariencia de software útil y absolutamente normal que puede resultar una importante amenaza contra la seguridad informática.

  Un subtipo de troyano es el ***backdoor,*** o puerta trasera, un programa cliente-servidor que abre una puerta en el equipo cliente a través de la cual el servidor toma posesión del equipo como si fuese propio, lo que le permite tener acceso a todos sus recursos, programas, contraseñas y correo electrónico, unas veces en modo vigilancia y otras para modificar la información o utilizarla con fines ilícitos.

  Los equipos pueden infectarse si ejecutan algún programa trampa, generalmente recibido como adjunto de un correo electrónico o descargado de internet. Igualmente puede ser instalado directamente en el equipo por algún delincuente informático que tenga acceso físico al mismo.



↑ Información de la presencia de un troyano tras un análisis antivirus, así como el impacto del riesgo.

- ***Bot* malicioso,** también conocido como **wwwbot** o **robot web.** *Bot* es la simplificación de robot y se trata un programa, realizado con cualquier lenguaje de programación, que pretende emular el comportamiento humano.

saber más

El mito del caballo de Troya

Los griegos ofrecieron a los troyanos el regalo de un inmenso caballo como ofrenda a la diosa Atenea. Estos últimos lo aceptaron y lo introdujeron en su fortaleza, pero resultó ser una trampa que en su interior ocultaba a un importante grupo de soldados griegos.

caso **práctico** inicial

Cuando aparecen barras de herramientas que no se han instalado voluntariamente, el equipo se vuelve extrañamente lento o el calendario de fechas de restauración del sistema no muestra ninguna fecha disponible, con casi total seguridad el equipo ha sido infectado por *malware.*

saber más

Más nombres de código malicioso:

- Bomba lógica.
- *Joke.*
- *Hoax.*
- *Keylogger* («lee» lo que se teclea: roba contraseñas).
- *Clicker.*
- *Ransomware.*
- *Downloader.*
- *Rootkit.*
- *Browser Hijack.*
- *Diales.*
- *Dropper.*
- *PWStealer.*

saber más

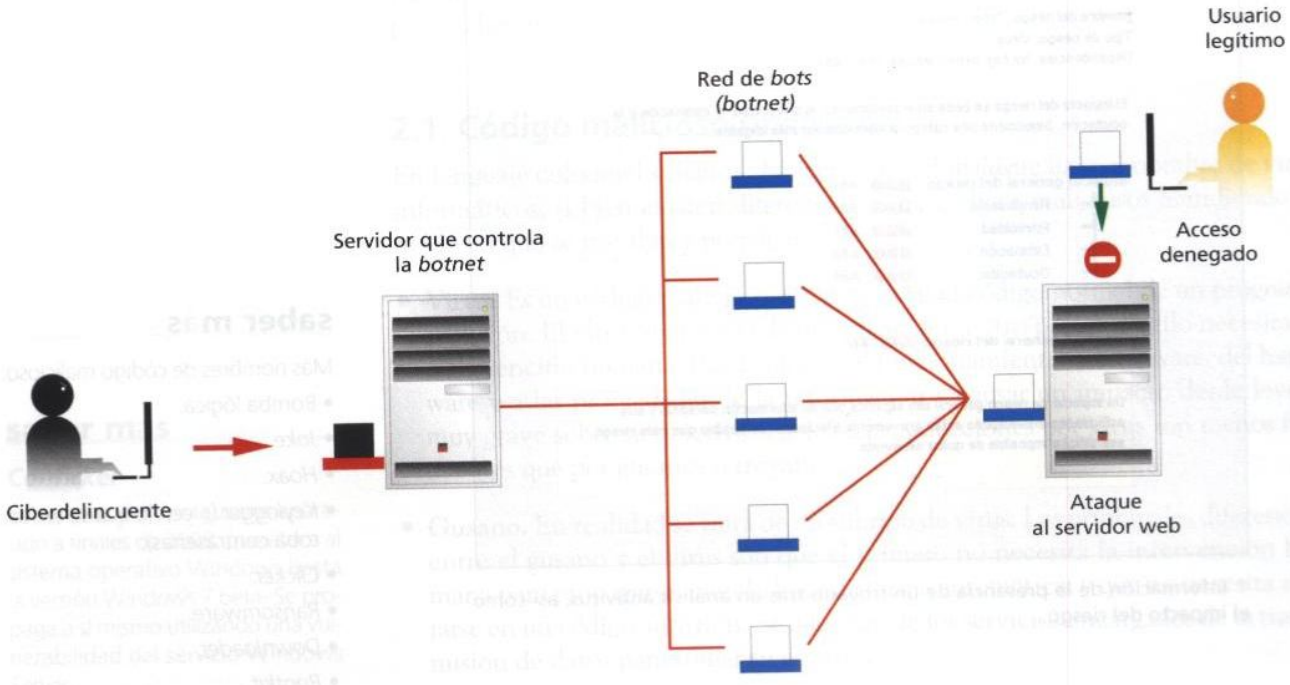
Spam

El spam es correo publicitario no solicitado enviado de forma masiva normalmente a una dirección e-mail, aunque también existe spam postal, telefónico y en forma de comentarios en foros y blogs.

Muchos robots informáticos fueron creados con fines lúdicos, como por ejemplo para mantener un chat con una persona, tomando como base las palabras que ella utiliza y respondiendo o preguntando con frases gramaticalmente correctas, normalmente de un diccionario de frases incorporado. Otros se utilizan como contrincantes o compañeros en juegos de mesa, para escribir poesías o artículos, etc. También se llaman *bots* los robots de rastreo que usan los buscadores, como Yahoo o Google, para detectar el movimiento que se produce en los espacios web y ofrecer las novedades en las búsquedas de usuario.

Los ***bots* maliciosos** son **troyanos** con funcionalidad *backdoor*, cuya particularidad es que se instalan en los equipos vulnerables mediante el sistema de rastreo en internet. Una vez infectado el equipo, el *bot* envía una señal a su creador y el equipo empieza a formar parte de una **botnet,** o red de bots. A los *bots* se les suele llamar zombies, porque cumplen las órdenes que reciben de los delincuentes cibernéticos que los crearon. Las tareas que realiza un *bot*, **de forma automática y transparente al usuario,** pueden ser:

- Enviar **spam** y virus.
- Robar información confidencial o privada.
- Enviar órdenes de **denegación de servicio** a sitios web.
- Hacer clic automáticamente en **anuncios publicitarios** que pagan por cada clic efectuado. El beneficiario será el delincuente informático que maneja la botnet.



↑ Funcionamiento y efectos de una botnet sobre un servidor web

El ciberdelincuente envía una orden al servidor que controla la *botnet*. El servidor envía instrucciones a todos sus *bots* de que ataquen un servidor web. El usuario *bot* no sospecha de que su ordenador es un zombi. Los usuarios legítimos que intentan acceder a la web atacada no pueden hacerlo porque se les deniega el servicio.

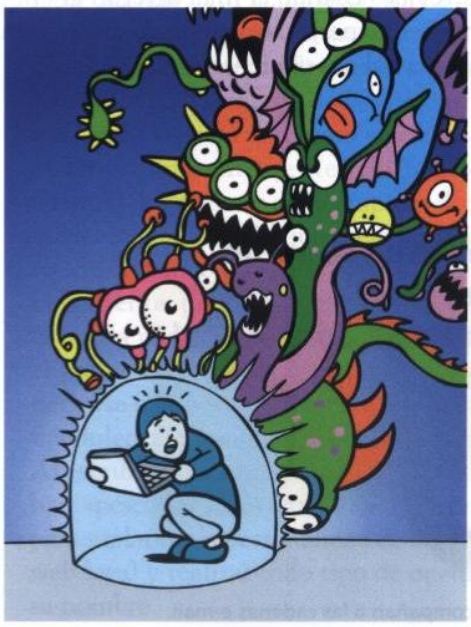
- ***Spyware*** o programa espía. Es un código malicioso que para instalarse en un ordenador necesita la participación de un virus o un troyano, aunque también puede estar oculto en los archivos de instalación de un programa normal. Su cometido es obtener información acerca de los usuarios de un ordenador. El objetivo más leve –y también más común– es aportar esos datos a determinadas empresas que a partir de ese momento y por distintos medios –principalmente correo electrónico o *pop-ups*– enviarán publicidad al usuario sobre los temas que han detectado que le interesan.

  Dado que el programa espía puede **indagar** en toda la información existente en el equipo, como lista de contactos, información recibida y enviada (tan importante como pueden ser: DNI, números de tarjetas de crédito o de cuentas bancarias, domicilio, teléfonos, etc.), software que hay instalado, direcciones IP, servidor de internet que utiliza, páginas web que se visitan, tiempo de permanencia en un sitio web, etc., determinados programas espías pueden ocasionar daños tan importantes como la quiebra de empresas debido a la difusión de información confidencial.

  Como contrapartida, el *spyware* puede servir como sistema de **detección de delitos** cometidos o urdidos a través de internet.

  Los **efectos** que puede causar sobre un ordenador son muy variados, desde la inutilización de algún software instalado o la aparición de ventanas emergentes, hasta la derivación desde una página web legal a un clon ilegal de la misma.

- **Virus de macro,** también llamado macro virus. Es un subtipo de virus, creado en modo macro, que está inscrito en un documento y no en un programa. Si el ordenador víctima abre un documento infectado, la macro pasará a la biblioteca de macros de la aplicación que lo ejecute, con lo que la macro se ejecutará en sucesivos documentos que se abran con esa aplicación cuando se den las circunstancias con las que haya sido programada.



  Los resultados de la ejecución del virus de este tipo son tan variados como posibilidades tienen las macros: abrir un archivo nuevo, auto-enviar el documento por correo electrónico a una dirección predefinida por la macro, realizar cálculos matemáticos (incluso erróneos), etcétera.

caso **práctico** inicial

Robo de contraseñas

Una forma de robar contraseñas consiste en el envío a la víctima de algún software *(keylogger)* que detecte las teclas pulsadas cuando se escribe la contraseña, y remita al emisor el resultado. También puede conseguirse mediante intrusión, en que el hacker observa todo lo que ocurre dentro del ordenador y tiene acceso a todos sus registros.

recuerda

Macro (macroinstrucción)

Se trata de una instrucción creada mediante software –por ejemplo, Visual Basic para aplicaciones– que permite ejecutarse de forma sencilla –como con la pulsación de una o varias teclas– y realizar de forma automática la tarea que se le haya encomendado.

2.2. Ingeniería social

La manipulación inteligente de la natural tendencia humana a confiar

Otra importante amenaza sobre el software y la información es la llamada ingeniería social, que consiste en obtener información a través de las personas que la manejan. No es necesario recurrir a sofisticados programas ni usar estrategias para entrar en el sistema por puertas traseras aprovechando las vulnerabilidades del software. Se trata simplemente de usar los tradicionales timos pero a nivel informático, basándose en la natural **tendencia humana a confiar,** y refuerza la idea, sostenida hasta ahora en este libro, de que **el ser humano es el eslabón más débil de la cadena** cuando nos referimos a la seguridad de los sistemas de información.

El método principal que se utiliza para el **fraude** por internet es el **correo electrónico.** Los argumentos que se utilizan para engañar al usuario son muy variados. Por ejemplo:

- **Cadenas.** Esos correos que con frecuencia contienen ñoños deseos de paz, amor y felicidad, acompañados de imágenes de malísima o estupenda calidad, que al final recomiendan que los reenvíes a todas las personas que quieras que sepan cuánto las quieres. Los hay aún más atrevidos cuando al final agregan la «noticia» de que una persona que no reenvió el mensaje cayó en desgracia y quien lo envió a 200 amigos, encontró la felicidad al día siguiente.

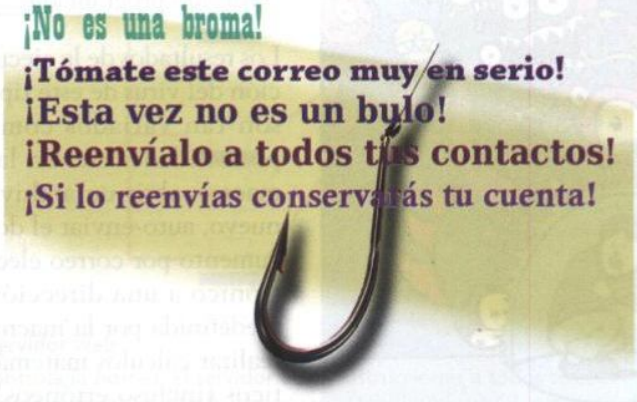
ALERTA AMONESTADORA:
Hotmail está sobrecargado y necesitamos conseguir librados a algunas personas y deseamos descubrir que los utilizadores realmente están utilizando sus cuentas de Hotmail. De modo que si usted está utilizando su cuenta, PASE POR FAVOR ESTE E-MAIL a cada utilizador de Hotmail que usted pueda, y **si usted no pasa esta carta a cualquier persona nosotros suprimiremos su cuenta !!!**
Mr.John Henerd.
Hotmail Admin. Departament.

PÁSALO A TODOS TUS CONTACTOS PORQUE AHORA SI ES DEFINITIVO

↑ Parte del encabezado de un correo-cadena auténtico. Para darle mayor credibilidad y conseguir el reenvío, adjuntan la firma del jefe de un imaginario departamento.

Varias veces a lo largo del correo, queda bien claro, y en mayúsculas, que se ha de reenviar.

El e-mail en cuestión, con sus variantes, circula por la red desde finales de la década de 1990 y suele ir acompañado de centenares de direcciones de correo electrónico.



↑ Muestra de mensajes que acompañan a las cadenas e-mail.

Otros mensajes contienen alarmas de que van a suprimir cuentas de correo electrónico de servidores de correo web muy conocidos –con argumentos desde muy infantiles a muy sofisticados– a quienes no reenvíen el correo que nos da la «noticia».

Lo que todos tienen en común es la recomendación de reenvío a un número determinado o indeterminado de contactos.

caso **práctico** inicial

El reenvío de correos en cadena supone también el reenvío de decenas o cientos de direcciones de correo electrónico que pueden ser utilizadas para el envío de spam.

- **¿Cuál es el origen y la pretensión de estas cadenas?** El origen es de una persona u organización interesada en obtener direcciones de correo electrónico para envío de spam. Un e-mail cadena se multiplica en progresión aritmética o exponencial, con lo que tarde o temprano el emisor volverá a recibirlo con miles o millones de direcciones e-mail. Otro objetivo es colapsar los servidores.

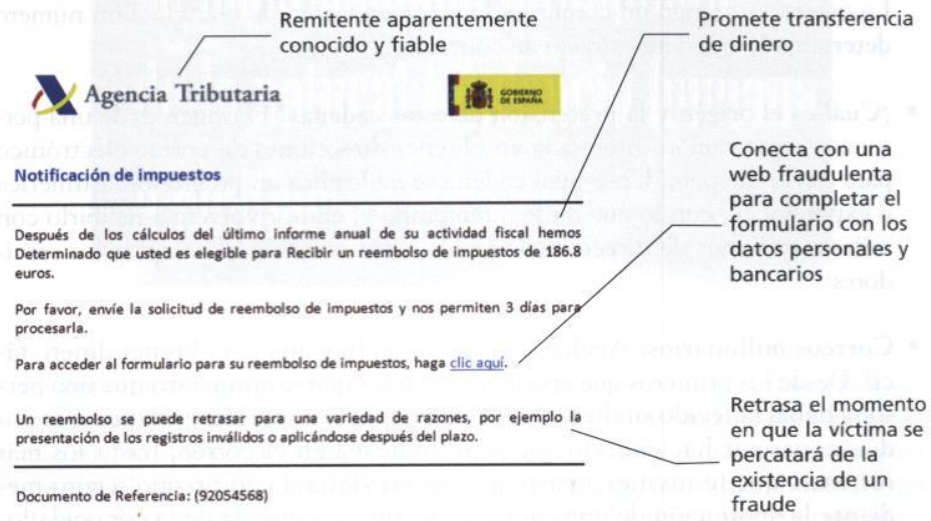
- **Correos millonarios.** Apelan a la ambición humana por obtener dinero fácil. Desde los primeros que aparecieron en los que se anunciaba que una persona había fallecido sin herederos y dejando una importante fortuna que podías conseguir haciendo lo que se te indicaba en el correo, hasta los más recientes que te invitan a participar en una lotería con premio seguro mediante la aportación de una cantidad de dinero, como la de la conocida lotería de Microsoft.

  En estos casos el lucro se obtiene de las aportaciones de las víctimas que pretenden conseguir el premio, la herencia o incluso un trabajo prometido.

- **Phishing.** Palabra similar y de igual lectura que *fishing* (pesca) en inglés. La «p» con la que comienza hace alusión a las contraseñas (*passwords*).

  Es uno de los métodos más frecuentes de «pesca» de contraseñas con fines de suplantación de personalidad. Puede provenir de correo electrónico de desconocidos o de sitios web de poca confianza, pero en ocasiones proviene de contactos conocidos, de bancos o de organismos oficiales, y constituye el llamado *spear phishing*. Por tratarse de supuestos correos de fuentes de confianza, aumentan las posibilidades de hacer caer en la trampa a la víctima. En este caso suele tramarse de la siguiente forma: se envía a la víctima un correo electrónico de procedencia aparentemente legítima, como por ejemplo del director de la empresa donde trabaja, de un amigo o –lo que suele ser más frecuente– de un banco en el que el usuario tenga cuenta corriente, pidiéndole que se conecte a la web bancaria para realizar unas comprobaciones. En el propio correo se le facilita el enlace para conectarse a la web, pero en realidad esa web será fraudulenta, un clon de la auténtica del banco. Al escribir el nombre de usuario y contraseña, ya han «pescado» estos datos y se tiene lo necesario para suplantar la personalidad de la víctima en la web legal y realizar todo tipo de operaciones en su nombre.

Uno de los últimos timos realizados por el sistema *spear phishing* fue remitido aparentemente desde la Agencia Tributaria en septiembre de 2009, con la notificación de una devolución de impuestos que corresponde al receptor del correo. Como remitente del e-mail figuraba impuestos@aeat.es.



ACTIVIDADES

1. Investiga y responde. ¿Qué es en informática un ataque DoS o de denegación de servicio?
2. En ocasiones leemos en la prensa que se ha detectado un agujero de seguridad en un sistema operativo o en una aplicación. ¿Qué es exactamente un agujero de seguridad?
3. ¿Por qué crees que se le ha dado ese nombre al troyano o caballo de Troya?
4. ¿Son sinónimos *bot* y *botnet?* Da una breve explicación a tu respuesta.
5. Analiza la imagen que ilustra el funcionamiento y los efectos de una *botnet* y explica de forma concisa con tus propias palabras cómo se produce todo el proceso de principio a fin.
6. ¿Crees que la policía podría utilizar software spyware para detectar la comisión de delitos en la red?
7. Si has utilizado algún programa de texto o una hoja de cálculo como los de Microsoft Office, es posible que hayas recibido alguna vez un mensaje de aviso de que el documento contiene macros, para decidir si quieres activarlas o no.
   a) ¿Te ha ocurrido?
   b) ¿Por qué te avisa el programa?
8. ¿Has recibido cadenas por correo electrónico con o sin archivos adjuntos? En caso afirmativo:
   a) ¿Una mayoría de esas cadenas te pide que reenvíes el correo?
   b) ¿Lo más normal de tu parte es reenviarlo a tu lista de contactos o a una selección de ellos?
   c) ¿Qué suele pretenderse con el envío de mensajes en cadena?
9. Cada vez es más frecuente que recibamos *phishing* por correo electrónico. Responde y comparte tus respuestas con el resto de la clase.
   a) ¿Has recibido alguno en los últimos meses?
   b) ¿Has picado en la trampa?
   c) ¿Quién era el aparente emisor y qué pretendía que hicieras?

3. Intrusismo informático

Hasta ahora hemos hablado de acceso a la información mediante virus, troyanos y gusanos, y a partir de técnicas de ingeniería social. El intruso informático va más allá de crear software malicioso y ponerlo en circulación por la red, sino que selecciona sistemas informáticos o servidores web para tomar el control de los mismos mediante técnicas de *hacking*, generalmente en modo remoto.

3.1. Clasificación de intrusos informáticos

Dependiendo de los conocimientos que tengan sobre técnicas *hacking* y de la acción que ejerzan sobre las redes, servidores o equipos invadidos, podemos describir distintos tipos de intrusos. El nombre que los agrupa es el de *hackers*, pero hay muchas variedades: *crackers*, *phreaker*, *newbies*, *script kiddies*, *lamers*...

- ***Hacker.*** Es el nombre genérico que se da a los intrusos informáticos, pero en realidad el *hacker* es el único de ellos que tiene un **código ético** para sus intrusiones, el verdadero profesional del *hacking*, que conoce a fondo los lenguajes de programación, las instrucciones y los protocolos de comunicación de redes para introducirse en ellas con privilegios de administrador.

  Los motivos que suelen alentar a un *hacker* a penetrar en un sistema son: aprender, curiosear sobre seguridad informática y demostrar la existencia de agujeros de seguridad o *bugs* en las redes, sistemas operativos y software.

  Su código ético incluye no dañar la información de los equipos en los que consigue entrar ni revelar a terceros la información obtenida; sin embargo, se cuestiona su ética, dado que irrumpen de forma ilícita en la privacidad de otras personas.

- ***Cracker.*** Utiliza las técnicas *hacker* pero para beneficio propio o causando daños a los sistemas que invade. También es un *cracker* el que tiene conocimientos de ingeniería inversa y los usa para ofrecer públicamente seriales, *cracks* o generadores de claves de programas comerciales.

- ***Phreaker.*** Suele tener experiencia en telecomunicaciones y su objeto de estudio son los teléfonos y las redes telefónicas. También se les denomina *hackers* de telefonía.

- ***Newbie.*** Es el nombre que se les da a los que están aprendiendo las técnicas de *hacking*. El término significa «novato».

- ***Script kiddie.*** Es el más denostado socialmente y por los propios *hackers*, ya que no tiene conocimientos de técnicas *hacking* pero utiliza los *scripts* y *exploits*, generados por expertos, para atacar sistemas remotos. Tiene pocas diferencias con el ***lamer*** en cuanto a conocimientos y comportamiento invasor.

saber más

White hack, o «*hacker* de sombrero blanco», es el nombre que se le da al experto en seguridad informática que conoce las herramientas de los *hackers* y las utiliza para proteger los sistemas TIC.

saber más

Crack

Es un pequeño programa que convierte en propio un software comercial que no ha sido adquirido por el usuario.

saber más

Exploit

Es un código escrito en uno de los muchos posibles lenguajes de programación, que aprovecha las vulnerabilidades de cualquier activo físico o lógico de un sistema informático, con el objeto de sacar provecho de ellas en beneficio propio o de terceros.

caso práctico inicial

Los *script kiddies* son autores de la mayor parte de robos de contraseñas e intromisiones dañinas en ordenadores personales y pequeñas redes.

3.2. Proceso de *hacking*

El aprendizaje de técnicas de *hacking* requiere tiempo y conocimientos profundos de las herramientas necesarias para detectar vulnerabilidades, crear *exploits*, conseguir entrar en los sistemas y no dejar rastro de ello. Son conocimientos de alta especialización que no se enseñan como tal en los estudios reglados de informática pero que pueden deducirse de ellos.

A continuación relacionamos el proceso lógico del *hacking* informático:

- **Decidir cuál va a ser la máquina objetivo de la infiltración.**
- **Obtener información acerca del sistema objetivo.** Desde el exterior aún del sistema, mediante unos cuantos comandos y herramientas, no es difícil conocer cómo está constituido el sistema: puertos abiertos, equipos que componen la red, IP privadas de cada ordenador, etc.
- **Detectar las medidas de seguridad y las vulnerabilidades,** una vez que se conocen las generalidades de todo el sistema informático, incluida la red y el ISP (proveedor de internet).
- **Aprovechar las vulnerabilidades** para acceder a los registros de contraseñas.
- **Hacerse con una cuenta de administrador** y, de ese modo, conseguir el control total del sistema. Para ello se pueden valer de la ingeniería social o de técnicas y servicios de red.
- **Conseguir mantener el acceso al sistema invadido.**
- **Trabajo prudente, metódico y minucioso.** Todo el proceso se ha de realizar de forma inadvertida para los administradores del sistema víctima.

saber más

Las macroempresas informáticas están muy interesadas en la formación de *hackers*. Microsoft convocó en 2001 el **concurso de *hacking* ético «Hack21»** al que concurrieron 1.600 hackers.

«Para nosotros, lo principal es asegurar los sistemas de información desde dentro. La labor de los hackers es clave para el desarrollo de unos sistemas de información seguros ante intentos de intrusión». Igor Unanue, director técnico de S21se.

3.3. Herramientas de *hacking*

Los intrusos informáticos, al margen de sus fines, utilizan las mismas herramientas, unas son comandos e instrucciones del sistema operativo y manejo de redes y otras son programas creados *ad hoc* para este propósito o para otros distintos, pero que permiten funcionalidades de *hacking*:

- Comandos del sistema operativo.
- Herramientas para escanear redes y sistemas.
- Herramientas para manipular redes cableadas o inalámbricas.
- Herramientas de auditoría de sistemas para detectar vulnerabilidades.
- Herramientas de rastreo de páginas web.
- Herramientas de ataque.

Al margen de los comandos del sistema operativo, las herramientas utilizadas pueden ser las mismas para un sistema operativo u otro pero también las hay específicas para cada uno de ellos.

Comandos de sistemas operativos

Como hemos explicado anteriormente, dentro del *hacking* se utilizan comandos de sistemas operativos que se usan de manera habitual para trabajar con el sistema, pero que por sí mismos y sus parámetros, y en conjunción con otras herramientas, pueden proporcionarle información valiosa al *hacker*.

Windows	Linux
ping	ipconfig
ipconfig	traceroute
tracert	netstat
nslookup	iwconfig
netstat	iwevent
net	iwgetid
nbtstat	iwspy
regedit	iwlist
arp	snmpget
WidnowsPowerShell	snmpset
dsadd	whois
dsrm	
dsget	
dsquery	
dsmove	

↑ Resultado de la ejecución del comando **net share.** Aporta información sobre un equipo, sus recursos compartidos y la dirección donde se encuentran sus controladores.

ACTIVIDADES

10. Dependiendo del sistema operativo que utilices, averigua la información que se obtiene de algunos de los comandos de la tabla superior, usando diferentes parámetros.

11. Busca información acerca de la acción que ejercen sobre un ordenador los siguientes códigos malignos:

a) Bomba lógica.

b) Hoax.

c) *Keylogger*

d) *Clicker.*

4. Entornos de riesgo

saber más

Web 2.0

Es un concepto reciente, mencionado por primera vez en 2004 por Tim O'Reilly, presidente de la editorial O'Reilly Media, que hace referencia a una nueva era de internet en la que aparecen las comunidades de usuarios, como las redes sociales, los blogs o los wikis.

Hemos visto cómo y quiénes pueden atacar un equipo, acceder a la información, al software, a la red o al sistema operativo, pudiendo solamente curiosear, pero también dañar tanto el software como el hardware.

Se puede atacar un equipo mediante **correo electrónico, mensajería instantánea, canales de chat** y **por dispositivos extraíbles,** aprovechando vulnerabilidades del software, del sistema operativo o de la red, o utilizando a las personas que lo manejan; pero en la era **Web 2.0,** haciendo uso de los mismos métodos, la ciberdelincuencia ha encontrado un filón apetecible sobre el cual ejercer sus acciones.

El ciberdelito avanza a la par que la tecnología, por lo que, en esta era de la virtualización, extiende su acción a las comunidades de usuarios, en donde encuentra un filón apetecible.

Otro de los filones en fase explotación es el *cloud computing*, que explicaremos con detalle en la Unidad 8.

Veremos a continuación la incidencia sobre la seguridad informática en estos nuevos conceptos que nacen con la Web 2.0 y en otros no contemplados a lo largo de esta unidad.

4.1. *Cloud computing*

saber más

Virtualización

En informática, la virtualización significa el trabajo sobre un equipo cliente conectado a un servidor, que es el que dispone del hardware que usa el cliente de forma transparente, es decir, con la sensación de que todo se encuentra en el equipo cliente. Es lo que se conoce como trabajar en un entorno virtual.

El ***cloud computing*** (computación en la nube) se considera el esqueleto de la Web 2.0. Son muchas las empresas que, por seguridad, ya no almacenan sus datos ni alojan sus webs en los servidores que tienen en el edificio donde ejercen su actividad, sino que contratan los servicios que ofrecen los grandes centros de datos del país o de países lejanos. Puede ser, incluso, que la empresa solamente mantenga terminales que trabajan como clientes con un servidor alojado en un *data center* de Alemania o Texas, que es el que tiene el software y se encarga de la gestión y conservación de la información. De hecho existen servidores de juegos, de correo electrónico y de gestión de redes sociales instalados en esos *data center*, a los que el usuario se conecta y ejecuta el software sin tenerlo instalado en su ordenador.

↑ Uno de los sistemas adoptados por millones de empresas en el mundo, para salvaguardar la seguridad de su información, es el *cloud computing* o computación en la nube, lo que hace que los delincuentes informáticos tengan la nube en el punto de mira.

Esos grandes centros de datos cuentan con las mayores medidas de seguridad redundante –tanto física como lógica– que permite la tecnología actual, lo que constituye una garantía para la seguridad de la información de las empresas que contratan sus servicios, aunque existen muchos objetores a esta técnica de computación remota.

Sin embargo, uno de los objetivos de los intrusos informáticos es desafiar la seguridad de estos macrocentros de computación y cálculo, lo que podría poner en peligro la privacidad, la integridad y la disponibilidad de los datos.

Una de las compañías más importantes del mundo que ofrece servicios de *cloud computing* es Amazon, que ya el 9 de diciembre de 2009 sufrió un ataque *hacker* y fue infectada por el troyano Zeus, aunque fue detectado y de inmediato eliminado del sistema. Los delincuentes informáticos buscan retos y apuntan en primer lugar a las empresas de más prestigio.

caso práctico inicial

Una encuesta de Sophos indica que el 63 % de los administradores de sistemas están preocupados por la información personal que publiquen sus empleados en las redes sociales, porque ello podría suponer un riesgo para la empresa.

4.2. Redes sociales

El mundo entero ha experimentado en estos últimos años el *boom* de las redes sociales: profesionales, de contenidos, de entretenimiento... En España hay alrededor de 15 millones de usuarios inscritos en una o más redes sociales. Las más importantes por número de socios son, en este orden, Tuenti, Facebook, Fotolog, Hi5, Metroflog, Sonico, MySpace y Badoo.

Ese inmenso número de personas en las redes sociales las convierte en un medio atractivo en donde distribuir código malicioso.

Uno de los peligros que encierran las redes sociales es el de robo de identidad. El primer caso de suplantación de la identidad en una red social fue denunciado a la Agencia Española de Protección de Datos (AEPD) en enero de 2009, lo que pone en evidencia la desprotección que existe actualmente en lo referente a protección de datos personales.

Ya en diciembre de 2009, Facebook sufrió varios ataques de troyanos y de ingeniería social.

Otro problema importante es el intercambio de software de usuarios que está habilitado en algunas redes sociales. No es difícil imaginar que el código malicioso puede distribuirse de la misma forma.

Los estudios señalan a las redes sociales como objetivo prioritario cada vez más frecuente, utilizando cualquier método para conseguir robar los datos personales de sus usuarios, preferentemente mediante ingeniería social.

Una encuesta realizada por Sophos en agosto de 2009 recogía la preocupación del 63 % de los administradores de sistemas de las empresas por el hecho de que sus empleados puedan compartir demasiada información personal a través de las redes sociales, que ponga en peligro a la propia organización.

4.3. Nombres de dominio

saber más

Secuestro de dominios

Cada vez se dan más noticias de secuestro de dominios. Incluso Google ha sido víctima de esta práctica en varias ocasiones.

Los nombres de dominio son otro de los objetivos del *hacking*. Cada nombre de dominio lleva aparejada una dirección IP única. Atacando a los servidores DND o a ordenadores concretos, un *hacker* malicioso puede deshacer la asociación entre IP y nombre de dominio y desviar el tráfico dirigido a una página a otra diferente, algunas veces de apariencia idéntica a la original. Esa es otra técnica de ingeniería social, denominada ***pharming***.

El propósito del secuestro de dominios puede tener como objeto aplicar técnicas de *phishing* sobre usuarios que creen estar navegando en la web cuyo nombre escribieron en el navegador y sin embargo se encuentran en otra web-clon que está destinada a captar sus datos de usuario y otros datos personales y privados que pudieran serle requeridos durante la navegación por la web fraudulenta. En otros casos, la pretensión de los *hackers* es obtener dinero para devolver el control de la web a su propietario legal.

4.4. Páginas web

Navegar por internet no está exento de peligro de infección por virus, gusanos o troyanos. No es necesario entrar en páginas de dudosa fiabilidad; cualquier página web legítima puede ser atacada por *hackers* e infectada con código malicioso que hace a sus visitantes susceptibles de descargarlo en su máquina de forma inadvertida. Cada día, miles de páginas web son infectadas en el mundo. El tiempo que tarden sus propietarios en darse cuenta de la infección y ponerle remedio es un tiempo de riesgo de infección para los equipos que naveguen por esa web.

4.5. Redes P2P

Algunos códigos maliciosos están disfrazados de nombres de archivos con mucha demanda.

ACTIVIDADES

12. Busca en Google Noticias alguna de las últimas noticias publicadas en español sobre el *cloud computing* o su equivalente «computación en la nube». Trata de encontrar alguna que refiera problemas de ataques o de caída de servidores o cualquier otro problema ocurrido en «la nube» recientemente.

13. En los mismos términos, busca alguna noticia relacionada con *malware* o *hackers* en redes sociales.

14. Cuando se usa el término pirata informático, muchas personas y medios de información hacen alusión a un *hacker*. Averigua si esa información es cierta o si los dos términos tienen diferente significado dentro de internet.

Los estudios señalan a las redes sociales como objetivo prioritario cada vez más frecuente, utilizando cualquier método para conseguir robar los datos personales de sus usuarios, preferentemente mediante ingeniería social.

Una encuesta realizada por Sophos en agosto de 2009 recogía la preocupación del 63 % de los administradores de sistemas de las empresas por el hecho de que sus empleados puedan compartir demasiada información personal a través de las redes sociales, que ponga en peligro a la propia organización.

4.3. Nombres de dominio

Los nombres de dominio son otro de los objetivos del *hacking*. Cada nombre de dominio lleva aparejada una dirección IP única. Atacando a los servidores DND o a ordenadores concretos, un *hacker* malicioso puede deshacer la asociación entre IP y nombre de dominio y desviar el tráfico dirigido a una página a otra diferente, algunas veces de apariencia idéntica a la original. Esa es otra técnica de ingeniería social, denominada ***pharming***.

El propósito del secuestro de dominios puede tener como objeto aplicar técnicas de *phishing* sobre usuarios que creen estar navegando en la web cuyo nombre escribieron en el navegador y sin embargo se encuentran en otra web-clon que está destinada a captar sus datos de usuario y otros datos personales y privados que pudieran serle requeridos durante la navegación por la web fraudulenta. En otros casos, la pretensión de los *hackers* es obtener dinero para devolver el control de la web a su propietario legal.

saber más

Secuestro de dominios

Cada vez se dan más noticias de secuestro de dominios. Incluso Google ha sido víctima de esta práctica en varias ocasiones.

4.4. Páginas web

Navegar por internet no está exento de peligro de infección por virus, gusanos o troyanos. No es necesario entrar en páginas de dudosa fiabilidad; cualquier página web legítima puede ser atacada por *hackers* e infectada con código malicioso que hace a sus visitantes susceptibles de descargarlo en su máquina de forma inadvertida. Cada día, miles de páginas web son infectadas en el mundo. El tiempo que tarden sus propietarios en darse cuenta de la infección y ponerle remedio es un tiempo de riesgo de infección para los equipos que naveguen por esa web.

4.5. Redes P2P

Algunos códigos maliciosos están disfrazados de nombres de archivos con mucha demanda.

ACTIVIDADES

12. Busca en Google Noticias alguna de las últimas noticias publicadas en español sobre el *cloud computing* o su equivalente «computación en la nube». Trata de encontrar alguna que refiera problemas de ataques o de caída de servidores o cualquier otro problema ocurrido en «la nube» recientemente.

13. En los mismos términos, busca alguna noticia relacionada con *malware* o *hackers* en redes sociales.

14. Cuando se usa el término pirata informático, muchas personas y medios de información hacen alusión a un *hacker*. Averigua si esa información es cierta o si los dos términos tienen diferente significado dentro de internet.

PRÁCTICA PROFESIONAL

El reconocimiento de un problema es el primer paso para su solución

En esta unidad no hemos querido entrar en la seguridad del software, sino que nos hemos centrado en la **inseguridad** de sistemas operativos, aplicaciones y datos. Hemos querido analizar las vulnerabilidades más frecuentes y las más probables en los próximos años, dada la evolución constante del mundo de la informática y la virtualidad.

OBJETIVO

- Investigar sobre la vulnerabilidad del software y de la información.

Resuelve

Investiga y opina sobre las siguientes cuestiones:

1. ¿Esta advertencia de Google aparece en algunas páginas web que han sido infectadas con código malicioso.

a) ¿Has encontrado alguna vez esta advertencia en tu navegación?

b) ¿Crees que se basa en una infección real de la web o se trataría de alguna trampa?

2. Otras veces, durante la navegación ocurre que, de manera imprevista, se abre una ventana que avisa de haber detectado *malware* peligroso en tu equipo. La advertencia enlaza con una página de descarga y pago del software necesario para eliminar la infección.

Investiga al respecto y opina sobre la credibilidad del aviso y sobre las consecuencias de descargar o no descargar el software antivirus que propone.

3. El concepto de ingeniería social habla de la tendencia humana a confiar y de quienes se aprovechan de esta característica. Para tu investigación, te dejamos un nuevo concepto, el ***«scareware».***

a) ¿Qué es el *scareware?*

b) ¿Está basado en los principios de la ingeniería social?

4. Un nuevo concepto: ***«Adware».***

a) ¿Qué es *adware?*

b) ¿Es un tipo de *malware?*

5. A continuación verás los nombres de algunos virus curiosos. Busca información y contesta qué tienen de anecdótico cada uno de ellos.

a) Waledac.AX b) Samal.A c) BCKPatcher.C

6. ¿Has leído el libro (o visto la película) *Los hombres que no amaban a las mujeres,* de Stieg Larsson? En cualquier caso, puedes buscar información y responder: el personaje de Lisbeth, ¿es un *hacker,* un *cracker* o un *script-kiddie?*

MUNDO LABORAL

Las compañías antivirus anuncian las amenazas para 2010

Las compañías antivirus han hecho balance de las amenazas que predijeron para 2009 y que se cumplieron prácticamente en su totalidad. A finales de 2009 hacen sus predicciones para 2010.

Kaspersky Labs predijo que para 2009 la lista de amenazas estaría encabezada por un aumento en las epidemias globales, lo cual se ha verificado. El año 2009 estuvo dominado por sofisticados programas maliciosos con funcionalidades de *rootkit* por *conficker, botnets* y ataques a redes sociales.

PandaLabs hace también balance de 2009 y apunta para 2010 las siguientes amenazas:

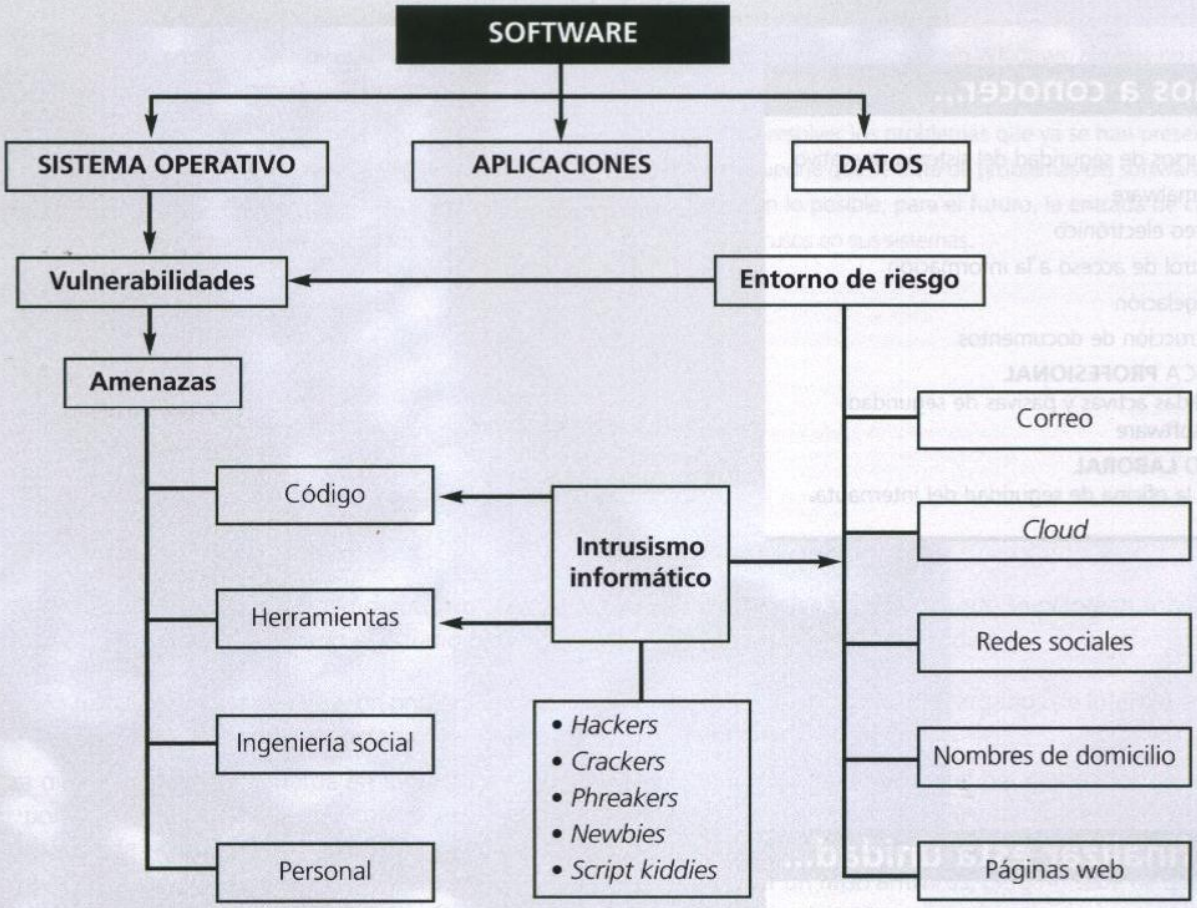
- Un aumento de los ataques sobre el *cloud computing,* informando que la compañía trabaja en cloud-antivirus desde 2007.
- El *malware* seguirá creciendo de forma exponencial. El objetivo principal será obtener un beneficio económico, por lo que se incrementarán los *bots* y los troyanos bancarios.
- Para obtener su propósito, los criminales utilizarán técnicas de ingeniería social y las aplicarán principalmente a buscadores, redes sociales y a las infecciones desde páginas web.
- La alta aceptación de Windows 7 hará a este sistema operativo favorito como objetivo de ataques *malware.*
- El incremento de ventas de Mac hará que muchos ojos dirijan su mirada hacia este sistema operativo como objeto de ataque.
- Incremento de la ciberguerra, o ataques a objetivos cibernéticos con motivaciones políticas.
- Continuarán creciendo el *malware* y las técnicas de *phishing* en redes sociales, como la creación en 2009 de varias páginas iguales que Facebook para atraer a ellas a los usuarios de esta red y robarles sus datos.

Extraído de los informes de Kaspersky Labs y PandaLabs para 2010.

Actividades

1. La noticia habla de programas maliciosos con funcionalidades de *rootkit.* Averigua qué es *rootkit* y a qué sistemas operativos puede afectar.
2. ¿Qué tipo de *malware* es el *conficker?*
3. ¿Desde qué año está creando PandaLabs software antivirus específico para el *cloud computing?*
4. ¿Crees que Windows es más vulnerable que el resto de los sistemas operativos? ¿Por qué?
5. ¿Sabes si se ha producido ya algún conato de ciberguerra en el mundo? Busca alguna noticia que hable del concepto y haz un pequeño resumen de lo hallado. Comentad en clase la repercusión que podría tener sobre el mundo una ciberguerra.

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **Recibe el nombre de *bug*:**
   a) Un hacker profesional que trabaja en el *cloud computing*.
   b) Un fallo de programación que hace peligrar la seguridad.
   c) Un tipo de virus que se reproduce y muta.
   d) Ninguna de las tres anteriores.

2. **Un gusano es:**
   a) Un subtipo de virus.
   b) Un subtipo de troyano.
   c) Un *hacker* malicioso.
   d) Un tipo de *bot*.

3. **El único intruso que entre su código ético tiene la norma de no hacer daño en sus intrusiones es:**
   a) El *script kiddie*.
   b) El *newbie*.
   c) El *cracker*.
   d) El *hacker*.

4. **¿Qué es la ingeniería social?**
   a) Un conjunto de técnicas para acceder a la información engañando a las personas.
   b) Una carrera universitaria de la rama de informática.
   c) Una forma de *hacking*.

Soluciones: 1b, 2a, 3d, 4a

6 Seguridad del software

vamos a conocer...

1. Recursos de seguridad del sistema operativo
2. Antimalware
3. Correo electrónico
4. Control de acceso a la información
5. Congelación
6. Destrucción de documentos

PRÁCTICA **PROFESIONAL**
Medidas activas y pasivas de seguridad del software

MUNDO **LABORAL**
OSI, la oficina de seguridad del internauta

y al finalizar esta unidad...

- Sabrás por qué existen los parches y la importancia de tener un software actualizado.
- Conocerás la diferencia entre tipos de cuentas de usuario y la precaución de uso de la cuenta de administrador.
- Podrás habilitar y utilizar otros recursos de seguridad de sistemas bajo Windows.
- Sabrás detectar el malware y las intrusiones, y aplicar las técnicas y herramientas de seguridad conocidas.
- Reconocerás el *spam,* el *hoax* y el fraude por correo electrónico y emplearás las correspondientes herramientas de seguridad activa y pasiva.
- Utilizarás el correo electrónico de forma respetuosa con la privacidad de otras personas y promoverás el uso de buenas prácticas.
- Sabrás qué son y para qué sirven las aplicaciones y tarjetas de tipo *freeze,* o congeladores, y cómo eliminar información de forma segura.

CASO **PRÁCTICO** INICIAL

situación de partida

Como vimos en el caso práctico inicial de la unidad anterior, Julia quedó en pasar por casa de su amiga Luisa para ayudarle a resolver sus dudas y problemas informáticos.

Recordemos que tiene un portátil, con sistema operativo Linux, sin antivirus instalado.

Aunque los problemas los tiene con su ordenador de sobremesa, que presumiblemente funciona bajo Windows, aunque no quedó claro en la conversación anterior.

Julia intentará resolver los problemas que ya se han presentado –en principio supone que se trata de problemas del software–, así como limitar en lo posible, para el futuro, la entrada de código malicioso o intrusos en sus sistemas.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Cuando Julia llega a casa de Luisa, en primer lugar decide ver el portátil. Funciona correctamente.

   Luisa dice que lo utiliza de tarde en tarde para navegar por internet, enviar y recibir correo y utilizar un procesador de texto. Ya sabemos que Linux no es invulnerable como Luisa y mucha gente piensa. Esto puede llevar a pensar que no se crea software antimalware para Linux.

   - ¿Existen aplicaciones antimalware que funcionan en sistemas bajo Linux?
   - ¿Qué aplicación básica y gratuita podría dejar instalada en el portátil como sistema de seguridad antimalware para la navegación y el correo electrónico?

2. El sistema operativo del portátil hace mucho tiempo que no ha sido actualizado.

   - ¿Pueden descargarse parches o actualizaciones de Linux? ¿De dónde?

3. En cuanto al equipo de sobremesa, tiene Windows Vista. Empezó a funcionar mal desde hace unos días, cuando descargó un antivirus de Internet. Si se pretende restaurar el sistema a un momento anterior, el calendario no muestra fechas disponibles.

   - ¿A qué puede deberse la falta de fechas disponibles en el calendario de restauración?
   - ¿Todos los antivirus descargados de Internet son de confianza?

4. El funcionamiento anormal del ordenador de sobremesa hace sospechar a Julia de la presencia de malware, seguramente adquirido al bajar el antivirus, que podría ser un falso antivirus, pero no sabe de qué tipo de malware se trata.

   - Cuando el funcionamiento anormal de un ordenador hace sospechar de la presencia de malware, ¿cómo podemos saber de qué tipo se trata?
   - Una vez descubierto el código malicioso, ¿cómo podemos eliminarlo?
   - Una vez eliminado todo el código malicioso detectado, ¿tenemos garantías de que el equipo volverá a funcionar con normalidad?

5. Live Messenger continúa sin poder abrirse, avisando de que el nombre de usuario o la contraseña son erróneos. Con toda seguridad la contraseña ha sido robada.

   - ¿Cuál es el sistema más utilizado para robo de contraseñas de programas de mensajería?
   - ¿Existe posibilidad de que pueda recuperarse la contraseña a pesar de que se calcula en varios días el posible robo de la misma?

1. Recursos de seguridad del sistema operativo

Como hablamos en la unidad anterior, los sistemas operativos están construidos con código y a todos los códigos de programa, antes o después, se les descubren *bugs* o agujeros de seguridad.

saber más

Diferentes estudios cifran el promedio de *bugs* a razón de uno por cada 1.000 líneas de código, tanto en software comercial como en código abierto.

La primera y fundamental norma que ha de seguirse en cualquier sistema operativo es que sea **original.** Solamente de esta forma se garantiza el servicio de descarga automático –o manual– de actualizaciones.

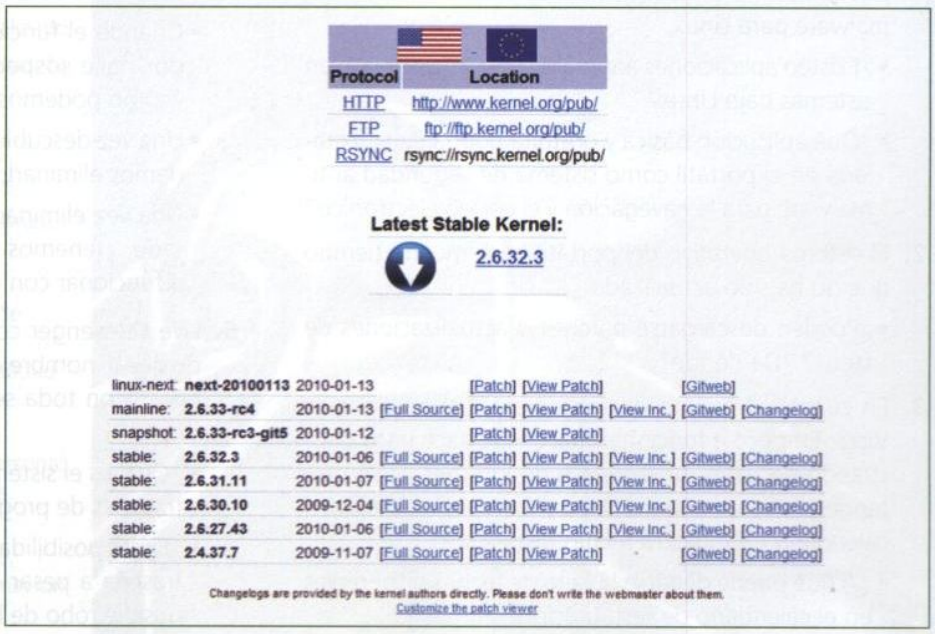
Cada sistema operativo de los que existen actualmente tiene sus propias herramientas de actualización en cuanto se detectan vulnerabilidades. **Linux,** el sistema operativo de software libre por excelencia, cuenta con la ventaja adicional de que al ser de código abierto, cualquiera tiene acceso al mismo, lo que hace que teóricamente cualquier persona del mundo experta en su código fuente, pueda detectar errores y comunicarlos o resolverlos directamente. Es decir, la «plantilla» de Linux en todo el mundo es inmensa. Las soluciones se encuentran de forma rápida y se aplican directamente. Esto también es motivo de desventajas: un código abierto lo es tanto para lo positivo como para lo negativo, pero hasta ahora Linux se ha considerado uno de los sistemas con menos vulnerabilidades, o tal vez sea que hay menos atacantes que se hayan impuesto el reto de boicotear su seguridad.

1.1. Parches

↑ Abstracción de la idea de parche.

Los parches son códigos que corrigen los errores de seguridad de los sistemas operativos.

En **Linux** se descargan desde el sitio www.kernel.org



Protocol	Location
HTTP	http://www.kernel.org/pub/
FTP	ftp://ftp.kernel.org/pub/
RSYNC	rsync://rsync.kernel.org/pub/

Latest Stable Kernel: 2.6.32.3

linux-next:	**next-20100113**	2010-01-13		[Patch]	[View Patch]	[Gitweb]	
mainline:	**2.6.33-rc4**	2010-01-13	[Full Source]	[Patch]	[View Inc.]	[Gitweb]	[Changelog]
snapshot:	**2.6.33-rc3-git5**	2010-01-12		[Patch]	[View Patch]		
stable:	**2.6.32.3**	2010-01-06	[Full Source]	[Patch]	[View Patch]	[View Inc.]	[Gitweb] [Changelog]
stable:	**2.6.31.11**	2010-01-07	[Full Source]	[Patch]	[View Patch]	[View Inc.]	[Gitweb] [Changelog]
stable:	**2.6.30.10**	2009-12-04	[Full Source]	[Patch]	[View Patch]	[View Inc.]	[Gitweb] [Changelog]
stable:	**2.6.27.43**	2010-01-06	[Full Source]	[Patch]	[View Patch]	[View Inc.]	[Gitweb] [Changelog]
stable:	**2.4.37.7**	2009-11-07	[Full Source]	[Patch]	[View Patch]		[Gitweb] [Changelog]

Changelogs are provided by the kernel authors directly. Please don't write the webmaster about them.
Customize the patch viewer

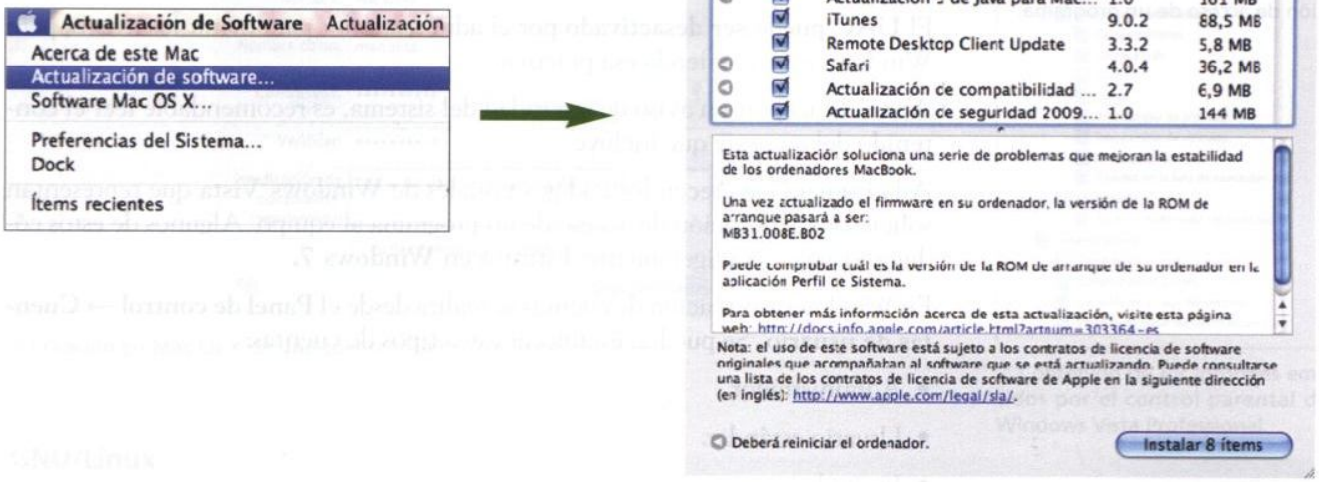
↑ Últimos parches anunciados por **Linux Kernel** en consulta realizada el 13 de enero de 2010.

saber más

Los parches no solamente se crean para los sistemas operativos, sino también para las aplicaciones.

La versión más reciente de las aplicaciones **Mac Os X** se encuentra en el sitio www.apple.com/es/software

Las actualizaciones se descargan en el propio equipo desde el menú **Apple → Actualización de software.** Enseguida se inicia una búsqueda de actualizaciones y se presentan las disponibles que necesita el equipo, como puede verse en la siguiente imagen.



En **Windows,** se accede a las actualizaciones desde **Windows Update,** en el Panel de control. Las diferencias del modo de acceso a actualizaciones difieren poco de una versión a otra de Windows.

1.2. Control de cuentas de usuario

Windows


Una función o programa de Windows


Un programa conocido que no forma parte de Windows


Un programa desconocido, sin firma digital


Un programa bloqueado por el administrador

↑ Códigos visuales de Windows Vista para la solicitud o denegación de acceso de un programa.

El control de cuentas de usuario (UAC, *User Access Control*) es una característica de **Windows** que ayuda a impedir cambios no autorizados en el equipo. **UAC funciona en modo de avisos o advertencias que se muestran en ventanas emergentes.** Si se está trabajando en modo administrador, solicitará la aceptación o denegación del cambio. Si se trabaja en modo usuario, solicitará la contraseña de administrador.

Cuando se trabaja en un equipo bajo Windows Vista, con frecuencia aparecen mensajes del UAC solicitando la autorización para realizar una tarea. Una práctica muy habitual a nivel de usuario estándar es otorgar la autorización sin leer el aviso, lo que puede comprometer la seguridad del equipo, puesto que este control está creado para evitar la entrada de ***malware***.

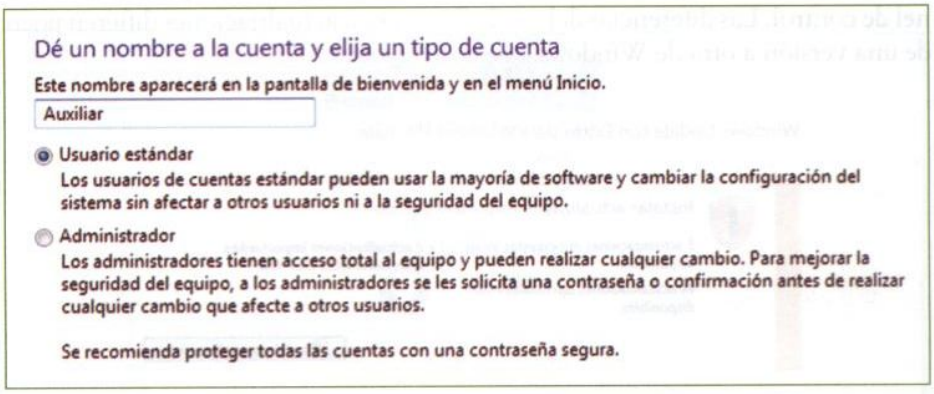
El **UAC puede ser desactivado** por el administrador para evitar los avisos, pero Windows no recomienda esa práctica.

Antes de aceptar un aviso de seguridad del sistema, es recomendable leer el contenido del mensaje que incluye.

A la izquierda aparecen los códigos visuales de **Windows Vista** que representan solicitud o denegación de acceso de un programa al equipo. Algunos de estos códigos visuales son ligeramente distintos en **Windows 7.**

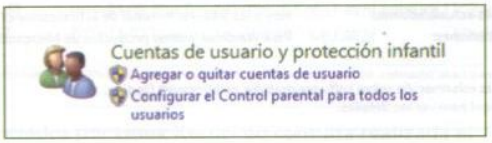
En Windows, la creación de cuentas se realiza desde el **Panel de control → Cuentas de usuario.** Se pueden establecer estos tipos de cuentas:

- Administrador.
- Usuario estándar.
- Invitado.



↑ Proceso de creación de una nueva cuenta de usuario estándar en Windows.

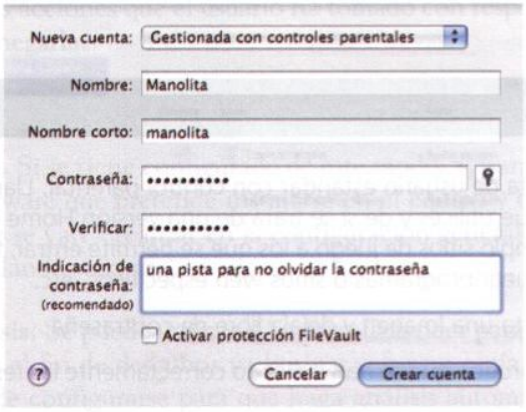
Puede establecerse control parental.



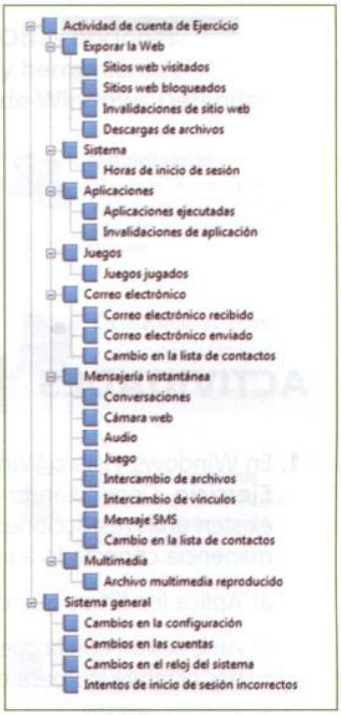
Mac OS X

En **Mac,** desde **Preferencias del sistema → Cuentas,** se pueden crear Grupos de cuentas y de ellas hay cuatro tipos:

- Root (súper administrador).
- De administrador.
- De usuario estándar.
- Gestionada con controles parentales.
- Invitado.



↑ Creación en Mac Os X de una cuenta infantil, con control parental



↑ Contenido de los informes emitidos por el control parental de Windows Vista Professional.

GNU/Linux

Linux permite una amplia configuración de las cuentas de usuario. Se pueden crear grupos de usuarios por privilegios asignados, aunque un usuario puede pertenecer a más de un grupo.

En Linux existen básicamente tres tipos de usuarios:

- **Root.** Súper administrador del sistema.
- **Usuario estándar.** Usuario con privilegios únicamente en su entorno de trabajo.
- **Usuarios especiales.** Tendrán los privilegios que determine el root.

Los usuarios pueden crearse, borrarse o modificar sus privilegios desde las herramientas de la interfaz que proporciona el sistema, según sus versiones, o desde la línea de comandos.

1.3. Cuenta de administrador

Cualquiera que sea el sistema operativo utilizado, la cuenta de administrador permite hacer todo tipo de cambios. No conviene que exista más de una cuenta de administrador en un mismo equipo, ya que pueden realizar operaciones contradictorias entre administradores, como modificar cuentas de usuario, instalar o desinstalar software o modificar los niveles de seguridad de Windows y otros programas.

Sin embargo, pueden crearse varias cuentas de usuario, con casi las mismas competencias que las de administrador, a excepción de permisos para realizar cambios que pueden afectar a la configuración de seguridad o de otros usuarios, además de tener vetada la instalación de software, para lo cual al usuario se le requiere la contraseña de administrador, que probablemente no conoce.

A la hora de realizar trabajo cotidiano en el equipo, es preferible utilizar una cuenta estándar en lugar de la cuenta de administrador, para evitar que la entrada de un intruso capte la configuración de administrador de forma fácil. Al intruso informático hay que ponerle el mayor número de impedimentos.

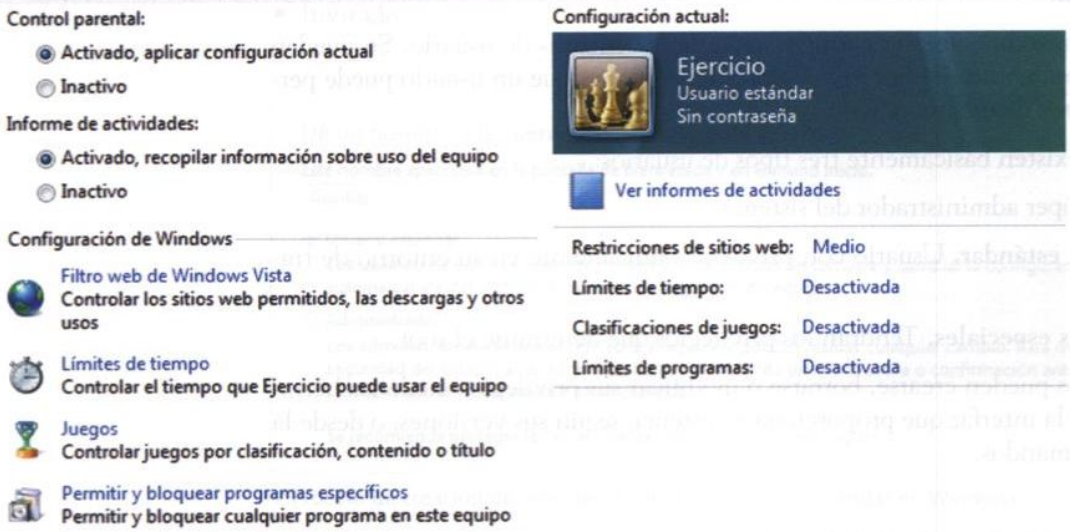
ACTIVIDADES

1. En Windows Vista o Windows 7, crea una cuenta de usuario estándar con control parental. Llama a la cuenta **Ejercicio.** Dependiendo del sistema operativo que utilices y de si se trata de una versión Home o Professional, existen unas restricciones u otras, como por ejemplo sitios de juego a los que se permite entrar, tiempo de permanencia conectado a internet, permitir o bloquear programas o sitios web específicos, etc.

a) Aplica los filtros que desees. Asigna a la cuenta una imagen y déjala libre de contraseña.

b) Abre sesión con la cuenta configurada y comprueba que se han aplicado correctamente las restricciones que has establecido para ella.

c) Si es posible en tu equipo, accede de nuevo a tu cuenta de administrador y observa el informe de actividades realizadas desde esa cuenta recién creada.



↑ Configuración del control parental con Windows Vista Professional.

Si no tienes disponible un sistema operativo bajo Windows, realiza el mismo ejercicio con tu sistema operativo, aprovechando las características de configuración de cuentas y de control parental que ofrece.

1.4. Otros recursos en Windows

Windows Defender

Cuando un usuario se conecta a internet puede estar recibiendo, de forma desapercibida, algún software espía que comenzará a actuar de inmediato o que se ejecutará cuando esté programado para hacerlo.

Windows Defender se abre desde el botón **Iniciar → Todos los programas → Windows Defender.**

Dispone de un menú en su parte superior que permite configurarlo y analizar el equipo. Además dispone de un **historial** por fechas de software **sospechoso** de ser *spyware* junto a las acciones que el usuario ha tomado con respecto a él: permitir su ejecución o denegarla.

Puede ejecutarse de dos formas distintas:

- **En tiempo real.** Si se tiene configurado de este modo, avisará cuando advierta que hay un spyware que pretende instalarse en el equipo y también advertirá de cambios que se van a realizar en la configuración general del equipo cuando se está instalando software.
- **En modo análisis.** Se puede utilizar Windows Defender para hacer un análisis del equipo con el fin de descubrir y eliminar software espía que se encuentre instalado. Puede configurarse para que haga análisis automáticos cada cierto tiempo y para que elimine el spyware que encuentre.

saber más

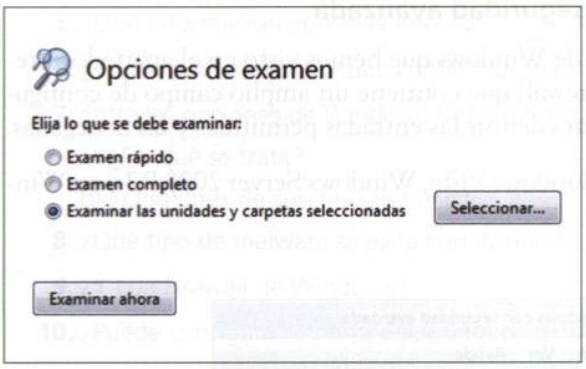
Otras opciones y herramientas de Windows Defender

Microsoft SpyNet
Únase a la Comunidad en línea que ayuda a identificar y detener las infecciones de spyware

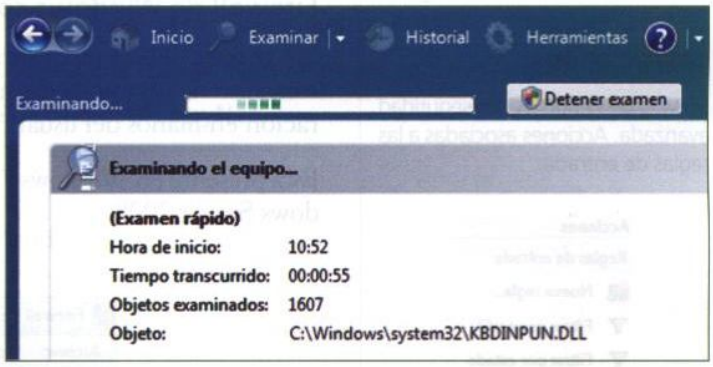
Explorador de software
Vea o supervise todo el software que se está ejecutando en el equipo

Elementos en cuarentena
Quite o restaure software que Windows Defender impidió que se ejecutara

Elementos permitidos
Vea el software que eligió que no supervisará Windows Defender

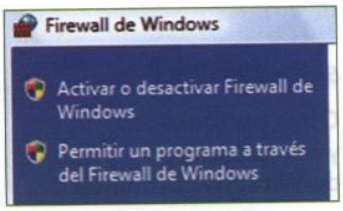


↑ Opciones de análisis que ofrece Defender.



↑ Examen rápido del equipo con Windows Defender. Muestra el total de objetos examinados hasta el momento y qué objeto está analizando ahora.

También puede decidirse realizar un análisis total o parcial de las unidades o carpetas que el usuario decida, que puede ser rápido o completo (más exhaustivo).



Firewall de Windows

Impide la entrada de intrusos y de programas maliciosos a través de la red o de internet. Del mismo modo, controla que no pueda salir malware hacia otros equipos.

El usuario puede decidir si desea tenerlo activado o desactivado.

En caso de tenerlo activado, y para evitar que el firewall emita avisos o impida la ejecución de programas que considera maliciosos y que, sin embargo, tienen la confianza del usuario, puede permitirse expresamente la ejecución de determinados programas.

Las opciones para este programa son:

- **Activado.** Emite avisos cuando se produce un intento de conexión al equipo desde el exterior. El usuario puede decidir si permite la entrada o la deniega. También puede configurar una lista de excepciones para que en lo sucesivo no se generen avisos para los elementos de la lista.
- **Desactivado.** No es recomendable a no ser que se disponga de otro firewall externo a Windows.
- **En modo bloqueo completo.** Es el sistema que proporciona más seguridad, aunque bloquea todos los intentos no solicitados de conexión al equipo sin dar aviso de ello al usuario. No obstante, es recomendable cuando se trabaja en un entorno de red no seguro, como puede ser la de hoteles, restaurantes, hospitales o aeropuertos, o cuando en la propia red circulan gusanos y otro malware.

saber más

El propio Firewall de Windows advierte de la necesidad de tener un firewall ejecutándose en el equipo. Si se desactiva el de Windows, debería habilitarse otro.

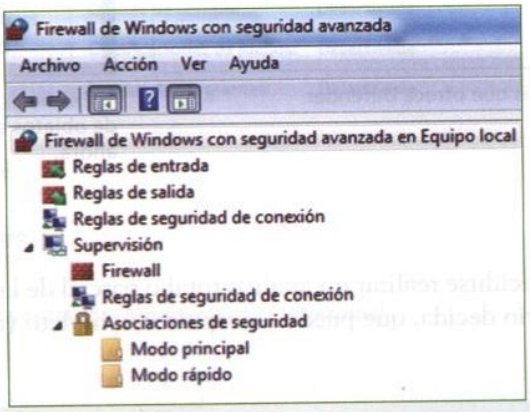
Firewall de Windows con seguridad avanzada

No se trata del mismo firewall de Windows que hemos visto en el apartado anterior, sino de otra aplicación firewall que contiene un amplio campo de configuración en manos del usuario para definir las entradas permitidas y las denegadas.

Está presente en Windows 7, Windows Vista, Windows Server 2008 R2 y en Windows Server 2008.

saber más

Firewall de Windows con seguridad avanzada. Acciones asociadas a las reglas de entrada:



↑ Firewall de Windows con seguridad avanzada permite crear reglas para las conexiones de entrada y salida, así como definir unas reglas de seguridad de la conexión y realizar una supervisión de cómo se encuentra configurado todo el entorno del firewall.

Al hacer clic en cada una de las reglas que se muestran en la imagen anterior, se despliega a la derecha una ventana de acciones relativas a esa regla, entre ellas los filtros por perfil, por estado o por grupo, así como la posibilidad de crear nuevas reglas y exportar la lista. Las listas de reglas exportadas se pueden conservar en una carpeta en modo texto normal o delimitado por comas.

El Firewall de Windows con seguridad avanzada es un potente conjunto de filtros que estudiaremos con mayor profundidad en la próxima unidad.

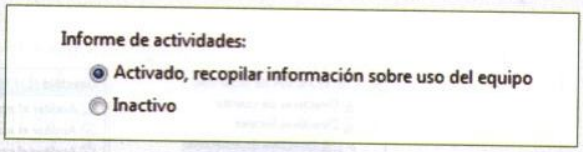
ACTIVIDADES

2. Responde a las siguientes preguntas:

a) ¿Para qué sirve el control parental?

b) ¿Puede utilizarse el control parental para restringir el acceso de personas adultas a determinados programas o sitios web?

3. ¿Cómo se puede activar la emisión de informes de actividades que se realizan con una determinada cuenta de usuario si usamos Windows Vista Professional?



4. ¿Y si lo que queremos es leer los informes de actividades generados con el filtro parental sobre una cuenta de usuario?

5. ¿Qué información aporta el informe de actividades realizadas por un usuario en su cuenta controlada?

6. ¿Cómo podemos saber qué contenidos tiene bloqueados el control parental realizado con Windows Vista?

7. Entre las opciones de Windows Defender está la de **Microsoft SpyNet.**

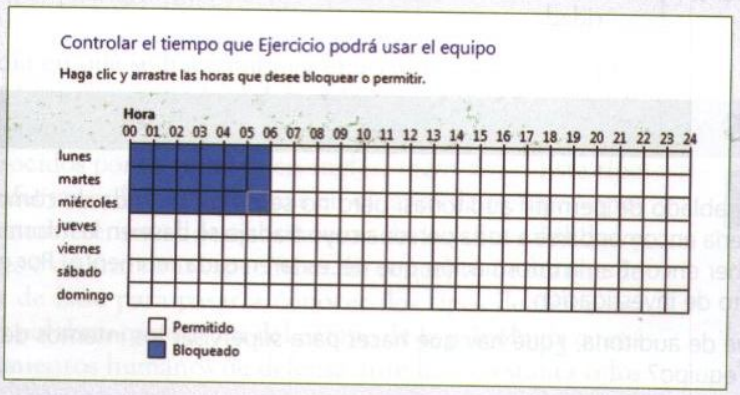
a) ¿De qué se trata?

b) ¿Qué tipos de suscripción tiene?

8. ¿Qué tipo de malware se evita con Windows Defender?

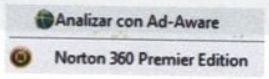
9. ¿Y con Firewall de Windows?

10. ¿Puede configurarse en tu equipo un control de tiempo limitado para un usuario? ¿Cómo?



saber más

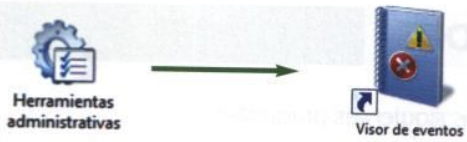
Para pasar un antivirus, un antiespía u otro programa antimalware, se hace clic sobre la unidad de disco, carpeta o archivo con el botón secundario del ratón y se selecciona el software de seguridad con el que deseemos hacerle un análisis, de los que tenemos instalados en el equipo.



Otras medidas de seguridad pasiva

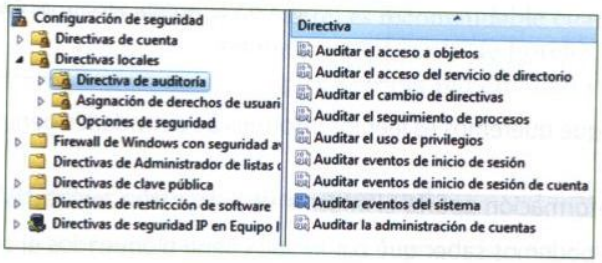
A continuación enumeramos algunas medidas de seguridad pasiva relativas al software y la información.

- **Eliminación de virus** con antivirus o de forma manual. Puede hacerse sobre una unidad de disco, una carpeta completa o un archivo concreto y debería ejecutarse periódicamente un **análisis completo** de todo el equipo.
- **Comprobar los registros de eventos.** En Windows se accede a los registros del siguiente modo:



↑ Visor de eventos de Windows.

- **Permitir auditorías de seguridad** en el sistema operativo. Para ello, en Windows se hace clic en el botón **Iniciar → Panel de control → Herramientas administrativas → Directiva de seguridad local.** Después se hace clic en la flechita junto a **Directivas locales → Directiva de auditoría** (versiones profesionales de Vista y 7).



- **Restaurar el sistema** a una fecha anterior al momento en que ha dejado de funcionar de forma correcta y no hayan servido las medidas antimalware aplicadas anteriormente ni otro modo de conseguir la estabilización del sistema para un uso normal. Con la restauración no se pierde la información archivada pero sí las aplicaciones y actualizaciones realizadas, así como los cambios de configuración de fecha posterior a la elegida para la restauración.
- **Recuperar datos** con software específico o reinstalarlos desde copias de seguridad.

caso práctico inicial

Algún código malicioso consigue eliminar del registro la relación de fechas disponibles para restaurar el sistema.

ACTIVIDADES

11. Investiga. Hemos hablado de permitir auditorías, pero no se ha dicho nada de cómo debe hacerse. Una de las tareas que debería encomendarse a toda persona cuyo trabajo se base en la informática (en constante evolución) es la de saber encontrar la información que necesita en cada momento. Por este motivo, la siguiente pregunta es un reto de investigación:

Usando la Directiva de auditoría, ¿qué hay que hacer para supervisar los intentos de acceso y de cambio de configuración del equipo?

2. Antimalware

2.1. Introducción

En los últimos años está descendiendo la creación de los tradicionales virus y gusanos, en tanto que se está produciendo un incremento en adware y spyware, pero, sobre todo, lo que más ha ido creciendo ha sido el número de troyanos. Cada vez hay más equipos infectados de malware y los creadores de antivirus creen que, en parte, se debe a la gran proliferación de **falsos antivirus** que se descargan creyendo que son antivirus gratuitos. Los troyanos más frecuentes hoy día son los que ejecutan acciones de *phishing*, también llamados troyanos bancarios. Si antes se creaba, por ejemplo, un virus capaz de infectar a millones de máquinas de manera indiscriminada, hoy día existen millones de códigos malware, capaces de infectar, cada uno de ellos, a un número limitado de máquinas. Entonces se habla de especialización del malware y de ataques dirigidos a intereses concretos.

2.2. Técnicas

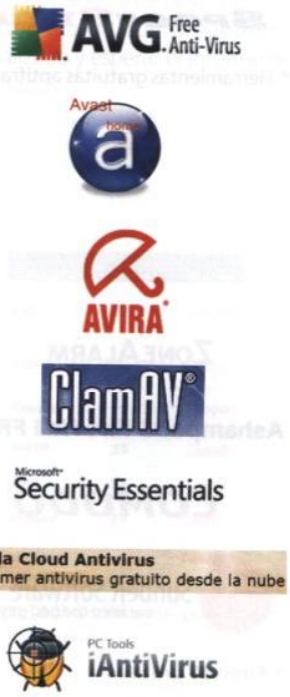
Los antivirus actuales detectan no solamente los virus que, como hemos dicho, cada vez se crean en menor cantidad, sino todo tipo de malware. Por lo tanto, al hablar de antivirus lo haremos en su significado más completo.

Sabemos que tener instalado un antivirus no es garantía de tener protegidos el equipo y sus periféricos de ataques mediante malware. Diariamente se crean nuevos códigos, cada vez más sofisticados, que incluso pueden mutar, que se regeneran y se reenvían, que utilizan las direcciones de correo electrónico que encuentran en los registros de usuario para envío de spam, códigos de bot, programas espía y aplicaciones destinadas a phishing. Symantec, el creador de Norton Antivirus, en septiembre de 2009 había detectado 120 millones de variantes de malware.

Los nuevos virus, al igual que los antiguos, explotan las vulnerabilidades del software para instalarse y ejecutarse.

Ataques de día cero

La víspera, o el mismo día en que se hace pública una vulnerabilidad, se producen ataques que la explotan, antes incluso de que las empresas antivirus hayan lanzado el código antimalware específico. A estos ataques se les llama de «día cero», también conocidos por su nombre en inglés, «*zero-day*». Este tipo de ataques es capaz de infectar miles de máquinas en el lapso de tiempo –apenas unas horas– que transcurre entre el descubrimiento de la vulnerabilidad y el lanzamiento de parches o de antivirus específicos. El concepto de **ataque de día cero** nos va a servir de base para pasar a conocer dos tipos de defensas: **reactiva** y **proactiva,** dos palabras que parten del campo de la **psicología** cuando explica los comportamientos humanos de defensa ante las agresiones o los contratiempos.



↑ Antivirus gratuitos.

↑ Software gratuito antiespía.

NETCRAFT

SPOOFSTICK

↑ Herramientas gratuitas antifraude.

ZONEALARM

Ashampoo® FireWall FREE

COMODO

Sunbelt Software
we keep the bad guys out™

↑ Firewall gratis.

caso **práctico** inicial

Existen programas antivirus y de seguridad en internet, también para Linux, algunos de código libre y otros comerciales.

Ejemplos:

- AVG Anti-Virus Free Edition.
- ClamAV.
- Avast.
- NOD32.

caso **práctico** inicial

El uso de un antivirus para desinfectar el sistema no implica que el sistema vuelva a funcionar con normalidad, a pesar de que el código malicioso haya sido suprimido.

Tipos de defensa

- **Reactiva.** Para que un antivirus detecte un malware determinado y pueda actuar contra él, antes tiene que conocer su código y su comportamiento. En pocas palabras, la defensa reactiva es aquella que se aplica después de que se haya producido un ataque.
- **Proactiva.** Consiste en dotar al software antimalware de unos algoritmos de **detección inteligente de código malicioso** sin necesidad de haber creado un anti-código específico para él, es decir, sin que ese código malicioso esté incluido en las bases de datos asociadas al programa antimalware. Estos algoritmos se basan en técnicas heurísticas que no solamente ven un código extraño sino que son capaces de detectar actividades anormales en el equipo, como el intento de modificación del código en un programa instalado o en los registros del sistema operativo.

Con el fin de hacer frente a los ataques de **día cero,** las compañías que fabrican software antimalware están empezando a crear un software de defensa **proactiva,** frente a la defensa **reactiva** del clásico antivirus.

Nuevas definiciones

Los mejores programas antivirus o, mejor dicho, antimalware, no solamente cubren el código malicioso sino también la acción de los intrusos informáticos, el spam y los intentos de phishing. Algunos incorporan utilidades específicas para la navegación, como por ejemplo cortafuegos.

2.3. Herramientas

Existen herramientas gratuitas y comerciales. En el margen encontrarás **algunas marcas** de software que producen herramientas y versiones gratuitas anti malware y cortafuegos. La lista está actualizada a diciembre de 2009. Posteriormente pueden haberse producido cambios.

Existen buenas firmas comerciales –como Norton, Panda o Kaspersky– para detectar el malware antes de que se instale en el equipo y, por supuesto, para eliminarlo una vez que se ha instalado.

No basta con tener instalado un buen antivirus –inclusive los que tienen aplicaciones de seguridad en internet– si no se descargan las actualizaciones y se realizan análisis exhaustivos cada cierto tiempo en todo el equipo.

2.4. Herramientas de auditoría parcial

Además existe la posibilidad de hacer un escaneo del equipo mediante herramientas on line. A continuación haremos una relación clasificada de ellas.

Escaneo de puertos

Los servicios más habituales, como HTTP, FTP o TELNET tienen asignados por defecto sus propios puertos. Por ejemplo, si se está navegando por internet, estará abierto el puerto 80, si se está realizando un envío FTP, el puerto 21, o si se está

usando TELNET, el número 23. Si no se están utilizando estos servicios o no se piensan usar durante largo tiempo, lo más seguro es cerrar los puertos correspondientes.

Algunos programas realizan un escaneo de puertos en el equipo para mostrar al usuario cuáles son los que tiene abiertos, cerrados o bloqueados por algún firewall. A continuación indicamos algunas herramientas on line de escaneo de puertos:

- **UPSEROS** – on line.

  http://www.upseros.com/portscan.php
- **Asociación de internautas** – on line.

  http://www.internautas.org/w-scanonline.php
- **GRC** – on line.

  https://www.grc.com/x/ne.dll?bh0bkyd2
- **SecurityMetrics** – on line.

  https://www.securitymetrics.com/portscan.adp
- **Simple Port Tester** – escritorio.
- **Free IP scanner** – escritorio. Analiza además las direcciones IP ocupadas en una red.
- **Free Port Scanner,** de NSAuditor.

  Análisis de aplicaciones inseguras, actualizaciones no instaladas y otras vulnerabilidades del sistema
- **Secunia** (on line)

  http://secunia.com/vulnerability_scanning/online
- **Microsoft Baseline Security Analyzer** (escritorio – shareware)
- **PC Security Test** (escritorio)
- **VirusPortal** (on line)

  http://www.virusportal.com/es/descargas/down_run.shtml

caso **práctico** inicial

Para conocer el código malicioso concreto que se ha instalado en un ordenador o dispositivo, la mejor forma es hacer un análisis exhaustivo del mismo con un antivirus actualizado y esperar el informe de resultados.

Program	Port	Status
FTP	21	Danger!
SSH	22	Stealth
Telnet	23	Danger!
SMTP	25	Closed
DNS	53	Closed
Finger	79	Closed
HTTP	80	Danger!

↑ Parte del análisis de puertos de SecurityMetrics.

saber más

Herramientas de **escritorio** son aquellas que se han de instalar en el ordenador para que funcionen. En cambio, las herramientas **on line** se ejecutan sin instalación, solamente con conexión a internet.

ACTIVIDADES

12. Desde que se descubre una vulnerabilidad hasta que se emite y publica el parche correspondiente pueden ocurrir ataques a equipos. ¿Cómo se llama este tipo de ataques?

13. Para la defensa proactiva, ¿se necesita conocer un código malicioso concreto para aplicar medidas de seguridad activa?

14. Si no estuviese instalado anteriormente, descarga e instala *Ad-Aware*. Escanea tu *pen drive* y haz un análisis general del disco duro. Tras el análisis, anota el número de códigos maliciosos encontrados.

15. Escanea tus puertos con cualquiera de las herramientas on line. Comprueba si tienes puertos abiertos que nunca utilizas.

3. Correo electrónico

3.1. Herramientas

Spamihilator Anti-Spam-Filter

SpamBayes

SpamAssassin

SPAMTERRIER

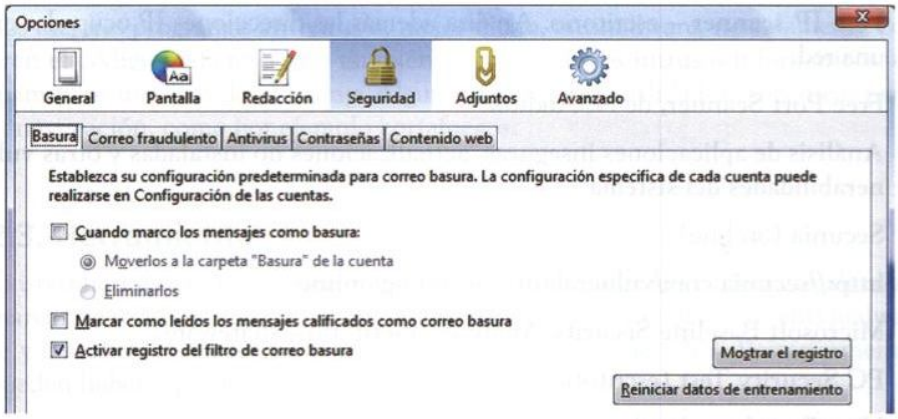
↑ Herramientas gratuitas antispam.

Uno de los principales problemas relacionados con el correo electrónico, aunque no el único, es el **spam,** es decir, la recepción de correos electrónicos, con publicidad u otro tipo de información, de forma indiscriminada.

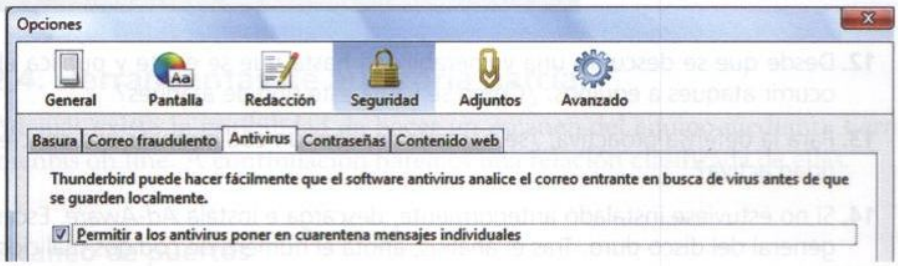
Normalmente, los servicios de correo electrónico así como los programas que los gestionan, ya sean web o no, cuentan con un filtro antispam, que **puede configurarse** según nuestras necesidades, y en caso de que algún e-mail se salte el filtro, se puede añadir manualmente a la lista de correos no deseados.

Mozilla Thunderbird es un gestor de correo electrónico que utilizaremos como ejemplo por contener casi todas las medidas de seguridad que se le pueden pedir a un programa de este tipo.

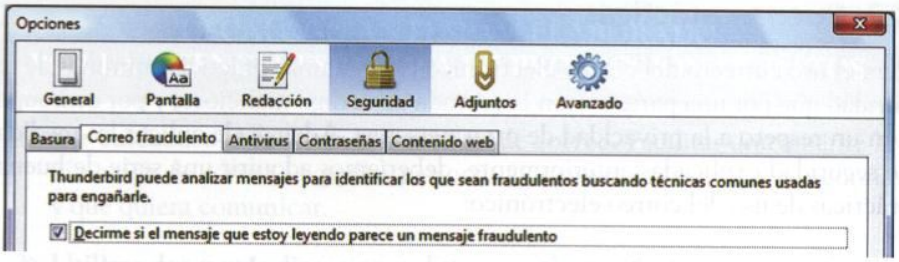
Este sistema tiene autoaprendizaje, y una vez marcado un correo recordará y actuará en consecuencia para el futuro.



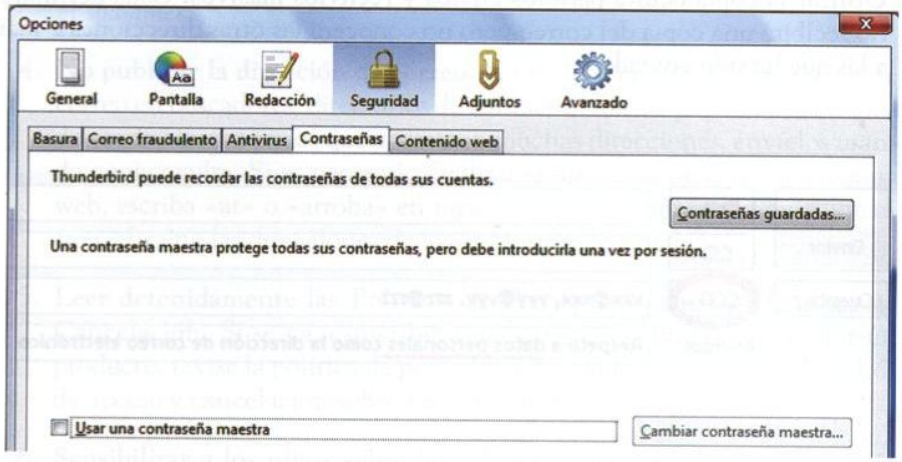
En las pestañas superiores tiene, además del **correo basura** o **spam,** filtros para correo fraudulento, antivirus, contraseñas y contenido web, que comentaremos a continuación; la explicación va después de cada imagen.



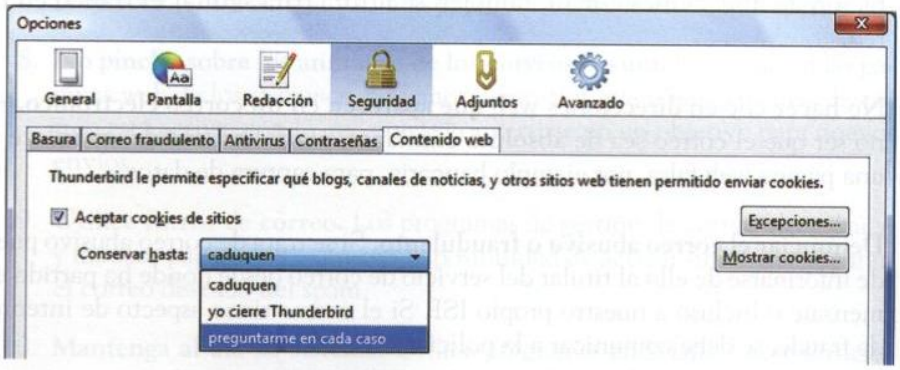
Con esta opción se permite que el antivirus que se tenga instalado en el equipo analice los mensajes recibidos.



Deja en manos de Thunderbird decidir qué correo tiene aspecto de **fraudulento.** En todo caso, si no lo es, puede indicársele lo contrario y «aprenderá» para el futuro.



Se puede configurar para recibir correo de cuentas y orígenes distintos. Es posible que para cada correo tengamos una contraseña diferente. El programa permite crear una **contraseña maestra** para gestionar todos esos correos.



Permite aceptar o denegar ***cookies*** de sitios, admitiendo las excepciones marcadas por el usuario. Se puede configurar el tiempo de permanencia de las *cookies*.

caso **práctico** inicial

Uno de los robos de identidad más frecuentes que se producen en internet es el de los programas de mensajería y correo electrónico, sobre todo si lo usan personas jóvenes que no dan demasiada importancia a la seguridad del correo electrónico.

Este tipo de robos suele producirse por correo, abriendo alguna postal o alguna aplicación que solicita la entrada de datos de usuario y contraseña.

El robo de contraseñas puede comunicarse a los proveedores de correo e incluso a la policía, pues está penalizado por la ley. Lo importante es tener medios para demostrar que una cuenta de correo o mensajería ha sido robada. Para ello es fundamental actuar lo antes posible, porque si transcurre mucho tiempo, poco puede hacerse, salvo en servidores de correo de pago, cuya titularidad puede demostrarse por factura.

3.2. Buenas prácticas

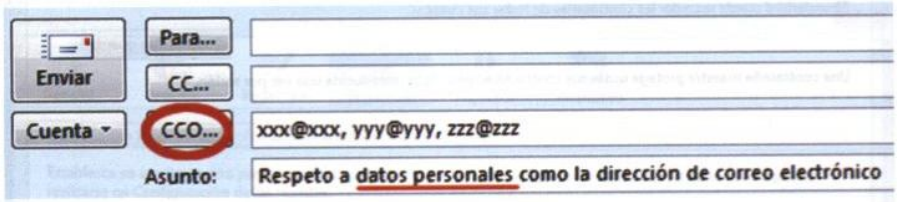
Para el uso correcto del correo electrónico existen unas prácticas mínimas de seguridad que por una parte evitan la entrada de código malicioso, y por otra suponen un respeto a la privacidad de otras personas. Además de aplicar las medidas de seguridad explicadas anteriormente, deberíamos adquirir una serie de buenas prácticas de uso del correo electrónico:

- **Prudencia antes de abrir archivos adjuntos,** aunque el emisor sea de confianza. Una fotografía, un documento de texto o cualquier otro archivo pueden contener oculto código malicioso. Conviene configurar el correo para que el antivirus instalado compruebe los mensajes. En todo caso también puede guardarse el archivo adjunto, sin abrir, en una carpeta y pasar por ella el antivirus antes de abrirlo, sobre todo si se trata de un fichero comprimido.

saber más

La dirección e-mail de una persona es un dato personal protegido por la ley.

- **Utilizar la copia oculta para los envíos y reenvíos masivos.** Cada destinatario recibirá una copia del correo pero no conocerá las otras direcciones e-mail a las que ha sido enviado.



- **Borrar lista de direcciones e-mail del correo recibido antes de reenviarlo.** En los correos recibidos que no han cumplido con la buena práctica del punto anterior, aparecerá la lista de direcciones de otros destinatarios del mismo correo que nos ha llegado. Antes de reenviarlo a otras personas, procederemos a borrar dicha lista, que figurará en el contenido del mensaje.

- **Romper cadenas o correo *hoax*.** Aparte de ser un correo con fines de captación de direcciones e-mail, también se utiliza para saturar el tráfico en la red.

- **No hacer clic en direcciones web que aparecen en un correo electrónico.** A no ser que el correo sea de **absoluta** confianza, puede tratarse de un enlace a una página web falsa, por ejemplo bancaria, para captura de datos.

- **Denunciar el correo abusivo o fraudulento.** Si se trata de correo abusivo puede informarse de ello al titular del servicio de correo desde donde ha partido el mensaje o incluso a nuestro propio ISP. Si el correo tiene aspecto de intento de fraude, se debe comunicar a la policía.

saber más

Las direcciones que habilitan los proveedores de correo para denunciar los abusos, suelen ser del tipo:
abuse@proveedordecorreo.xx

A la hora de dar parte de uno de estos abusos y fraudes, es necesario conservar y presentar el **encabezado** del mensaje, que explica con detalle de IP los puntos por donde ha pasado y, sobre todo, la IP de donde partió.

DECÁLOGO ANTI SPAM ELABORADO POR LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

1. **Ser cuidadoso al facilitar la dirección de correo.** Facilitar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y que quiera comunicar.

2. **Utilizar dos o más direcciones de correo electrónico.** Utilice una dirección para aquellos casos en los que no se confíe o conozca lo suficiente al destinatario, y otra dirección personal que sea conocida únicamente por sus amigos o por sus contactos profesionales.

3. **Elegir una dirección de correo poco identificable.** Para crear una dirección de correo electrónico y reducir el envío de spam, sería conveniente no introducir campos que sean potencialmente identificables por el *spammer*.

4. **No publicar la dirección de correo.** No se debe anunciar la dirección de correo en buscadores, directorios de contactos, foros o páginas web. Cuando envíe correos en los que aparezcan muchas direcciones, envíelos usando copia oculta. Si es necesario facilitar la dirección de correo en alguna web, escriba «at» o «arroba» en lugar de @. Asimismo, si reenvía un correo, elimine las direcciones de los anteriores destinatarios.

5. **Leer detenidamente las Políticas de Privacidad y las Condiciones de Cancelación.** Si se va a suscribir a un servicio on line o a contratar un producto, revise la política de privacidad. No dude en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

6. **Sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea.** Los niños son objetivos ideales para proporcionar información sobre la composición y las prácticas de consumo del hogar. Además, los correos pueden tener contenidos no aptos para los niños.

7. **No es conveniente contestar al spam.** Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un *spammer* recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más spam.

8. **No pinche sobre los anuncios de los correos basura.** Entrando en las páginas web de los *spammers* podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos.

9. **Utilice filtros de correo.** Los programas de gestión de correo electrónico y muchas páginas web ofrecen la posibilidad de activar filtros que separan el correo deseado del spam.

10. **Mantenga al día su sistema.** Utilice programas **antivirus** y **actualizaciones y parches** que corrigen los problemas detectados en los programas de su equipo. Además, es muy recomendable la instalación de **cortafuegos** para monitorizar lo que ocurre en el ordenador.

↑ *Pen drive* biométrico con acceso a su información mediante huella dactilar.

4. Control de acceso a la información

Para velar por los principios de la seguridad de la información: **confidencialidad, integridad y disponibilidad,** es necesario establecer controles de acceso, que pueden implementarse sobre el sistema operativo, sobre las aplicaciones, en bases de datos, sobre programas específicos de control de acceso o mediante dispositivos hardware.

Conviene repasar y recordar los controles de acceso al entorno físico, porque para acceder a la información se aplican prácticamente los mismos.

Identificación y autenticación. Mediante algo que se pueda portar (por ejemplo, tarjeta magnética), algo que se conoce (contraseña) o algo físico, biológico o fisiológico (biometría). Una vez realizada la identificación y la autenticación, cada usuario dispondrá de un determinado nivel de acceso a la información en función de los parámetros que se establezcan, como por ejemplo:

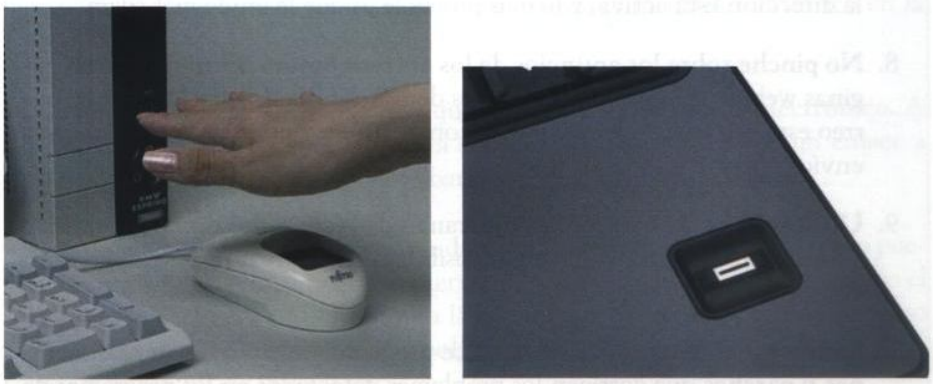
- **Permisos por roles.** Permitir o denegar el acceso a determinadas aplicaciones o bases de datos, según el rol que desempeñe cada persona en la organización. Por ejemplo: analista de sistemas, programador o usuario base.
- **Modalidad de acceso.** Aunque todas las personas reseñadas en el ejemplo anterior tuviesen acceso a las mismas aplicaciones o bases de datos, es posible establecer unos permisos determinados para cada una de ellas en cuanto a lectura, escritura (modificación y eliminación) o ejecución.
- **Limitaciones horarias.** Permitir o denegar el acceso al equipo, o a un determinado software o información, según franjas horarias o días de la semana o del mes.

Los criterios de acceso se establecerán asociados a cada contraseña, tarjeta, llave o factor biométrico. Una vez realizada la autenticación solamente se podrá trabajar basándose en ellos.

saber más

Trabajando en la nube ¿se necesita antivirus local?

«En el *cloud computing,* las aplicaciones no se ejecutan en la nube. Se ejecutan en el equipo del usuario. Y este no es un terminal tonto. Seguirán existiendo vulnerabilidades que se ejecutarán en el *desktop* que seguirá disponiendo de almacenamiento de disco, que los cibercriminales intentarán infectar con un capturador de teclado, un capturador de pantalla, un ladrón de identidades, etc. En este nuevo paradigma también existirán "oportunidades", que sin duda serán explotadas». *David Perry, experto mundial en hacking, malware y cibercrimen.*



↑ A la izquierda, lector de las venas palmares incorporado al ratón, sistema creado por Fujitsu & IBM. A la derecha, lector de huella dactilar en un portátil HP. Ambos sistemas realizan la autenticación y, en función de ella, permiten o deniegan el acceso por áreas, tiempos o modalidades de acceso. Una manera de proteger información crítica.

ACTIVIDADES

16. Escribe verdadero o falso para cada una de las siguientes afirmaciones:

a) El correo-cadena que me envía un amigo pidiéndome el reenvío a otras personas es spam.

b) Un e-mail recibido de un banco en donde tengo una cuenta corriente, pidiendo mis datos de usuario, es spam.

c) El fraude por correo electrónico enfocado a obtener contraseñas de usuarios y otros datos personales se llama phishing.

d) Si mi gestor de correo electrónico decide enviar a la carpeta spam un correo recibido que no es spam, puedo configurarlo para que la siguiente vez que se reciba correo de la misma fuente ya no lo considere spam.

e) En términos generales, podemos decir que Thunderbird (como otros gestores de correo de las mismas características) es un gestor inteligente, porque aprende con el tiempo.

17. Si aún no has descargado ni configurado Thunderbird, descárgalo e instálalo en tu ordenador del aula o de casa. Configúralo para recibir y enviar correo de tu cuenta habitual de correo (por ejemplo, Gmail, Live o Hotmail). Los pasos son muy sencillos, ya que el mismo Thunderbird «sabe» cómo tiene que hacerlo y conoce el POP3 y SMTP del proveedor de correo.

- Cuando el correo haya sido configurado correctamente, comenzarán a bajarse todos los correos que tengas en tu cuenta, con lo que el proceso puede resultar bastante largo (incluso horas, dependiendo del número de mensajes enviados y recibidos que tengas en tu cuenta).
- A partir de ese momento, los mensajes quedan archivados en tu equipo, con lo cual no necesitas tener conexión a internet para consultarlos.
- No necesitarás entrar en tu correo web para enviar o recibir mensajes, ya que estos llegarán de forma automática a tu equipo avisándote mediante una señal de que hay correo nuevo.
- Tampoco necesitarás entrar en tu correo web para enviar mensajes de correo electrónico.
- Configura todo lo relativo a seguridad que se ha visto al explicar Thunderbird.

18. Unas cuantas preguntas sobre tus correos recibidos, enviados y reenviados:

a) Cuando recibes correos que te ha reenviado alguna persona amiga o conocida, ¿lo habitual es que pueda verse en ellos el listado de direcciones de correo electrónico a las que ha enviado el mismo mensaje a la vez que a ti?

b) ¿Es habitual también que en el texto del mensaje aparezca la lista de direcciones e-mail a las que fue enviado en un envío anterior?

c) Habitualmente, cuando haces reenvíos de correo que te parece interesante:

- ¿Escoges directamente como destinatarios a todos tus contactos o sueles seleccionar aquellos a los que crees que puede interesarles el tema?
- ¿Has pensado alguna vez por qué se insiste tanto en que se reenvíen ciertos mensajes de correo?
- ¿Has recibido alguna vez correo de algún banco u organismo público en donde se te solicite que accedas a una web para comprobar tus datos debido a algún tipo de error que han observado?
- ¿Has denunciado en alguna ocasión haber recibido correo abusivo o fraudulento? En caso afirmativo, ¿a quién has escrito para comunicarlo?

19. Si ya tienes instalado y estás utilizando Thunderbird, ¿cómo puedes hacer para que se vean los datos de cabecera completos? (Recuerda que los datos de cabecera indican el camino por servidores y sus IP, que ha recorrido el mensaje hasta llegar a destino).

5. Congelación

No podíamos terminar esta unidad sin hacer referencia a un software que resulta de mucha utilidad en múltiples ocasiones. Se trata de los programas que llamamos «congeladores», que por lo general permiten al usuario instalar programas o realizar todos los cambios que quieran en la configuración, navegar por internet, enviar o recibir correos, dejar «recordar contraseñas» por defecto en el equipo y cualquier otro cambio. Pero lo relevante es que, tras reiniciar el equipo, todo vuelve a estar como quedó inmediatamente antes de instalar el software congelador. Desaparece el historial de internet, las cookies, las contraseñas guardadas y, ¡ojo!, los archivos almacenados posteriormente a la congelación. Por esta última razón, para guardar un archivo creado mientras se usa el ordenador, se debe utilizar un dispositivo externo, una partición no congelada del disco o un disco duro adicional igualmente no congelado. También, en último extremo, enviarse por correo electrónico o a un almacenamiento remoto.

¿En qué lugares es conveniente o necesario instalar un congelador?

En los ordenadores especialmente vulnerables porque son usados por muchas personas, que introducen dispositivos extraíbles probablemente infectados de malware, que realizan cambios de configuración, que descargan programas dañinos... Por ejemplo:

- Aulas de centros académicos.
- Cibercafés.
- En cualquier ordenador que se quiera conservar siempre con la configuración que se decidió como óptima.

¿Se puede considerar un sistema de protección del hardware?

Sí, puesto que el sistema operativo, las aplicaciones y los datos quedan siempre «en el mismo estado» que cuando se hizo la «congelación». No obstante, mientras el ordenador está en uso, es vulnerable al malware y a cualquier otro peligro de los que hemos estudiado. La ventaja es que, tras el reinicio, todo vuelve a ser como antes, excepto las intrusiones que haya podido haber durante sus horas de funcionamiento sin apagar, que, por supuesto, pueden haber servido para captar datos del equipo y del usuario.

¿Qué ocurre si en un ordenador con el disco duro «congelado» entran virus?

Teóricamente, al apagar y reiniciar el equipo, todo vuelve a estar como al principio, es decir, sin virus, a pesar de que alguno se haya colado mientras estuvo en funcionamiento.

Esta es la teoría. La práctica dice que en algunas ocasiones los virus y otro malware tienen tal potencia de penetración que consiguen saltarse el congelador y quedarse residiendo en el equipo. Ocurre en pocas ocasiones y con mucho tiempo de uso, pero hay que pensar en esa posibilidad, por ese motivo son recomendables los «congeladores» que admiten actualizaciones de los programas antivirus o descongelarlos periódicamente para actualizar.

saber más

Dispositivos dañados

Según los estudios, los dispositivos y soportes que más se dañan, comprometiendo la integridad de la información, son:

- **CD y DVD,** que se rompen o se rayan.
- **Unidades de memoria USB.**
- **Discos duros** que se averían por problemas mecánicos, eléctricos o electrónicos.

Entonces, las actualizaciones del sistema operativo y el antivirus, ¿se pierden tras el apagado?

En algunos programas sí. Otros «dejan pasar» este tipo de actualizaciones.

¿Qué aplicaciones ofrecen este servicio?

La mayoría de las aplicaciones de este tipo son comerciales, aunque algunas ofrecen una prueba completa y gratuita durante un número de días. A continuación señalamos algunas de ellas.

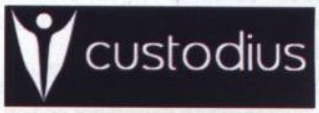
- **Deep Freeze.** Es la herramienta *freezer* más conocida y utilizada. Puede descargarse en español desde **www.faronics.es** una versión de prueba durante 30 días, que más tarde dejará de funcionar si no se compra la comercial. Tiene una versión a precio reducido para centros educativos: Deep Freeze STD Educación. Hay versiones para Windows (hasta W7), Mac OS y Linux.

- **Clean Slate.** Corre en sistemas Windows hasta la versión Windows 7. A pesar de congelar el equipo, permite que se realicen las actualizaciones del sistema operativo y antivirus. Dispone de una demo y se descarga desde **www.fortresgrand.com**

- **DriveShield.** Dispone de una versión de evaluación en **www.centuriontech.com,** y de otra para educación en **http://downloads.centuriontech.com/Education.** Puede correr en Mac OS y en todas las versiones de Windows hasta la 7.

- **ShadowUser.** Dispone de varias versiones, incluida una de prueba para 30 días. Las especificaciones particulares pueden leerse en **http://www.storagecraft.com/shadow_user.php**

- **Custodius.** Es un congelador de tipo hardware (tarjeta PCI) aunque tiene una de tipo software pensada sobre todo para portátiles o equipos que no disponen de *slots* PCI. Existen varias versiones adaptadas a las necesidades de los usuarios. Las características de cada una de ellas aparecen en la siguiente dirección: **http://www.custodius.com/html/productos.html**



- **Windows SteadyState.** En el momento de redactar este texto no existe aún una versión para Windows 7, pero sí para XP y Vista. Es una aplicación gratuita de Microsoft que se puede instalar si el sistema operativo es original. Puede encontrarse más información en: **http://www.microsoft.com/spain/windows/products/winfamily/sharedaccess/default.mspx**

ACTIVIDADES

20. ¿Has usado alguna vez un equipo con el disco o parte del disco congelado? ¿Dónde?

21. ¿Consideras que estos programas (o tarjetas, en su caso) son una buena medida para proteger la configuración inicial del sistema operativo y el software?

22. ¿Alguna objeción a este tipo de programas?

6. Destrucción de documentos

Cuando la información ya no sirve ni servirá en el futuro, se puede almacenar en sus soportes de forma indefinida en un lugar seguro o se puede optar por destruirla.

Debemos insistir en la importancia que tiene la seguridad de los datos, sobre todo los que son de carácter personal, especialmente protegidos por la ley.

Un disco duro puede formatearse varias veces y aún existe el riesgo de que parte de la información se pueda recuperar usando técnicas especiales, al igual que un CD, un DVD, una memoria o un pen drive rotos o deteriorados. Al borrar archivos, incluso de correo electrónico o de la papelera, o formatear un disco, solamente se elimina el índice de localización de los archivos, pero la información permanece oculta y recuperable.

Antes de decidir tirar a la basura soportes deteriorados que contenían información confidencial o deshacerse de ese material, es aconsejable:

- **Destrucción física del soporte.** Existen empresas especializadas en recogida y reciclaje de este tipo de materiales informáticos, que garantizan mediante un certificado la destrucción de los mismos y la confidencialidad de los datos que contenían.

↑ Máquina diseñada y creada por la empresa norteamericana Security Engineered Machinery para destrucción completa de discos duros. Ver vídeo en: http://www.semshred.com/contentmgr/showdetails.php/id/1277

- **Reescritura de los soportes o formateo seguro** mediante el empleo de un software diseñado para ese propósito. Hay muchas aplicaciones creadas con esa finalidad, que utilizan algoritmos de borrado seguro, como GOST, HMG, Ondata, Gutmann o DoD: **East-Tec DisposeSecure, Eraser, Clean Disk Security, DataStorageEraser o Comodo System Cleaner.**

Los documentos en papel que se desechan, también deben destruirse de forma segura, contratando servicios especializados o utilizando destructoras de documentos en papel.

saber más

Recuperar datos borrados o dañados

Cuando se han perdido los datos por accidente, malware o cualquier otro motivo, puede intentarse su recuperación con software específico, sea cual sea el sistema operativo. Ejemplos de estos programas:

- Stellar Phoenix.
- Recover My Files.
- Pandora Recovery.
- Data Doctor Recovery *(pen drives)*.
- Undelete Plus.
- Drive Rescue.

saber más

Lectura de discos formateados

Un estudio realizado por estudiantes de la universidad de Granada en 2009 confirmó otros estudios publicados por varias universidades del mundo.

De 100 discos duros desechados por inservibles o revendidos en tiendas de segunda mano previamente formateados, de 25 de ellos pudieron extraer información, alguna extremadamente confidencial como datos bancarios y médicos, con identificación de clientes y pacientes: diagnósticos, tratamientos o números de tarjetas de crédito.

ACTIVIDADES

23. Busca empresas que reciclen material informático y que entreguen certificado de garantía de confidencialidad de los datos. Haz un pequeño resumen del trabajo que realizan y las garantías que ofrecen.

24. Busca algún vídeo demostrativo de la destrucción de material informático, como CD, DVD o discos duros como el de las imágenes superiores, de www.semshred.com. Indica si el reciclaje se puede hacer también como medida ecológica y explica brevemente las razones.

PRÁCTICA PROFESIONAL

Medidas activas y pasivas de seguridad del software

OBJETIVOS

- Identificar las herramientas y medidas activas y pasivas de seguridad del software.
- Informarse sobre las suites de seguridad más valoradas en el momento presente.
- Decidir, basándose en la propia experiencia, qué suite de seguridad se adapta mejor a las características particulares de una persona, familia o empresa.

INSTRUCCIONES

Primera parte. Seguridad del software activa y pasiva

A continuación hay una lista de medidas, herramientas o estrategias de seguridad para el software y la información. Junto a cada una de ellas indica con una P si es seguridad pasiva y con una A si es seguridad activa:

Medida	A/P	Medida	A/P	Medida	A/P
Instalar parches		Contraseñas		Auditorías	
Control de cuentas de usuario		Antivirus en modo desinfección		Restaurar sistema	
Windows Defender		Software de detección de intentos no autorizados de acceso		Antivirus en modo prevención	
Firewall de Windows		Visor de registros de eventos		Escaneo de puertos	

Segunda parte. Análisis de la realidad antivirus en el momento actual

En algunos sitios de internet se hacen comparativas de suites antivirus comerciales y gratuitos, en donde titulares y usuarios valoran mediante una puntuación una serie de factores, como el nivel de protección, actualizaciones, precio o consumo de recursos del programa. Prácticamente nadie está de acuerdo en cuál es el mejor antivirus, entre otras cosas porque cada situación particular requiere una solución diferente.

Busca en internet alguna página web con comparativas actualizadas de suites antivirus y realiza las siguientes actividades:

- ¿Qué cinco antivirus tienen mejor puntuación en la página que has consultado?
- ¿Qué características de cada uno de ellos se han analizado para hacer la comparativa?
- ¿Se trata de aplicaciones gratuitas, comerciales o de ambas?

Tercera parte. Compara y decide

	AV1	AV2
Facilidad de uso		
Limitaciones versión gratuita		
Consumo de recursos		
Actualizaciones		
Complementos (correo electrónico, firewall, etc.)		
Puntuación media		

- Haz una pequeña tabla comparativa de antivirus, parecida a la que mostramos.
- Instala un antivirus gratuito de los más recomendados en el sitio que consultaste o en algún otro. Recuerda que existen antivirus falsos, por lo tanto cuida que el sitio de donde lo descargues sea de confianza y que el antivirus tenga un nombre conocido.
- Prueba el antivirus y dale una puntuación de 0 a 10 en cada uno de los ítems de la tabla.
- Desinstala el antivirus e instala otro también gratuito y de confianza.
- Pruébalo y puntúalo según esos criterios.
- Puntúa en promedio las características estudiadas de cada antivirus.

MUNDO LABORAL

OSI, la oficina de seguridad del internauta

La **O**ficina de **S**eguridad del **I**nternauta (OSI) es un **servicio del Gobierno** para proporcionar la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden afectarnos al navegar por internet.

OSI es un servicio de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información puesto en marcha por el **Instituto Nacional de las Tecnologías de la Comunicación** (INTECO).

Nuestro objetivo es elevar la cultura de seguridad, prevenir, concienciar y formar proporcionando información clara y concisa acerca de la tecnología y el estado de la seguridad en internet. Al mismo tiempo impulsamos la detección y denuncia de nuevas amenazas en la red, de fraudes, estafas on line o de cualquier otro tipo de ataque de seguridad informática.

En este portal encontrarás **información general** sobre la seguridad en internet, **recomendaciones, guías y herramientas** con las que navegar más seguro.

Además, ponemos a tu disposición una sección de ayuda donde encontrarás soporte a tus problemas o dudas de seguridad. Puedes acceder a esta ayuda a través de los siguientes medios:

- Nuestro **Centro de Atención Telefónica,** en el 901 111 121, presta atención personalizada a la resolución de tus consultas y problemas de seguridad.
- Los **foros de Seguridad** de la OSI, atendidos por nuestros expertos y donde también participa la comunidad internauta.
- Nuestro **Asistente de Seguridad,** que te guiará para la resolución del problema y te permite contactar con nuestros técnicos.
- Guías específicas para resolución de problemas de seguridad.

Recuerda que nuestro equipo de expertos y técnicos especialistas está a tu disposición para ayudarte a resolver tus dudas y problemas de seguridad.

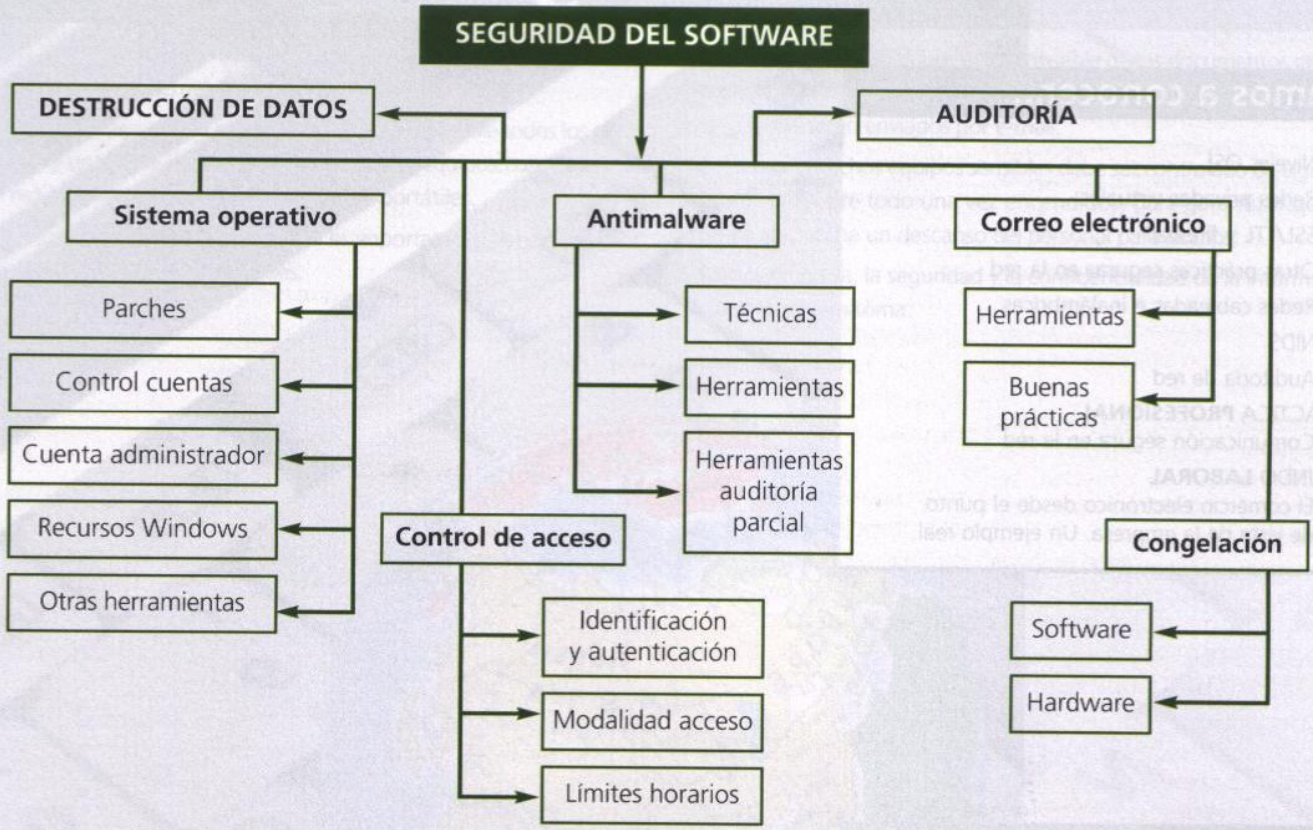
http://www.osi.es/econf/Quienes_Somos/

Actividades

1. Antes de leer esta presentación, ¿conocías este servicio del Gobierno?
2. ¿Cuál es el principal objetivo de la OSI?
3. ¿Qué vías de asesoramiento y ayuda propone?
4. Visita el sitio web de la OSI (www.osi.es) y haz una relación de las cinco secciones y temas que consideres de más interés para el desempeño de tu profesión, agregando una corta explicación al porqué de tu interés y la probabilidad (alta, media o baja) de que en un futuro necesites consultar cada una de ellas.

Nombre de sección o tema	Qué tiene de especial interés para tu futuro profesional	Probabilidad de consultar la sección o el tema en el futuro

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **Una o más de las siguientes afirmaciones sobre la auditoría son ciertas. Indícalas:**
   a) Puede ser parcial.
   b) Puede señalar vulnerabilidades del sistema.
   c) Puede detectar ataques producidos.
   d) Se puede hacer en cualquier momento.
   e) Se puede realizar con herramientas del sistema operativo.
   f) Se puede llevar a cabo con software específico.
   g) Puede hacerla el personal de la empresa.
   h) Pueden efectuarla empresas especializadas.

2. **¿Puede configurarse el correo electrónico para que el antivirus instalado en el equipo controle el correo entrante y el saliente?**
   a) Sí.
   b) No.

3. **Señala una de las siguientes opciones sobre el control de acceso al software:**
   a) Protege el sistema operativo.
   b) Protege las aplicaciones.
   c) Protege los datos.
   d) Las tres afirmaciones anteriores son ciertas.

4. **Las buenas prácticas en el envío y recepción de correo electrónico son un tipo de seguridad:**
   a) Activa.
   b) Pasiva.
   c) Ninguna de las dos.
   d) Ambas.

Soluciones: 1a, 1b, 1c, 1d, 1e, 1f, 1g, 1h, 2a, 3d, 4a

7 Redes seguras

vamos a conocer...

1. Niveles OSI
2. Redes privadas virtuales
3. SSL/TTL y firewall
4. Otras prácticas seguras en la red
5. Redes cableadas e inalámbricas
6. NIDS
7. Auditoría de red

PRÁCTICA **PROFESIONAL**
Comunicación segura en la red

MUNDO **LABORAL**
El comercio electrónico desde el punto de vista de la empresa. Un ejemplo real

y al finalizar esta unidad...

- Habrás alcanzado conocimientos suficientes para controlar la red, poner atención frente a posibles ataques y saber distinguirlos.
- Comprenderás que la red es un medio cambiante, por lo que siempre habrá que mantenerse al día.
- Podrás mantener redes seguras, las contraseñas serán eficientes y los envíos de datos a través de la red no podrán ser interceptados porque viajarán adecuadamente protegidos.
- Sea cual sea el tipo de red que uses, el firewall estará correctamente configurado junto a las listas de acceso, de modo que ningún intruso dañará los equipos, y podrás comprobar que los archivos descargados no contienen software malicioso mediante comprobaciones con funciones *hash*.
- Estarás en condiciones de impedir, en la medida de lo posible, la interceptación de información por parte de intrusos o de malware.

CASO **PRÁCTICO** INICIAL

situación de partida

La empresa que contrata tus servicios está permanentemente conectada a internet.

Además, hay una red interna que conecta con cable todos los equipos y una señal inalámbrica para algunos equipos con tarjeta de red inalámbrica y para los dispositivos portátiles.

La información que se almacena es importante, y tiene que viajar de forma segura por las redes.

El personal directivo debe ser responsable de los documentos que redacta y envía a otras empresas y organismos públicos. Además, la mayoría serán enviados por e-mail.

El acceso a muchos equipos sensibles debe ser controlado de alguna forma, sobre todo una vez encendidos, para garantizar que nadie aproveche un descanso del personal para usarlos.

Para la empresa, la seguridad y la confidencialidad de la información son una máxima.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Mensualmente se emiten numerosos documentos, generalmente para organismos públicos, pero también en la relación con clientes y proveedores.
   - ¿Es posible firmar digitalmente un documento?
   - ¿Cómo conseguir que los documentos que viajan por internet lo hagan de manera segura?
2. Como explica la empresa, su máxima es la seguridad y la confidencialidad de la información. Puertas abiertas a intrusos acabarían, como mínimo, con la confidencialidad.
   - ¿Cómo se podrían controlar los accesos no autorizados a la red?
   - ¿Se debe establecer una longitud mínima de contraseña?
3. La empresa recibe multitud de documentación, como pedidos, comunicaciones de pago y otros documentos administrativos y contables.
   - ¿Cómo se puede verificar que los documentos que se reciben no han sido alterados durante el camino hasta los dispositivos de destino?
4. La empresa tiene la red mixta, en parte cableada y en parte inalámbrica.
   - ¿Es más segura la red inalámbrica o por cable?
5. Es posible que si se coloca algún tipo de software que inspeccione la red en busca de intrusos, se colapse el tráfico por la misma.
   - ¿Puedo disponer de algún software que trabaje «en la sombra» buscando ataques al sistema?

1. Niveles OSI

1.1. Descripción

El modelo OSI (*Open System Interconnection*) es un modelo conceptual que define los niveles o capas hardware y software de las redes de comunicaciones de datos por donde circula la información. No existen métodos ni protocolos establecidos para todo el modelo OSI, debido, sobre todo, a las diferentes topologías de red que existen y a los sistemas con los que están implementadas, pero cada capa tiene sus propios protocolos.

recuerda

Glosario de términos

DNS. *Domain Name System.* Sistema de nombre de dominio.

Firewall. Cortafuegos, controla la entrada de información no permitida. Puede ser físico o lógico.

IP. *Internet Protocol.* Protocolo de internet que identifica de manera única, lógica y jerárquica cada dispositivo que pertenezca a una red bajo protocolo IP.

Protocolo. Puede ser software o hardware y determina o controla la forma en que se conectan, se comunican o transfieren datos dos puntos A y B.

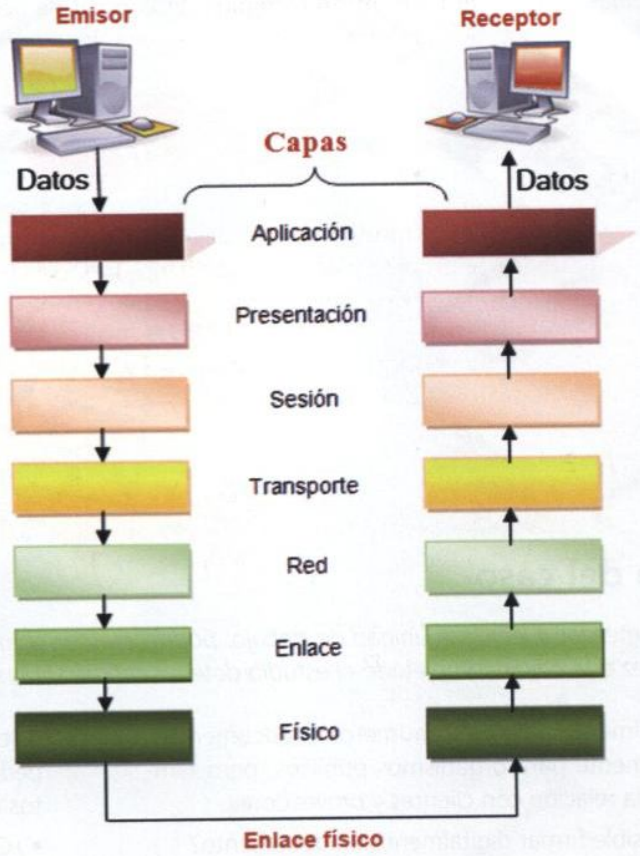
Proxy. Punto intermedio entre un ordenador conectado a internet y el servidor que está accediendo. Se puede utilizar un proxy para suplantar la propia IP por otra.

Puerto físico. Las conexiones directas o indirectas que tiene la placa base. Por ejemplo, un puerto USB o un puerto paralelo para impresoras.

Puerto lógico. Interfaz de comunicación de un programa con el exterior, a través de una red. Hay un total de 65.535 puertos lógicos, algunos definibles para cada aplicación y otros reservados para el sistema operativo.

TCP. Protocolo de control de transmisión. Está orientado a conexión y se utiliza en el nivel 4 de OSI.

UDP. User Datagram Protocol. Protocolo utilizado en el nivel 4 de OSI y que no está orientado a conexión.



↑ **Niveles OSI.** Cada una de las **capas** por las que transcurre la **información** desde el emisor hasta el receptor. Como puede verse, la información atraviesa las mismas capas de manera inversa desde el punto de vista del emisor y del receptor.

Cada uno de estos niveles tiene una serie de vulnerabilidades y se le pueden aplicar unas medidas de protección para evitar la materialización de amenazas. Las vulnerabilidades y sistemas de seguridad sobre los que profundizaremos en esta unidad abarcan desde el nivel 1 al nivel 5, los más ligados al concepto de red.

1.2. Funciones y vulnerabilidades de los niveles OSI

Nivel 1. Físico

La capa física define los componentes mecánicos, eléctricos, de procedimiento y funcionales para activar, mantener y desactivar la conexión física entre los distintos dispositivos que componen las redes, tales como concentradores, repetidores o cables.

La seguridad en torno a este nivel consiste en garantizar que el cableado y los dispositivos mencionados contengan medidas de protección para impedir la pérdida fortuita o fraudulenta de información.

Hay varias medidas y herramientas para proteger el nivel físico, como por ejemplo los sistemas de alimentación ininterrumpida, el control de acceso físico de personas y la protección del hardware frente a robo, pérdida o destrucción.

recuerda

Direcciones MAC (*Media Access Control*)

Control de acceso al medio. La dirección MAC es un identificador de tarjetas de red que consiste en 48 bits que identifican de forma única a la tarjeta en todo el mundo.

Nivel 2. Enlace

Esta capa hace referencia a la transferencia (enlace) de datos de un nodo a otro de la red. Es aquí donde se preparan los datos mediante unas señales de inicio y final de cada paquete, para después transmitirlos a través del nivel 1 (físico).

En la capa de enlace se encuentran las direcciones MAC, las definiciones de las VLAN, así como los protocolos para las redes WAN. El papel de los *switches* es importante en este nivel OSI.

Una de las principales vulnerabilidades del nivel 2 es la propia vulnerabilidad de las direcciones MAC, fáciles de falsificar. Otra es la localización de redes inalámbricas mediantes distintos sistemas como el *wardriving*.

Algunas medidas de seguridad que pueden aplicarse sobre este nivel son el filtrado de direcciones MAC, aunque signifiquen una protección débil, y el cifrado de claves en conexiones inalámbricas.

recuerda

WAN (*Wide Area Network*)

Red de amplio alcance en donde no todo está en el mismo local o edificios adyacentes, sino que cubre distancias de hasta miles de kilómetros, como las que podría tener una entidad bancaria para abarcar las sucursales de un país.

Nivel 3. Red

Es la capa que define el diseño de la red lógica. La función de la capa de red es hacer que la información que envía el emisor llegue al receptor. El principal dispositivo de esta capa es el enrutador, que solemos llamar *router*.

Esta capa trabaja con el protocolo de red IP y es propensa a múltiples vulnerabilidades, como puede ser la suplantación de IP que utilizan los hackers, modificando la cabecera de los paquetes de información de modo que parezca que provienen de una IP de confianza. Uno de los ataques más frecuentes que aprovecha la vulnerabilidad de este nivel OSI es la DoS (ataques de denegación de servicio) o DDoS (ataques de denegación de servicio organizados desde distintos orígenes), que generan un tráfico excesivo, fraudulento y premeditado mediante técnicas de *flooding* o *spoofing*.

saber más

Flooding

Saturación de un canal, normalmente de chat, mediante el envío repetitivo y abusivo de mensajes.

saber más

Spoofing

Suplantación de la personalidad mediante modificación de IP, nombre de dominio u otras técnicas.

Medidas elementales de seguridad sobre el nivel de red:

- Limitación de accesos por IP, es decir, impedir entradas continuas por parte de la misma IP al sistema, como puede ser al servicio SMPT del correo electrónico.
- Utilizar filtros de correo.
- Sistemas de detección de intrusos (IDS).
- Utilización de firewalls.

Nivel 4. Transporte

Este nivel se ocupa de que esa información que se envía en el nivel de red, llegue a su destino libre de errores. Soporta los protocolos UDP (no destinado a conexión) y TCP (orientado a conexión). Uno de los puntos más vulnerables de este nivel son los puertos lógicos.

Para controlar la seguridad en el nivel de transporte pueden hacerse controles de puertos abiertos (por ejemplo, con ***netstat***) y del tráfico que se genera a través de ellos.

Nivel 5. Sesión

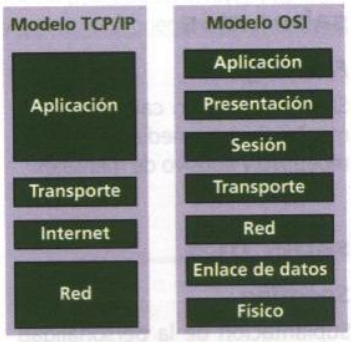
Esta capa se encarga de la relación entre los usuarios y la red, gestionándola y sincronizándola. Es un punto vulnerable a la acción de los *sniffers*, pero puede utilizarse el firewall como medida de seguridad.

Nivel 6. Presentación

Es el nivel que trata el contenido de la información, que puede estar constituida por datos, imágenes, sonido, etc. Los datos llegan mediante una u otra codificación, dependiendo del sistema que los trate, y este nivel los traduce para que el usuario pueda verlos y comprenderlos.

Nivel 7. Aplicación

Permite a las aplicaciones acceder a los servicios que ofrecen las demás capas. Cada aplicación tiene sus propios protocolos, con lo que sería imposible enumerarlos todos, pero hay unos protocolos claros para este nivel OSI, como son los POP y SMTP para correo electrónico, o el FTP como servicio de ficheros.



↑ Correspondencia de las capas entre los modelos TCP/IP y OSI.

1.3. Equivalencia entre el modelo OSI y el TCP/IP

Al hablar de seguridad en la red podemos utilizar la nomenclatura del modelo OSI o del TCP/IP. Para evitar confusiones, en esta unidad hablaremos de sistemas de seguridad sin hacer referencia a modelos, sino a vulnerabilidades y situaciones concretas que, obviamente, suceden al margen del nombre del modelo.

2. Redes privadas virtuales

Las Redes Privadas Virtuales son conocidas a menudo como conexiones **VPN** *(Virtual Private Network)*. **A través de una red VPN los datos viajan cifrados** y solamente podrán ser descifrados por el destinatario y, por supuesto, por el emisor, por lo cual todo el proceso resulta transparente para ambas partes. De este modo no quedan expuestos a la captación fraudulenta en su camino por la red.

La tecnología VPN permite la conexión a una red local desde una localización remota, a través de otro tipo de red, como por ejemplo internet.

Una aplicación de ejemplo es la que se da en muchas instituciones, donde solo son accesibles algunos recursos desde equipos que se encuentran en su propia red local por motivos de seguridad. Para permitir el acceso desde fuera deberá crearse una conexión mediante VPN, lo que «registrará» a nuestro equipo como perteneciente a la red local y permitirá su acceso.

Para que todo el **tráfico** VPN pueda considerarse **seguro,** es necesario que se garanticen cuatro principios básicos.

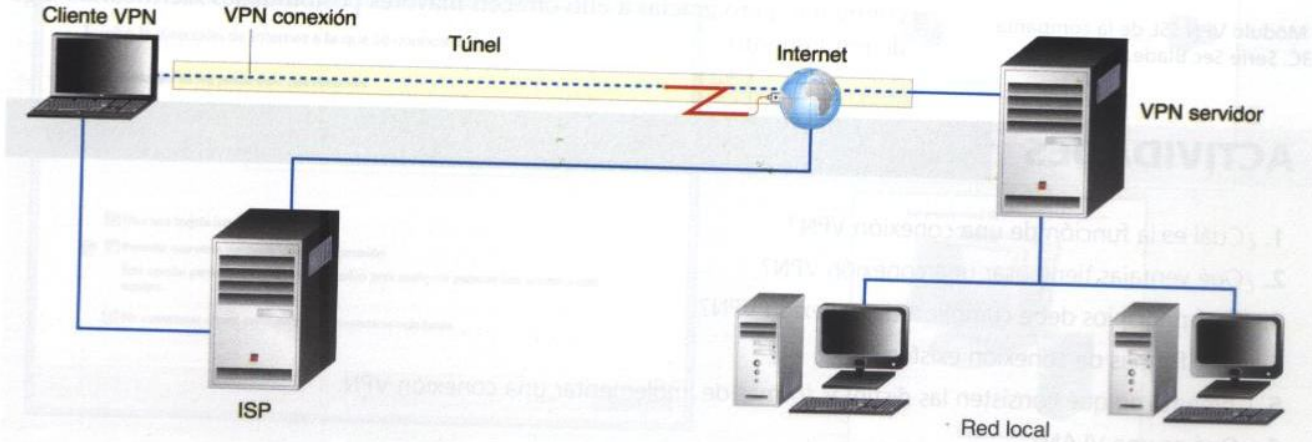
- **Autentificación y autorización.** Debe conocerse en todo momento qué persona realiza las operaciones, para que tenga las mismas garantías que si las realizara personalmente en la empresa.
- **No repudio.** Debe poder garantizarse que las tareas que se efectúen han sido realizadas, efectivamente, por la persona que se ha autenticado para que, de esta forma, no exista posibilidad de repudio.
- **Integridad.** Los datos enviados y recibidos no pueden ser modificados durante el trayecto, ya sea por terceras personas o por fallos en la red. Para ello se incluyen herramientas de *hash* (se estudiará más adelante).
- **Confidencialidad.** Los datos enviados y recibidos deben ser encriptados para que en su trayecto a través de internet no sean interceptados, y en caso de serlo, no resulten entendibles.

recuerda

Hablar de un proceso «transparente» significa que pasa inadvertido.

caso práctico inicial

Las VPN son uno de los sistemas más usados en instituciones para garantizar la seguridad de documentos sensibles y facilitar el acceso remoto a documentos.



↑ Comunicación de una red local VPN mediante túnel.

2.1. Formas de conexión en una red VPN

Dentro las conexiones VPN, se puede decir que existen tres formas de conexión distintas:

- ***Tunneling.*** Se intenta transmitir el concepto de un túnel a través de internet. Si pensamos en internet como un medio **inseguro** por definición, y carecemos de sistemas que encripten la comunicación, podemos crear a través de internet un paso seguro o túnel por el cual enviemos información insegura. La información, en caso de ser interceptada, podría ser interpretada, pero esto no es posible ya que para la transferencia se usa un protocolo seguro, como por ejemplo **SSH.**

  Para usar este tipo de técnica se necesita una **cuenta segura** en la máquina con la que queremos transmitir los datos.

- **VPN de acceso remoto.** Se trata de acceder a los recursos disponibles desde **ubicaciones remotas,** utilizando internet como plataforma de acceso. Realizada la conexión y autenticado el usuario, puede acceder a los **mismos recursos** que si estuviera presente en la red local de los sistemas a los que accede.

- **VPN punto a punto.** Similar al funcionamiento del *tunneling*, se trata de crear un túnel sobre internet para la transmisión de datos, pero en lugar de aceptar la conexión de un equipo, el servidor VPN conectado permanentemente a internet acepta la conexión de diversos servidores y sitios, estableciendo el túnel.

Existe un cuarto tipo de conexión VPN, la denominada **VPN interna** o **VLAN.** Con esta conexión, equivalente a la de acceso remoto solo que funcionando sobre la propia red local en lugar de internet, se consigue **aislar,** para mayor seguridad, determinadas zonas de la red, como **servidores sensibles** o redes inalámbricas.

saber más

SSH (*Secure Shell*)

Es el nombre de un protocolo y de su programa asociado, que sirve para acceder a otras máquinas de forma segura mediante un sistema de cifrado de datos.

saber más

Diferencias entre VPN y VLAN

VPN (*Virtual Private Network*).

VLAN (*Virtual Local Area Net-work*).

Hay quien confunde ambos conceptos. La VLAN es una división virtual de una red local en varias más pequeñas, pero sin salirse del entorno físico de la LAN. La VPN en cambio es una extensión de horizontes de la LAN, pudiendo pertenecer a una LAN un nodo remoto, por ejemplo, en otra ciudad o en otro país.

2.2. Implementación de VPN

Para implementar lo estudiado hasta ahora, existen soluciones tanto de hardware como de software.

- **Hardware.** Más fácil de configurar y proporciona un mejor rendimiento de la red.
- **Software.** Las implementaciones mediante software son algo más complejas de configurar, pero gracias a ello ofrecen mayores posibilidades sacrificando algo de rendimiento.

↑ Módulo VPN SSL de la compañía H3C. Serie Sec Blade.

ACTIVIDADES

1. ¿Cuál es la función de una conexión VPN?
2. ¿Qué ventajas tiene usar una conexión VPN?
3. ¿Qué principios debe cumplir toda conexión VPN?
4. ¿Qué formas de conexión existen?
5. Comenta en qué consisten las distintas formas de implementar una conexión VPN.
6. ¿Qué es una VLAN?

EJEMPLO

Conectarse a una red privada virtual

Desde nuestro ordenador podemos formar parte de una red privada virtual VPN, aunque estemos distantes de ella, como podría ser nuestro lugar de trabajo. En los siguientes ejemplos veremos cómo podemos hacerlo con Mac OSX y con Windows 7.

MAC OSX

Si deseamos conectarnos a una VPN, en primer lugar hay que configurar adecuadamente la conexión a internet. En estos ajustes hay que **incluir la dirección del servidor VPN**, el **nombre de cuenta** y los **datos de autenticación,** tales como la contraseña o el certificado que se haya recibido del administrador de la red.

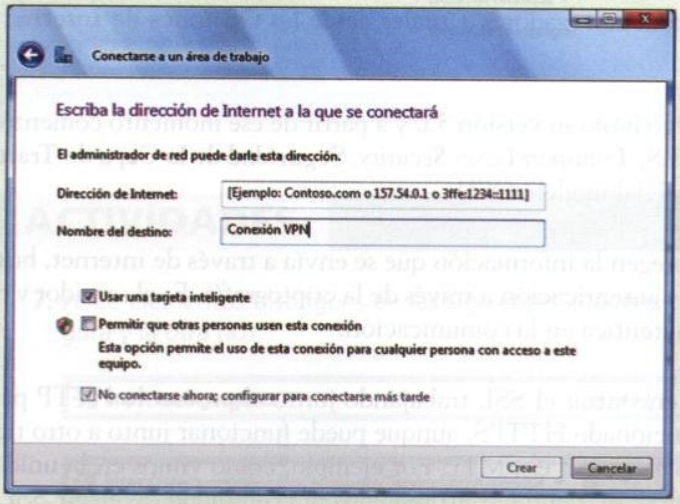
Es posible que esos datos se hayan recibido ya mediante un archivo de configuración. En ese caso solamente hay que **importar el archivo** para realizar los ajustes.

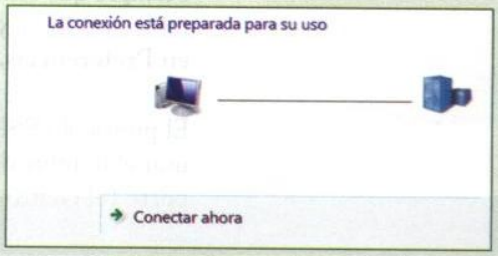
Para configurar manualmente una conexión VPN:

- Entra desde **Apple** → **Preferencias del Sistema** y haz clic en **Red.**
- Haz clic en Añadir (+) en la parte inferior de la lista de servicios de conexión a redes y selecciona **VPN** en el menú local **Interfaz.**
- Selecciona el **tipo de conexión VPN** que desees configurar en el menú local «Tipo de VPN», en función de la red a la que vayas a conectarte. Asigna un **nombre** a ese servicio VPN.
- Introduce la **dirección del servidor** y el **nombre de cuenta** para la conexión VPN.
- Haz clic en **Ajustes de autenticación** e introduce la información de autenticación de usuario suministrada por el administrador de red.
- Una vez introducida la información de autenticación del usuario, haz clic en **OK** y después clic en **Conectar.**

WINDOWS 7 (se realiza de igual forma con **Windows Vista**)

En el Centro de redes y recursos compartidos se abre una ventana para crear la conexión VPN. Se completa con los datos que hayamos obtenido del administrador de la red VPN, se hace clic en Crear y ya estará lista la conexión VPN para ser usada. Desde ese momento podremos trabajar con nuestro equipo en una red remota con seguridad. En las conexiones de red aparecerá la VPN creada.





3. SSL/TTL y firewall

Desde sus primeros momentos, internet ha sido un medio básicamente inseguro. Por ello, las comunicaciones se establecieron sin ningún tipo de cifrado, que es como aún hoy día permanecen la mayoría de ellas, sobre todo en el ámbito personal.

saber más

Debido al aumento de ataques en la red, cada vez es más frecuente encontrar páginas que aumentan su seguridad usando cifrado de datos.

Esto provoca que cualquier usuario sin buenas intenciones pueda interceptar lo que estamos comunicando, desde datos de poca o mediana importancia hasta otros cuya pérdida o difusión pueden acarrearnos serios problemas, como pueden ser los datos personales de terceros cuya obligación de proteger está regulada por la ley.

Es por esto que surgen diferentes soluciones para distintos tipos de ataques que podemos sufrir al enviar y recibir información por la red. La propia navegación deja rastros de nuestra presencia en la red, el correo electrónico puede ser interceptado, la navegación por sitios inseguros puede infectar de malware nuestro equipo, la cumplimentación de formularios con datos privados en formularios de páginas web inseguras puede ser utilizada con fines ilícitos o ser interceptada por terceros, etcétera.

3.1. Conexión segura SSL/TTL

saber más

HTTPS (*H*ypertext *T*ransfer *P*rotocol *S*ecure).

Se diferencia del protocolo HTTP en que utiliza SSL y un puerto de comunicación distinto.

El protocolo que habitualmente se utiliza para el cifrado en internet se llama **SSL** *(Secure Sockets Layer)* o **Protocolo de Capa de Conexión Segura.**

El protocolo **HTTPS** utiliza el cifrado basado en **SSL/TTL.** Una buena forma para saber si los datos que introducimos en una web viajan de forma segura, es observar en la barra de direcciones de nuestro navegador si aparece **https://** lo que indicaría que es una web segura, o en su lugar aparece **http://** que significa que no cuenta con cifrado **SSL.**

Siempre que sea posible trabajaremos con cifrados, lo que es fácilmente configurable con la mayoría de navegadores actuales desde las **Opciones de Internet** o en **Preferencias.**

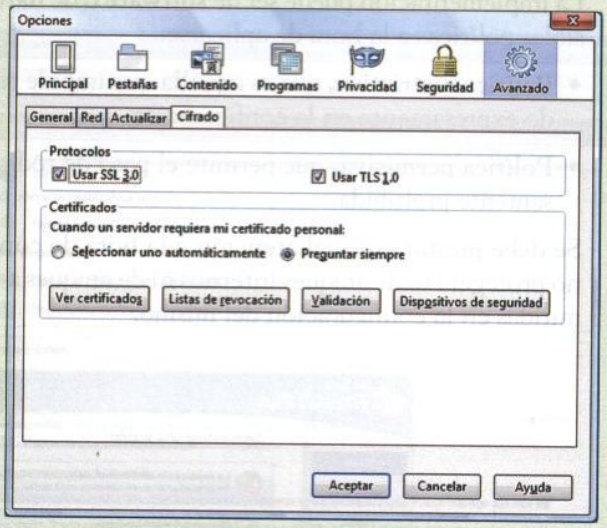
El protocolo SSL llegó hasta su versión 3.0 y a partir de ese momento comenzó a usar el nombre de **TLS,** *Transport Layer Security*, **Seguridad de la Capa de Transporte** (el cuarto nivel del modelo OSI).

Estos protocolos protegen la información que se envía a través de internet, brindándole privacidad y autenticación a través de la criptografía. Es el servidor y no el cliente quien se autentica en la comunicación.

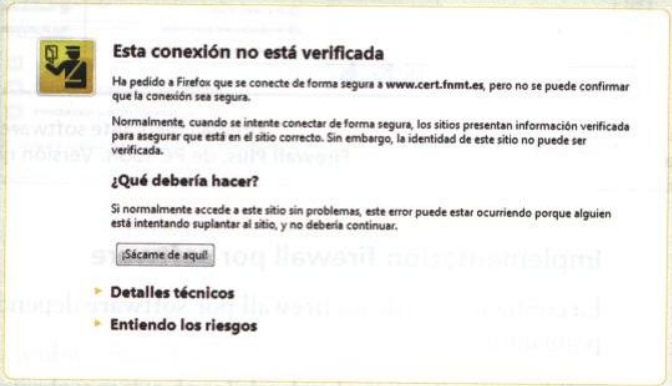
Lo más habitual es encontrar el SSL trabajando junto al protocolo HTTP para conformar el ya mencionado HTTPS, aunque puede funcionar junto a otro tipo de protocolos como el TCP o el SMTP. Por ejemplo, como vimos en la unidad anterior, en Outlook o en Thunderbird tenemos la posibilidad de elegir SSL y TTL para el correo electrónico.

EJEMPLO

Si estamos navegando por la red y deseamos entrar solamente en páginas seguras, tendríamos que configurar nuestro navegador. En la imagen siguiente, usamos esta configuración en el navegador Mozilla Firefox en su versión 3.5.7. En la ventana de **Herramientas → Opciones → Avanzado,** pestaña **Cifrado,** deberemos comprobar que tenemos activadas las casillas de Cifrado SSL 3 y TLS 1, o al menos una de ellas.

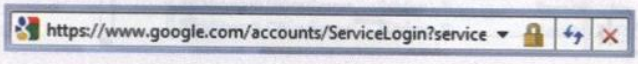


Si después de haberlo configurado de este modo, pretendemos entrar en una página que no aplica protocolos de seguridad, recibiremos un aviso del navegador y podremos decidir si abandonarla o asumir los riesgos y entrar en ella.



ACTIVIDADES

7. ¿Qué elementos distingues en las siguientes imágenes, además de la «s», que indiquen que una web es segura y la otra no?



3.2. Firewall o cortafuegos

saber más

La mayoría de sistemas operativos modernos incluyen un firewall por defecto, aunque su configuración suele ser permisiva.

Un firewall es un dispositivo, o conjunto de ellos, que está configurado para impedir el acceso no autorizado a una determinada zona de una red o dispositivo, pero que al mismo tiempo permite el paso a aquellas comunicaciones autorizadas.

La implementación puede ser de **software** o de **hardware,** y ambas tienen dos posibles políticas a la hora de aplicarse:

- **Política restrictiva,** que es aquella que impide todo el tráfico salvo el autorizado expresamente en la configuración.
- **Política permisiva,** que permite el paso de toda comunicación salvo la expresamente prohibida.

Se debe prestar especial atención a la hora de configurar un firewall ya que este no protegerá ni de ataques internos ni de ataques a través de comunicaciones permitidas en la configuración del mismo.

↑ Firewall mediante hardware. Router + Firewall de la compañía D-Link

↑ Firewall mediante software. **Firewall Plus,** de PC Tools. Versión gratuita.

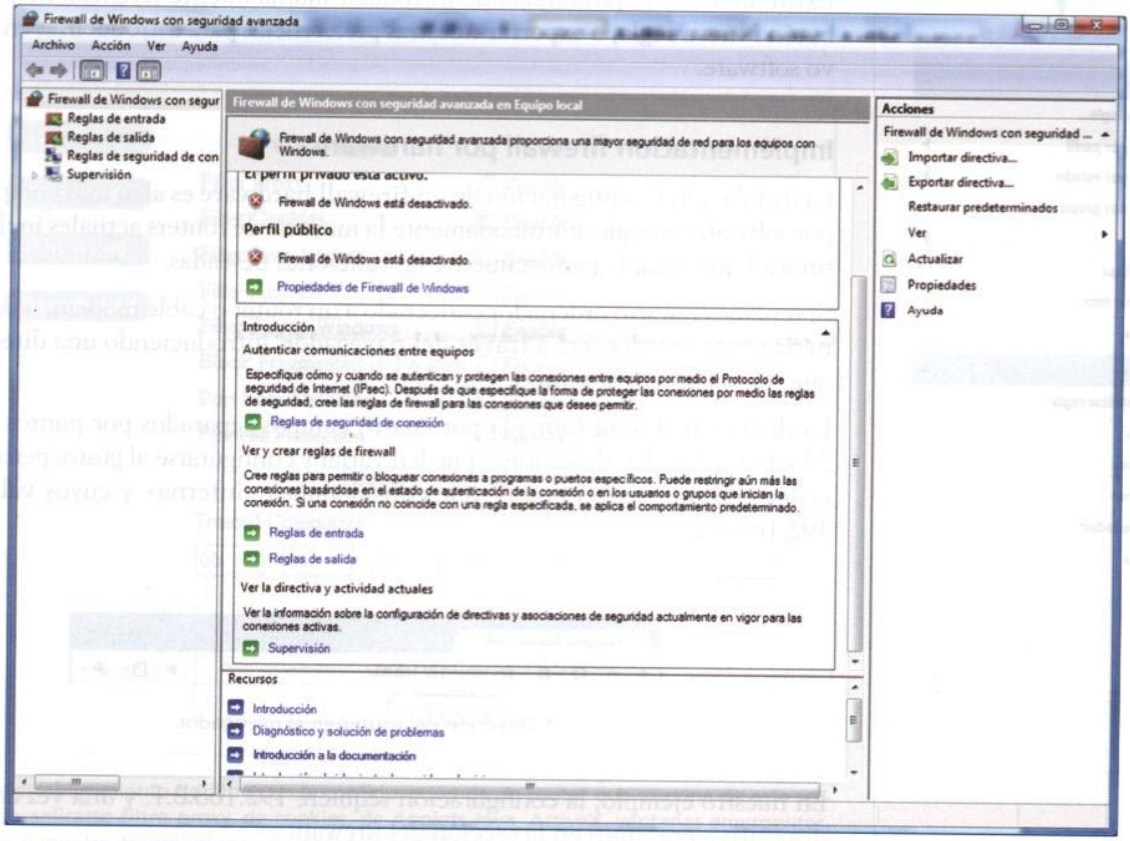
Implementación firewall por software

La configuración de un **firewall por software** dependerá del programa de que dispongamos.

↑ Petición de acceso a WinRar, que intenta controlar otra aplicación.

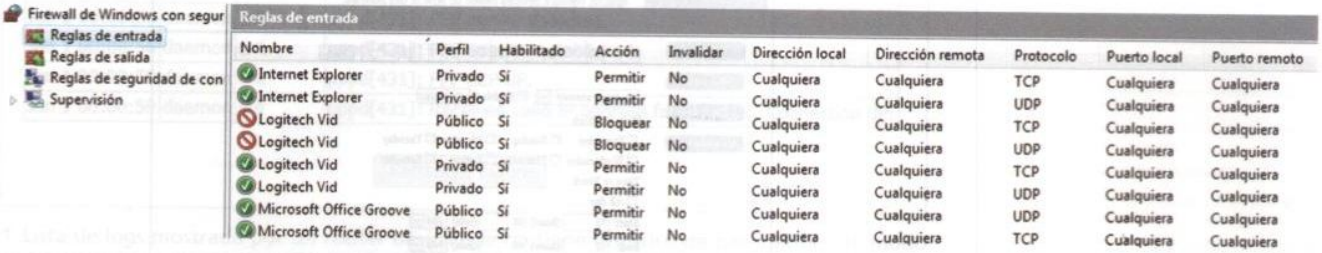
↑ Ventana de configuración de Firewall Plus.

Windows Vista y **Windows 7** cuentan, entre sus aplicaciones, con un firewall sencillo, ya presente en anteriores versiones, y con un **firewall con seguridad avanzada,** que permite configurar un amplísimo conjunto de reglas a modo de cortafuegos, tanto de entrada como de salida, además de otras importantes funciones y filtros de seguridad.



↑ Firewall de Windows con seguridad avanzada.

Aunque el funcionamiento cambie, en todos los firewalls existen elementos comunes, como las reglas de entrada y reglas de salida, donde se configura si el firewall debe o no permitir el tráfico de ciertas aplicaciones.



Nombre	Perfil	Habilitado	Acción	Invalidar	Dirección local	Dirección remota	Protocolo	Puerto local	Puerto remoto
Internet Explorer	Privado	Sí	Permitir	No	Cualquiera	Cualquiera	TCP	Cualquiera	Cualquiera
Internet Explorer	Privado	Sí	Permitir	No	Cualquiera	Cualquiera	UDP	Cualquiera	Cualquiera
Logitech Vid	Público	Sí	Bloquear	No	Cualquiera	Cualquiera	TCP	Cualquiera	Cualquiera
Logitech Vid	Público	Sí	Bloquear	No	Cualquiera	Cualquiera	UDP	Cualquiera	Cualquiera
Logitech Vid	Privado	Sí	Permitir	No	Cualquiera	Cualquiera	TCP	Cualquiera	Cualquiera
Logitech Vid	Privado	Sí	Permitir	No	Cualquiera	Cualquiera	UDP	Cualquiera	Cualquiera
Microsoft Office Groove	Público	Sí	Permitir	No	Cualquiera	Cualquiera	UDP	Cualquiera	Cualquiera
Microsoft Office Groove	Público	Sí	Permitir	No	Cualquiera	Cualquiera	TCP	Cualquiera	Cualquiera

↑ Firewall de Windows con seguridad avanzada. Reglas de entrada.

En esta imagen, el nombre **avgupd.exe** hace referencia al tráfico generado por las actualizaciones de un conocido software antivirus; si deseáramos bloquearla usaríamos la opción **eliminar** que aparece en el panel derecho de la pantalla.

Si no queremos que el cambio sea permanente, sino que nos gustaría hacerlo reversible, podemos utilizar la opción **deshabilitar regla,** que desactivará el filtrado para este programa pero no lo eliminará de la lista.

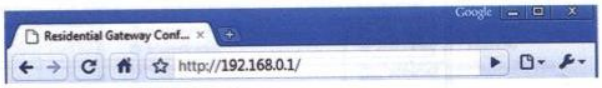
Existe también la posibilidad de introducir manualmente restricciones, desde el botón **Nueva regla,** o **exportar** nuestras preferencias para introducirlas en un nuevo software.

Implementación firewall por hardware

La instalación y configuración de un **firewall hardware** es algo más compleja que por software, aunque afortunadamente la mayoría de routers actuales incluyen un firewall que cumple perfectamente las funciones deseadas.

Si tenemos nuestro ordenador conectado a un router o cable módem, la forma genérica para acceder será **a través del navegador,** introduciendo una dirección IP que nos da acceso al mismo.

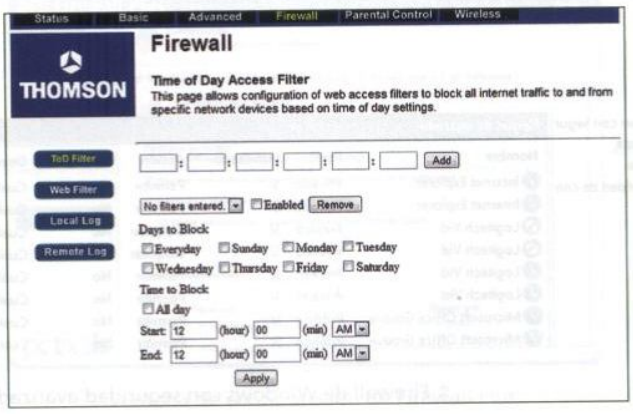
La dirección IP está formada por cuatro campos separados por puntos del tipo 255.43.67.129. Las direcciones pueden variar y configurarse al gusto, pero para acceder al router se usa una IP que consideramos «interna» y cuyos valores son 192.168.x.x.



↑ Dirección del router en el navegador.

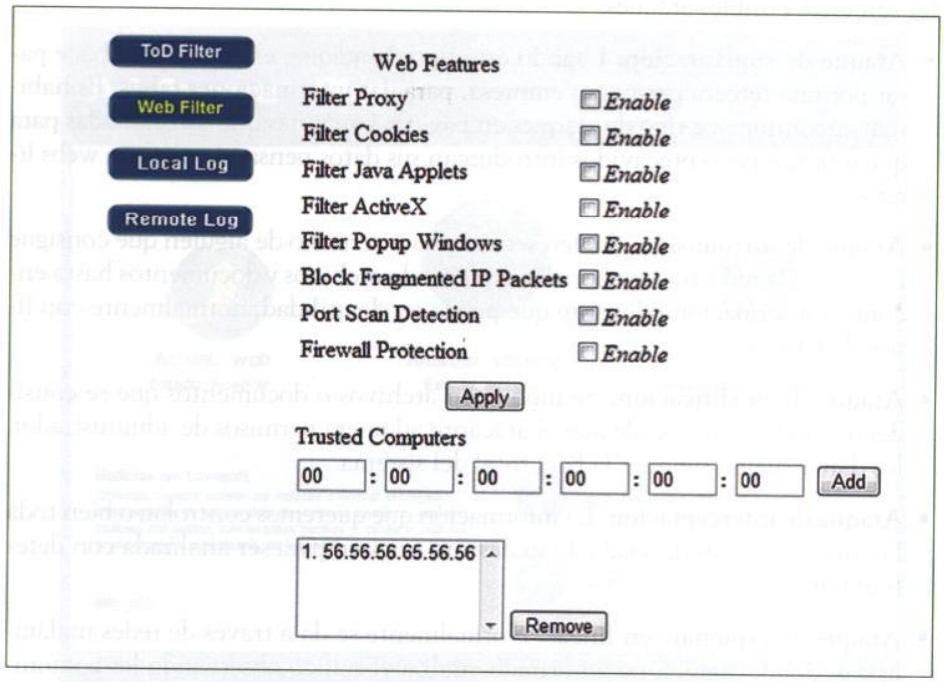
En nuestro ejemplo, la configuración requiere 192.168.0.1, y una vez dentro del dispositivo entramos en la sección del firewall.

Podemos configurarlo para que funcione durante todo el día o bien determinados días de la semana y a cierta hora. Esta aplicación es útil en empresas donde los fines de semana los equipos encendidos están desatendidos y queremos garantizar que solo se usan para la función deseada y nadie pueda acceder a ellos con otro fin.



También podemos establecer filtros para páginas web y su tráfico, sobre la opción **Web Filter,** tales como JavaScript o ActiveX, que en ocasiones resultan peligrosos, o cookies.

El firewall trabaja a nuestro servicio una vez configurado, pero en cualquier caso es necesario revisar los archivos **log** generados, donde se guarda la información de la actividad realizada, que también puede ser enviada por e-mail. Así detectaremos los ataques más frecuentes y el tráfico, para poder mejorar nuestra configuración.



↑ Panel de establecimiento de filtros en la configuración de un router que dispone de este servicio. Puede aplicarse filtro proxy, de cookies, de Applets Java, ActiveX, ventanas emergentes, bloques de paquetes fragmentados de datos, detección de escaneo de puertos y protección firewall.

System Log

Date/Time	Facility	Severity	Message
Jan 1 00:00:20	user	crit	klogd: ADSL G.992 started
Jan 1 00:00:20	user	crit	klogd: eth0 Link UP.
Jan 1 00:00:20	user	crit	klogd: ADSL G.992 channel analysis
Jan 1 00:00:23	user	crit	klogd: ADSL link up, interleaved, us=320, ds=6016
Jan 1 00:00:56	daemon	crit	pppd[431]: PPP server detected.
Jan 1 00:00:56	daemon	crit	pppd[431]: PPP session established.
Jan 1 00:00:58	daemon	crit	pppd[431]: PPP LCP UP.
Jan 1 00:00:59	daemon	crit	pppd[431]: Received valid IP address from server. Connection UP.

Refresh Close

↑ Lista de logs mostrada por un router básico que no tiene histórico de navegación, de modo que solamente está mostrando lo realizado desde que fue encendido hasta el momento en que se consulta su registro de actividades.

4. Otras prácticas seguras en la red

Para establecer la adecuada seguridad en nuestras redes deberemos seguir unas normas generales como mantener al día la configuración de nuestros **antivirus,** tanto en servidores como en equipos personales, configuraremos los **firewall** y podremos utilizar alguna técnica aprendida anteriormente, como las conexiones **VPN.**

En cualquier caso, hablar de seguridad en las redes es hacerlo de los posibles ataques que podemos sufrir y cómo defendernos. Recordamos, de forma sucinta, cuáles son estos posibles ataques:

saber más

Todos estos ataques pueden producirse en paralelo desde muy diferentes lugares, lo que complica su solución así como detectar a los causantes.

- **Ataque de suplantación.** Usando este tipo de ataque, el atacante se hace pasar por una tercera persona o empresa, para dar informaciones falsas. Es habitual encontrar este tipo de ataques en páginas bancarias que son clonadas para que usuarios poco precavidos introduzcan sus datos pensando que son webs lícitas.
- **Ataque de intromisión.** Suelen ser ataques internos o de alguien que consigue colarse en la red y navega por ella explorando archivos y documentos hasta encontrar información relevante que pueda ser de utilidad, normalmente con fines delictivos.
- **Ataque de modificación.** Se modifican archivos o documentos que se consideran válidos. En caso de que el atacante adquiera permisos de administrador, los daños suelen suponer la baja total del sistema.
- **Ataque de interceptación.** La información que queremos controlar, o bien toda la información, es desviada de su destino original para ser analizada con detenimiento.
- **Ataque de espionaje en líneas.** Normalmente se da a través de redes inalámbricas, donde alguien no autorizado analiza el tráfico observando las comunicaciones.
- **Ataque de denegación de servicio.** Se trata de impedir el correcto funcionamiento de los sistemas a los usuarios autorizados para ellos. Son muy habituales, en el caso de las redes, saturar servidores web a base de accesos simultáneos de forma que las peticiones de los usuarios no puedan ser atendidas.

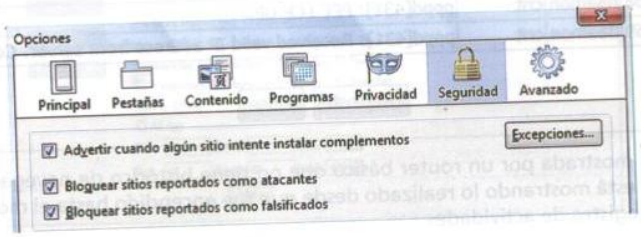
recuerda

Es habitual el uso de ordenadores «zombies» para realizar estos ataques, normalmente junto a otros zombies, formando una BotNet.

Un ordenador zombie es aquel que trabaja, sin saberlo, al servicio de un tercero a causa de infección de algún tipo de malware.

4.1. Navegación

Estos tipos de ataques, además de mediante las técnicas aprendidas, se pueden controlar desde nuestro navegador. Por ejemplo, Mozilla Firefox incluye una opción de seguridad que permite establecer filtros contra los ataques de **suplantación** e **interceptación** y avisos contra sitios presuntamente falsos.



Durante la navegación por internet, si no se utilizan filtros en los navegadores –a veces incluso utilizándolos–, es posible que de alguna manera se filtren en nuestro ordenador troyanos, gusanos y otro malware. En caso de detectar este tipo de infección deberemos eliminarla con un antivirus o programa especial, como **Spybot Search & Destroy,** o como **Ad-Aware,** que realizan análisis **en tiempo real** o contextual sobre dispositivos, carpetas o archivos, para detectar, impedir la entrada y eliminar *spyware*, virus, troyanos, *rootkits*, gusanos, *bots*, *keyloggers* y *hijackers*.

La seguridad que se debe establecer en internet es similar a la de cualquier red, teniendo en cuenta que habrá que dedicar más recursos a la protección ya que los ataques pueden ser dirigidos desde cualquier parte del mundo y por muchos atacantes distintos, coordinados o no.

Son recomendables algunas prácticas seguras, como la navegación por páginas que cuentan con **certificado de seguridad,** y en caso de no contar con el certificado no introducir ningún dato que sea susceptible de ser robado.

Se deben utilizar navegadores actuales y mantenerlos siempre **actualizados** ya que es la única forma de reparar las posibles vulnerabilidades que se hayan detectado.

Además, puede resultar útil **bloquear el acceso a páginas con contenido potencialmente peligroso** así como la ejecución de JavaScripts que pudieran realizar tareas sin nuestra aprobación.

Muchos navegadores actuales cuentan con *plugins* que se encargan de hacer más seguro nuestro paso por internet, pudiendo configurar filtros contra la suplantación de identidad y otros tipos de ataque.

caso **práctico** inicial

Además de actualizar los navegadores es conveniente utilizar los que brinden la máxima seguridad en cada momento.

Actualmente se considera **Mozilla Firefox** como el navegador más seguro.

↑ *Plugin* del navegador Firefox que avisa de la posible suplantación de una web auténtica.

4.2. Comercio electrónico

Tradicionalmente, el comercio electrónico, es decir, el comercio que usa como plataforma de sustentación internet, ha sufrido diversos problemas en cuanto a seguridad se refiere.

- **Tecnológicos.** Son los que hacen mención a la protección física de los sistemas que gestionan el comercio. Servidores que manejan bases de datos y transacciones económicas que deben ser seguras al cien por cien.
- **Legales.** Las relaciones comerciales se mantienen entre zonas con diferentes legislaciones e impuestos, una vez realizado un acuerdo comercial debe respetarse y no existe posibilidad de repudio del mismo.
- **Psicológicos.** Se debe superar la barrera que supone el miedo de las personas a realizar una operación a través de internet, dejando datos como sus números de tarjetas de crédito.

↑ Proceso de pago seguro a una firma de venta por internet, mediante la TPV (Terminal Punto de Venta) de 4B.

Si la web reúne las condiciones adecuadas de seguridad, no debe existir ningún riesgo, y estaremos avalados por las leyes siempre y cuando cumplamos las normas de seguridad mencionadas hasta el momento.

Ofrecer transacciones seguras desde la web de la empresa

Para las transacciones seguras, los negocios deben tener alojada su web en un **servidor seguro** que disponga del software correspondiente para aplicar protocolos seguros como **SSL** o **S-HTTP.**

Existe otro protocolo, llamado **SET,** *Secure Electronic Transaction*, es decir, **Transacción Electrónica Segura,** que fue desarrollado por dos grandes compañías como son VISA y MasterCard colaborando con compañías de software. SET está claramente orientado a actividades de comercio electrónico y ofrece gestión de registros del comerciante, autorizaciones y liquidaciones de pagos así como sus anulaciones, etc.

Autoridad Pública de Certificación Española

OBTENGA SU CERTIFICADO DE COMPONENTE

Seleccione el tipo de certificado de componente que desee obtener y recuerde que su petición se conservará durante un mes, tiempo en el que deberá de presentar la documentación correspondiente. En caso de superar dicho plazo será necesario realizar una nueva petición:

■ **Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por el nombre del dominio**
Este certificado permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servidor se identificará a los clientes con el nombre del dominio donde se encuentra su servicio Web.

■ **Solicitar un certificado de F.N.M.T. Clase 2 CA para un servidor web identificado por la dirección IP**
Este certificado le permitirá establecer comunicaciones con sus clientes utilizando la tecnología SSL, el estándar para comunicaciones seguras en la Web. Su servidor se identificará a los clientes con la dirección IP donde se encuentra su servicio Web.

↑ Primeros pasos para solicitar en la Fábrica Nacional de Moneda y Timbre un certificado para servidor web identificado por dominio o por dirección IP

Cómo instalar un SSL en el dominio

Se debe acudir a los servicios de una empresa de confianza que proporcione **certificados de seguridad SSL para dominios,** y seguir las instrucciones y consejos para su instalación.

A partir de tener instalado el certificado de seguridad, el usuario no tendrá que hacer nada, pero en el momento en que necesite hacer alguna transacción comercial a través de nuestra web, será informado de que existe el certificado, de si está o no está vigente, y del lugar donde se halla localizado geográficamente el titular del dominio.

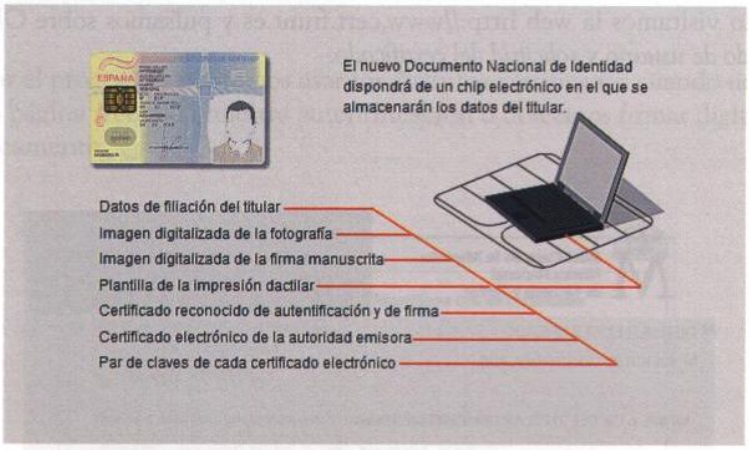
4.3. Firma digital

La firma electrónica sirve para vincular un documento o comunicación, de forma unívoca, a una persona física.

La firma tiene una utilidad similar a la manuscrita, y sus **características** también son equivalentes e incluso más fiables en cuanto a posibilidad de falsificación.

- **Únicas.** Cada firma es única para cada usuario.
- **Infalsificables.** A día de hoy no se ha podido falsificar una firma digital, y la forma en que se tratan los datos hace previsible que no se consiga en un largo tiempo.
- **Fáciles de autentificar.** Una tercera persona que recibe un documento firmado puede identificar de forma sencilla y comprobar la veracidad de la firma recibida.
- **Imposibles de rehusar.** El autor de un documento firmado digitalmente no puede negar la autenticidad del documento ni de la firma.
- **Fáciles de generar.** Las firmas digitales se generan mediante un sencillo proceso.

Para firmar un documento se necesitará poseer una **firma digital.** El actual **DNI-e** que usamos en España incluye una firma digital que puede ser usada mediante un lector de tarjetas. Los datos que incluye el chip electrónico lo convierten en un medio de firma digital tan fiable o más que la firma manuscrita.



Todos los pasos para la configuración se encuentran disponibles en la web del Ministerio del Interior www.dnielectronico.es. Una vez instalado, al introducirlo en el lector, se pedirá el PIN, que si es correcto nos permitirá su uso como certificado y firma.

Si aún no se posee DNI electrónico o lector de tarjetas, se pueden **firmar** documentos mediante un **certificado digital,** que se obtiene gratuitamente a través de la web de la **Fábrica Nacional de Moneda y Timbre.**

saber más

Firmar digitalmente significa haber adquirido un **certificado digital** y utilizarlo para cualquier tipo de operación telemática que requiera nuestra firma. También se firma digitalmente si se posee un DNI-e y un lector de tarjetas.

↑ Lector USB de ChipNet para DNI-e, disponible para Windows, Linux y Mac OSX.

↑ Chip electrónico del DNI-e

4.4. Certificados digitales

caso práctico inicial

Todos los trabajadores deberían contar con un certificado digital que los acredite como tales para realizar las tareas administrativas más delicadas.

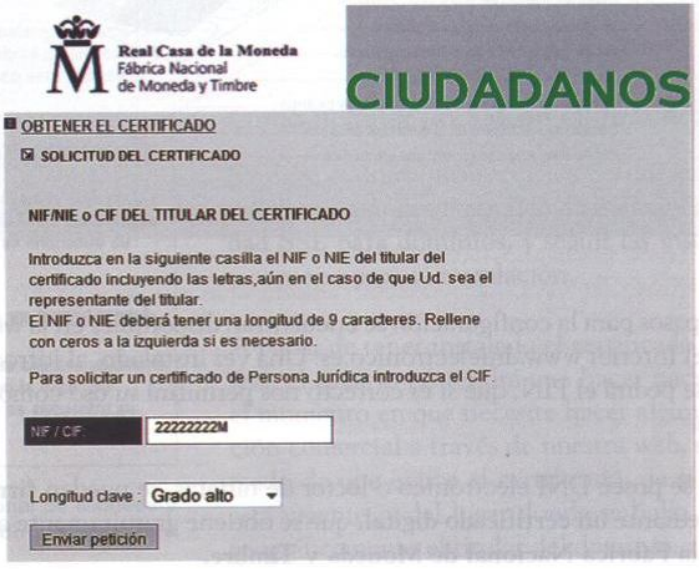
El **certificado digital** es un documento en el que una **autoridad de certificación,** que es una empresa u organismo de confianza que se encarga de emitir y revocar los certificados digitales y certificados de **firmas electrónicas,** garantiza que una clave pública y un determinado sujeto están realmente asociados, evitando de esta forma posibles suplantaciones de identidad.

Los certificados que son emitidos por autoridad de certificación suelen utilizar el estándar UIT-T X.509 y contendrán la siguiente información:

- **Firma digital de la autoridad de certificación.** Para comprobar que realmente la autoridad garantiza que la información contenida es cierta y la vinculación entre clave y sujeto es correcta.
- **Nombre y dirección.** De la persona que solicita el certificado digital.
- **Nombre y dirección.** De la autoridad certificadora.
- **Clave pública.** Del propietario del certificado.
- **Método de verificación.** De la firma digital incluida en el certificado.
- **Numero de serie.** Para identificar el certificado.
- **Fecha de validez.** Se incluye la fecha en que es emitido el certificado y la fecha en que expira.

La Fábrica Nacional de Moneda y Timbre, FNMT, es una autoridad de certificación a la que podemos solicitar nuestro certificado digital.

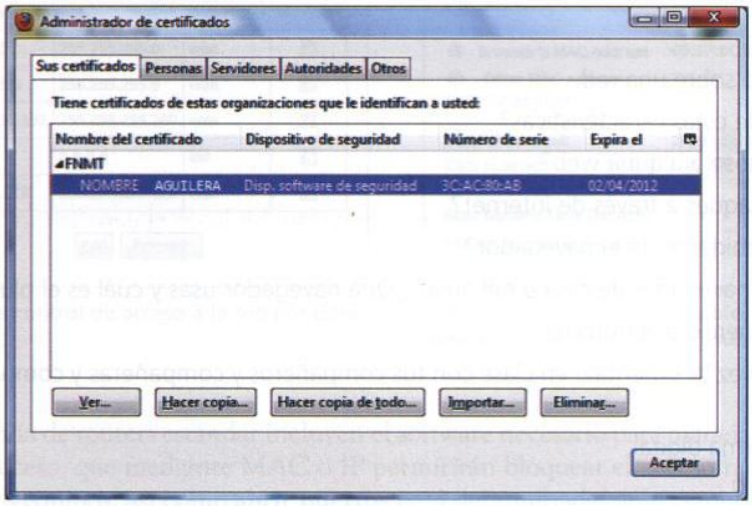
Para ello visitamos la web http://www.cert.fnmt.es y pulsamos sobre *Obtenga el certificado de usuario* y *solicitud del certificado*.



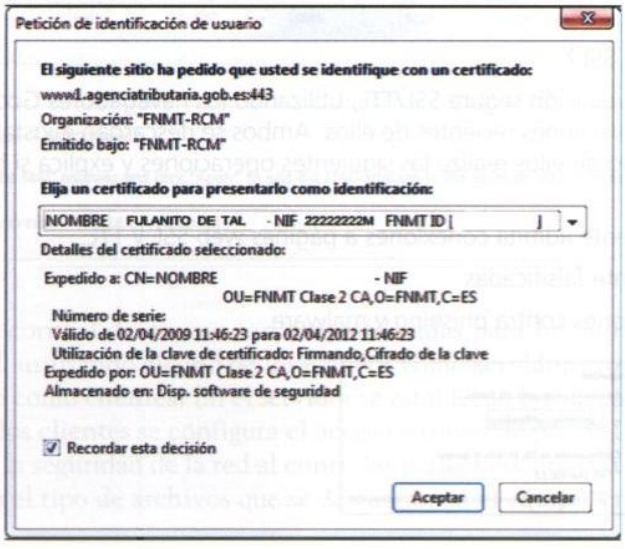
Rellenamos los datos solicitados y enviamos la petición. Se nos ofrecerá ver una lista de los sitios más cercanos al lugar donde nos encontremos, en donde podemos realizar la autentificación física, es decir, una oficina estatal donde presentemos nuestro DNI y el código que hemos recibido por la web, para verificar que nosotros hemos realizado la petición y no un tercero en nuestro nombre.

Una vez hecho esto podremos descargarnos en la misma página web nuestro certificado e instalarlo en el navegador para comenzar a usarlo. Para ello el navegador incluye herramientas, y su funcionamiento es común para los distintos sistemas que existen.

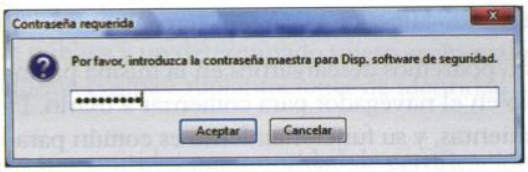
En Mozilla Firefox, desde **Herramientas → Opciones,** pestaña **Avanzado, Sus certificados,** tenemos las opciones para importarlo.



Al acabar el proceso ya podremos usar los distintos certificados cuando una aplicación o página web pida nuestra autentificación o deseemos firmar digitalmente un documento.



Si se desea, puede configurarse para que pida una contraseña adicional de control, para evitar que el certificado pueda utilizarse si se pierde o roban el ordenador donde se encuentra instalado.



ACTIVIDADES

8. ¿Cuál es la principal función del firewall?

9. ¿De qué tipos puede ser el firewall?

10. Enumera los posibles tipos de ataque sobre una red.

11. ¿Has sufrido alguna vez un ataque de estas características?

12. ¿Conoces algún caso de ataque famoso a alguna web?

13. ¿Qué particularidad presentan los ataques a través de internet?

14. ¿Por qué es importante actualizar debidamente el navegador?

15. ¿Tienes algún plugin instalado en el navegador de casa o del aula? ¿Qué navegador usas y cuál es el plugin?

16. ¿A qué problemas se enfrenta el comercio electrónico?

17. ¿Has comprado por internet alguna vez? Coméntalo en clase con tus compañeros y compañeras y comparad vuestras experiencias.

18. Enumera las características de una firma digital.

19. ¿Es posible falsificar una firma digital?

20. ¿Qué diferencia hay entre firma digital y certificado digital?

21. Busca información adicional sobre las autoridades de certificación y cita el nombre de alguna.

22. Describe brevemente el proceso para obtener un certificado digital.

23. ¿Qué elementos contiene, como norma general, un certificado digital?

24. ¿Qué diferencia, no de código o técnica, hay entre SSL y TLS?

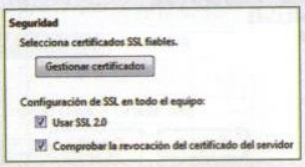
25. ¿Dónde solemos utilizar SSL?

26. ¿Cuál es la principal diferencia entre SET y SSL?

27. Realiza las siguientes actividades sobre navegación segura SSL/TTL, utilizando los navegadores Google Chrome y Mozilla Firefox, a ser posible usando versiones recientes de ellos. Ambos se descargan e instalan en pocos minutos. A continuación, con cada uno de ellos realiza las siguientes operaciones y explica si has conseguido hacerlas y cómo.

- Configura el navegador para que solamente admita conexiones a páginas web SSL y TTL.
- Aplica los filtros de páginas presuntamente falsificadas.
- Habilita, si lo permite el navegador, opciones contra phishing y malware.

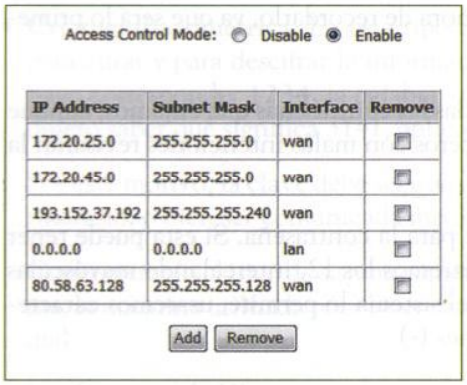
Una pequeña pista para Chrome:



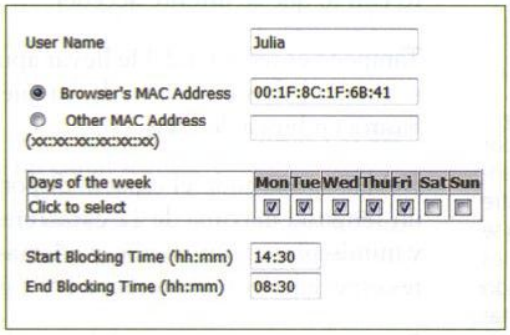
4.5. Listas de control de acceso

Las listas de control de acceso son un elemento más en la seguridad de las redes ya que son utilizadas para permitir el acceso de los usuarios a determinadas aplicaciones, bases de datos u otras áreas de la información, agrupándolos según el criterio de privilegios de acceso.

Controlan el tráfico en routers y switches, encargándose de filtrar el tráfico que pasa por estos dispositivos, pudiendo permitir o denegar el acceso, así como restringirlo durante determinadas horas y días a la semana.

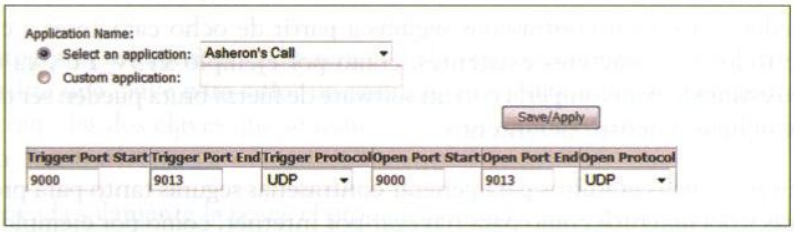


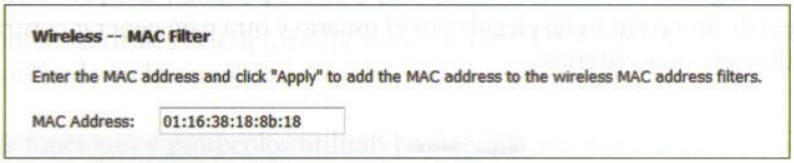
↑ Lista de control de acceso a la red por dirección IP.



↑ Restricciones horarias establecidas en el router para el uso de la red de una usuaria.

La mayoría de routers estándar incluyen el software necesario para manejar las listas de acceso, que mediante MAC o IP permitirán bloquear el acceso no permitido a los equipos, así como **abrir puertos** para determinadas aplicaciones.





Las listas de control de acceso son muy utilizadas para la configuración de proxys de red, utilizando alguno de los equipos como **servidor proxy** y configurando el resto como **clientes.** En el servidor se establecen las adecuadas listas de control y en los clientes se configura el acceso a través de proxy. De esta forma aumentamos la seguridad de la red al controlar perfectamente la navegación de los usuarios o el tipo de archivos que se descargan en el equipo, entre otras posibilidades.

4.6. Política de contraseñas

Las contraseñas son básicas en todos los aspectos de la seguridad, y por ello se deben establecer contraseñas suficientemente seguras para cada nivel, estableciendo períodos de tiempo para su cambio y llevando una adecuada política sobre este aspecto.

Las contraseñas deben ser completamente secretas, y ni siquiera los administradores de los sistemas deben conocerlas, ya que estos tienen otros métodos para acceder, en caso necesario, a nuestra información.

Como norma general, no utilizaremos como contraseñas nuestros nombres, DNI o fecha de nacimiento por facilidad a la hora de recordarlo, ya que será lo primero con lo que se intente acceder.

Tampoco es recomendable llevar apuntadas las contraseñas que elijamos, aunque se tiren a la basura más tarde, ya que terceros con malas intenciones revisarán la basura en busca de estas.

Debemos usar todo el espacio disponible para la contraseña. Si esta puede tener un longitud máxima de 12 caracteres, usaremos los 12, intercalando mayúsculas y minúsculas con números, y además, si el sistema lo permite, usaremos caracteres especiales como asteriscos (*) y guiones (-).

Bajo ningún concepto se deben utilizar contraseñas con palabras que aparezcan en el diccionario ni combinaciones de estas, ya que uno de los ataques más comunes es mediante el uso de un diccionario, probando todas las posibilidades hasta encontrar la correcta.

También evitaremos usar contraseñas que, a pesar de cumplir lo anteriormente dicho, sean fáciles de descubrir por factores sociales (*barcelona*), de actualidad (*crepúsculo*) o comodidad (*quieroentrar*).

Se pueden considerar contraseñas seguras a partir de ocho caracteres y combinando todos los caracteres existentes, como por ejemplo **x73v_Pt***, ya que el tiempo estimado para romperla con un software de fuerza bruta pueden ser tan largo que obligue a desistir del intento.

Existen programas gratuitos para generar contraseñas seguras tanto para proteger carpetas y documentos como para navegar por internet, como por ejemplo **Password Strength Analyser and Generator,** con dos pestañas, una para analizar la fortaleza de una contraseña elegida por el usuario y otra para generar contraseñas basándose en unos criterios:

saber más

Las contraseñas que se utilizan en un ordenador son guardadas por el sistema operativo en sus registros, mediante un sistema de encriptación. Aun así, los avances tecnológicos hacen que *hackers* expertos que accedan a la información de nuestro equipo, puedan encontrar y descrifrar nuestras contraseñas.

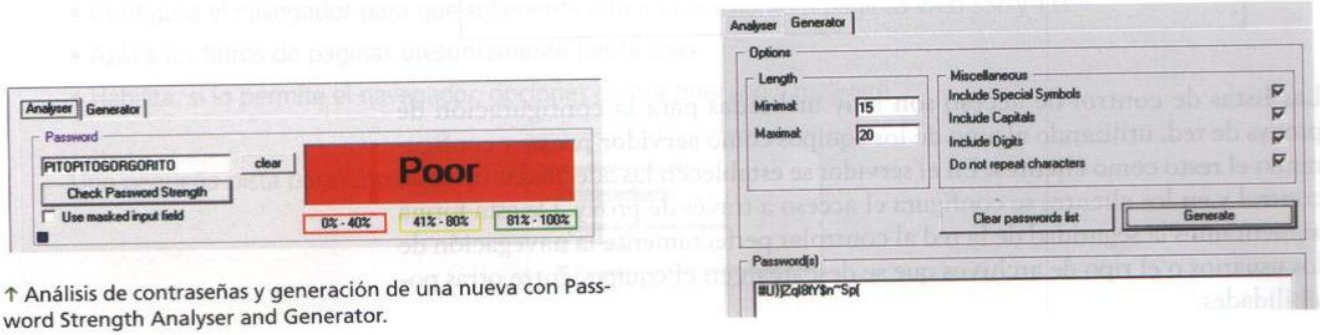
saber más

Ataque de fuerza bruta

Al contrario que el ataque por **diccionario,** que se utiliza probando palabras y combinaciones entre ellas, el ataque de **fuerza bruta** se utiliza probando combinaciones hasta dar con la clave de cifrado que se ha utilizado para encriptar un documento o una contraseña. Cuanto más complicada sea la clave más difícil es atacarla. A veces se necesitan horas o meses de cálculo de ordenador para dar con la clave. Otras veces no se consigue.

caso **práctico** inicial

La mínima longitud de contraseña debería adaptarse al máximo permitido por la aplicación o el sitio web que la vaya a solicitar. Se empieza a considerar segura a partir de ocho caracteres.



↑ Análisis de contraseñas y generación de una nueva con Password Strength Analyser and Generator.

4.7. Encriptación de datos

Criptografía

La criptografía es la ciencia que se encarga del cifrado y descifrado de información para ser transmitida de forma segura, garantizado que solo será entendida por el emisor y el destinatario final.

Para llevar a cabo esta misión, la criptografía utiliza diferentes tipos de cifrado y descifrado:

- **Criptografía simétrica.** En este tipo de criptografía se utiliza **la misma clave** para cifrar y para descifrar la información. Por ejemplo, si a las letras **abcd** les hago corresponder **1234,** la palabra «cada» en clave cifrada sería «3141». Y si quiero saber qué significa 3141, aplico la misma clave pero al revés.

  Por este motivo, la clave debe ser conocida de antemano por el emisor y el destinatario, o bien ser comunicada mediante un canal seguro.

  Como ejemplo clásico de sistema simétrico de encriptación encontramos Enigma, la máquina utilizada por el ejército alemán durante la segunda guerra mundial.

  Las funciones **hash,** que veremos más adelante, pertenecen a la criptografía simétrica.

  Ejemplo actual sería el algoritmo **DES** que utiliza claves de 56 bits, o lo que es lo mismo, existen 2^{56} posibles llaves de cifrado. Otros algoritmos de criptografía simétrica son **IDEA, RC2, Bowfish** y **3DES.**

  El principal inconveniente de la criptografía simétrica es que la clave «única» puede llegar a interceptarse por terceros.

- **Criptografía asimétrica.** A diferencia de la criptografía simétrica, la asimétrica utiliza una clave para cifrar un mensaje y otra distinta para descifrarlo. En concreto, las dos claves que se usan se llaman **pública** (para cifrar) y **privada** (para descifrar).

  La privada solamente la posee el propietario y debe garantizarse que nadie tenga acceso a ella. La clave pública la puede tener cualquier persona.

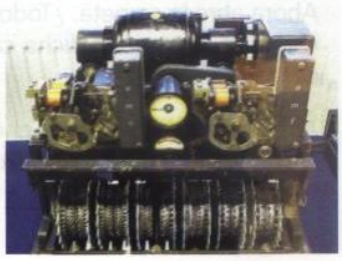
  Algunos algoritmos de criptografía asimétrica son **DSA** y **RSA,** este último el más utilizado en la actualidad.

Algunas funciones y protocolos utilizan criptografía simétrica o asimétrica. Por ejemplo, uno de los protocolos más conocidos en encriptación mediante clave pública y privada es **PGP.**

saber más

La máquina Enigma fue descifrada por **Alan Turing,** que es considerado uno de los padres de la informática moderna.

↑ La máquina **Enigma** utilizada por el ejército alemán en la Segunda Guerra Mundial.



→ Máquina **Lorenz,** utilizada en la Segunda Guerra Mundial para cifrar comunicaciones telegráficas de alto nivel militar.

Herramientas de cifrado

saber más

CryptoForge tiene una opción muy útil con la que podremos realizar **borrado seguro** de archivos, para de esta forma garantizar que ningún software recuperador de archivos los pueda reparar.

Puede utilizarse en los sistemas Windows™ 2000, XP, Server 2003, Vista, Server 2008, Server 2008R2 y Windows 7.

Existen multitud de herramientas para el cifrado y descifrado de documentos.

Si no vamos a enviar información, sino que deseamos proteger los datos almacenados en nuestro propio equipo, podemos contar con la herramienta de código abierto **TrueCrypt,** que permite crear una unidad o partición encriptada y oculta donde podemos guardar los archivos que consideremos importantes.

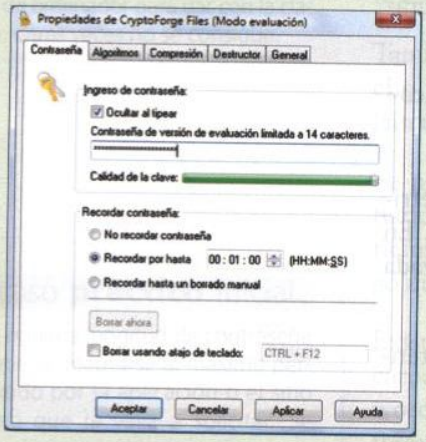
En cambio, si deseamos encriptar un archivo para posteriormente enviarlo por correo electrónico, transportarlo en un *pen drive* sin miedo a que lo utilicen en caso de robo o pérdida o, simplemente, tenerlo guardado en el ordenador de forma segura, podemos utilizar **CryptoForge** (www.cryptoforge.com).

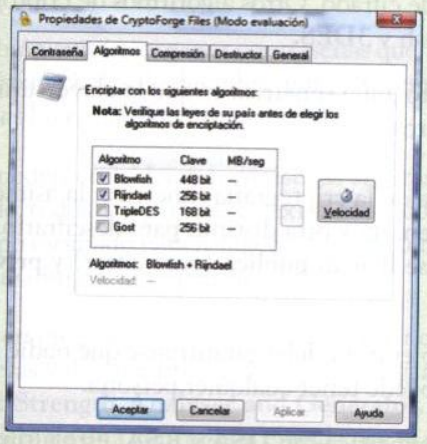
La versión gratuita de prueba es para 30 días. Después de ese período se puede seguir usando para desencriptar, pero para encriptar debe comprarse.

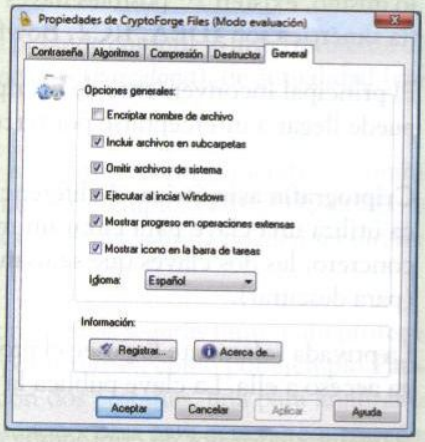
EJEMPLO

Si en tu equipo hay alguno de los sistemas operativos que soporta el programa, descarga CryptoForge de la dirección indicada. Ocupa muy poco espacio en disco. Instálalo y configura sus ventanas, por ejemplo como muestran las imágenes siguientes. En la primera necesitas introducir la contraseña que te servirá para encriptar y desencriptar. En la segunda, los algoritmos que deseas que se apliquen a la encriptación y en la tercera otras opciones que puedes elegir o dejar como están.

Una vez configurado, acepta y cierra la ventana de configuración.



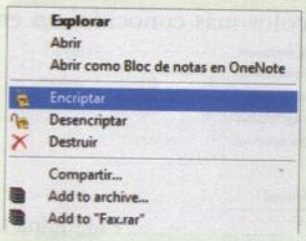




Haz clic con el botón secundario del ratón sobre una **carpeta** que desees encriptar. Verás que existen tres opciones que antes no estaban: Encriptar, Desencriptar, Destruir. Encripta la carpeta, pero para ello antes deberás introducir la contraseña.

Ahora abre la carpeta. ¿Todo normal? Hasta llegar a los archivos que contiene dicha carpeta, que se mostrarán con candado.

Al hacer doble clic sobre el candado o seleccionar Desencriptar, el programa solicita la contraseña. Si es correcta, podrá verse el archivo.



Hash y MD5 hash

- **Hash.** Llamamos hash a una función utilizada para generar claves que representen a un archivo o documento, principalmente a su contenido.

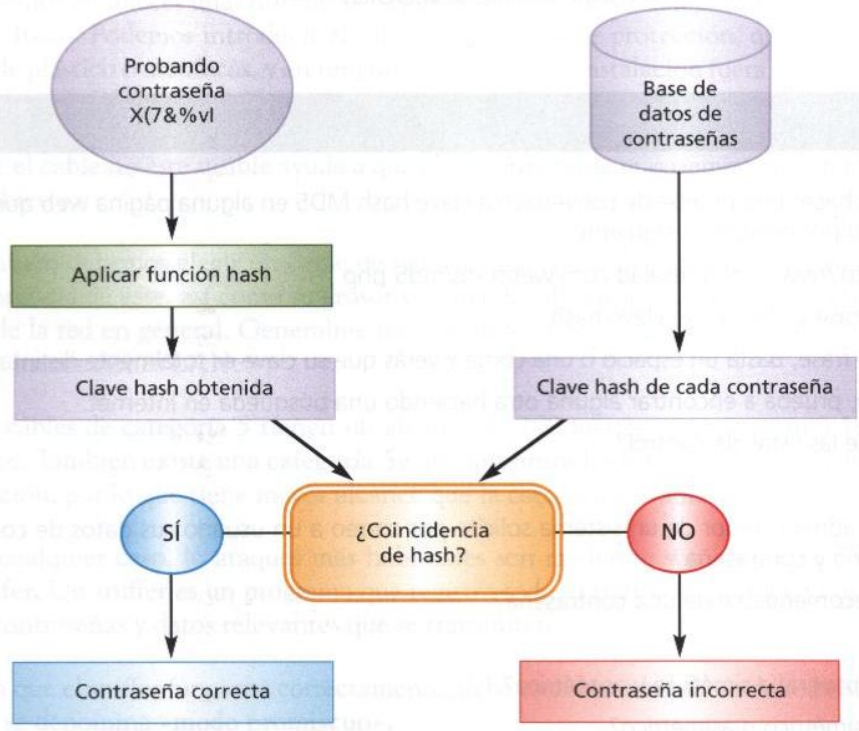
  Se llama también hash o hashing el resultado de la ejecución de una **función hash,** para comparar dos archivos. Si la comparación da dos claves diferentes, con casi toda probabilidad los dos archivos no son iguales.

  Si durante un transporte a través de la red, algún tercero malintencionado modifica un archivo (por ejemplo, le agrega un código malware), se puede comprobar si el archivo final es exactamente igual al original comparando sus claves hash.

  Puede utilizarse para muchos propósitos distintos, uno de ellos podría ser la comprobación de contraseñas: si un usuario (o un intruso) introduce una contraseña y esta se compara con las bases de datos de contraseñas guardadas en clave hash, puede ocurrir que la clave generada por la prueba de contraseña coincida con una de las que hay en la base de datos, con lo que, con mucha probabilidad, la contraseña probada será correcta. En caso contrario, es casi seguro que la contraseña de intento será errónea.

caso **práctico** inicial

El hash proporciona una utilidad de comprobación de que un documento original y una copia del mismo son exactamente iguales. Es una herramienta a tener en cuenta si no se utilizan vías seguras de comunicación.



↑ Comprobación de contraseñas por sus claves hash, una función que suele estar mecanizada mediante programas específicos.

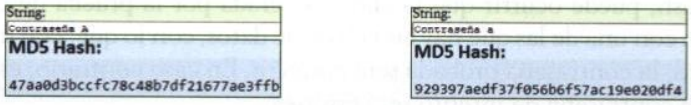
- **MD5.** Es un algoritmo de reducción criptográfico muy utilizado actualmente, sobre todo en lo referente a descargas en internet, para comprobar que el archivo descargado se corresponde con el que se deseaba descargar, protegiéndonos de esta manera contra el malware que pudiera haberse incluido.

Para hacer la comprobación necesitamos comparar la suma MD5 del archivo original y comprobar que coincide con la que obtenemos nosotros al hacer el cálculo.

Son muchas las empresas que utilizan estos sistemas, por ejemplo, en la web del sistema operativo Ubuntu encontramos todos los hashes MD5 de las imágenes ISO de sus distribuciones.

(Karmic Koala): October 2009 (Supported until April 2011)

md5 Hash	*Version*
836440698456aa2936a4347b5485fdd6	ubuntu-9.10-alternate-amd64.iso
3faa345d298deec3854e0e02410973dc	ubuntu-9.10-alternate-i386.iso
dc51c1d7e3e173dcab4e0b9ad2be2bbf	ubuntu-9.10-desktop-amd64.iso
d91659de6e945dbb96eb8970b2b4590a	ubuntu-9.10-desktop-armel+dove.img



↑ Solamente cambiar una «A» por una «a» hace que el hashing MD5 proporcione códigos totalmente diferentes.

ACTIVIDADES

28. Si aún está disponible, puedes hacer una prueba de conversión a clave hash MD5 en alguna página web que disponga de ese servicio, como por ejemplo la siguiente:

http://www.miraclesalad.com/webtools/md5.php

a) Escribe una palabra o una frase y observa su clave hash.

b) Cambia cualquier cosa de la frase, basta un espacio o una coma y verás que su clave es totalmente distinta.

Si no está disponible la página, prueba a encontrar alguna otra haciendo una búsqueda en internet.

29. ¿Cuál es la principal función de las listas de control?

30. ¿Dónde suelen configurarse?

31. ¿A qué puede deberse que el administrador de un sistema solicite por correo a un usuario sus datos de conexión como nombre de usuario y contraseña?

32. ¿Cuál es la longitud mínima recomendable de una contraseña?

33. ¿Qué es la criptografía?

34. ¿Cuál es la diferencia entre criptografía simétrica y asimétrica?

35. ¿El sistema de cifrado RSA es simétrico o asimétrico?

36. ¿Por qué DES ya no se considera seguro?

37. ¿Necesita el administrador de un sistema saber las contraseñas de los usuarios?

38. Indica una contraseña que consideres segura y otra insegura. Compáralas con las de tus compañeros.

a) ¿Usas la misma contraseña para el correo y los chats?

b) ¿Es seguro hacer esto?

c) ¿Por qué?

5. Redes cableadas e inalámbricas

Una red LAN es una **red de área local,** del inglés **Local Area Network.**

5.1. Red cableada

Mediante este tipo de red se conectan equipos y periféricos y su limitación es física, ya que el alcance de los cables será limitado y, normalmente, dentro de un mismo edificio.

Este tipo de redes son las más utilizadas en empresas y edificios para conectar los equipos locales a los servidores y trabajar con los datos almacenados en ellos.

Para que se lleve a cabo un ataque dentro de una red LAN, el atacante deberá estar físicamente conectado a ella, lo que implica encontrarse dentro de la empresa. Es por esto que este tipo de ataques lo suelen realizar **personas de confianza descontentas** o bien intrusos profesionales que consiguen burlar la seguridad del entorno físico.

Debemos establecer unas **normas de seguridad** en su instalación para evitar el acceso físico. Podemos introducir el cable en canaletas de protección, que pueden ser de plástico o metálicas, y en ningún caso realizar la instalación fuera de la zona de seguridad del edificio.

Que el cable no esté visible ayuda a que el atacante tarde más tiempo en cumplir su objetivo.

También debemos elegir un cable de red adecuado en cada momento, ya que la resistencia de este, así como su grosor y forma de fabricación, mejorarán el estado de la red en general. Generalmente usaremos cable de **categoría 5** o mejores para instalaciones LAN.

Los cables de categoría 5 tienen un alcance de 100 metros y comunican a 100 Mbps. También existe una **categoría 5e** que **minimiza las interferencias** y la atenuación, por lo que tiene mayor alcance que la categoría 5 tradicional.

En cualquier caso, lo ataques más habituales son mediante software, como los **sniffer.** Un sniffer es un programa que registra todo el tráfico de la red en busca de contraseñas y datos relevantes que se transmiten.

Para que el sniffer funcione correctamente, debe establecer la tarjeta de red en lo que se denomina **«modo promiscuo».**

La mejor forma de **protegernos de los sniffer** y analizadores de protocolos es crear una **conexión privada** para cada dispositivo de forma que ese canal que usemos esté al margen del sniffer.

Se pueden, además, realizar filtrados **por MAC,** que es el identificador exclusivo de una tarjeta de red, y **por IP,** así como cerrar y abrir puertos del router, accediendo al mismo mediante un navegador, para impedir el ataque a través de los puertos estándar de aplicaciones peligrosas.

caso **práctico** inicial

Tradicionalmente se ha optado por el cableado como solución más segura, pues además aporta un mayor rendimiento, aunque hay que estudiar cada caso individualmente.

saber más

Una de las técnicas utilizadas para captar señales de redes inalámbricas es la llamada ***wardriving,*** que consiste en recorrer zonas (normalmente con un vehículo en movimiento) utilizando un portátil o una PDA con conexión wifi y ver qué redes hay disponibles en cada zona, además de comprobar el tipo de protección de que disponen (contraseña segura, menos segura o sin contraseña).

Existen herramientas específicas, muchas de ellas gratuitas, para facilitar la tarea del *wardriver.*

saber más

Un ordenador trabaja en «modo promiscuo» cuando **forma parte de** una LAN y captura todo el tráfico que circula por ella.

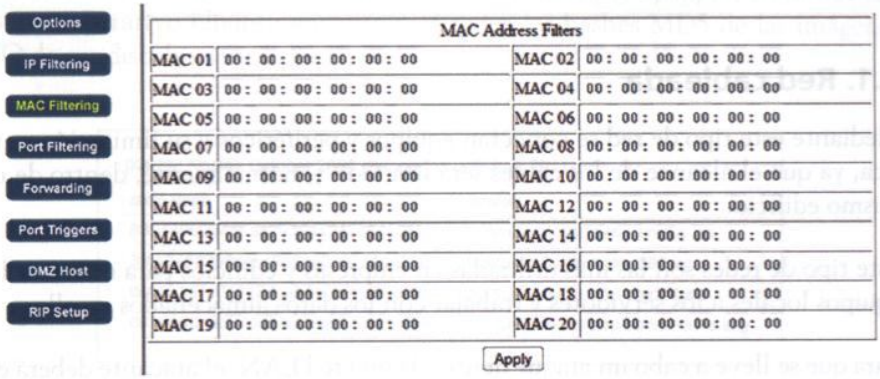
saber más

Sniffer

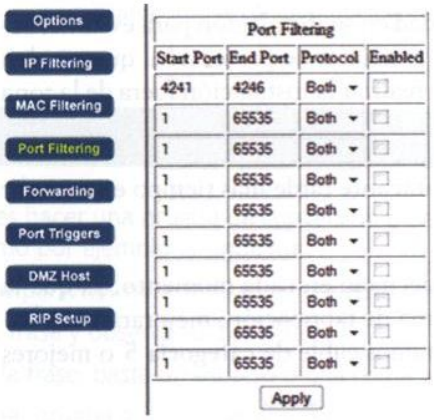
Programa que sirve para monitorizar la red, ya sea con fines de diagnóstico o con objetivos maliciosos.

Puede escanear tanto redes cableadas como inalámbricas.

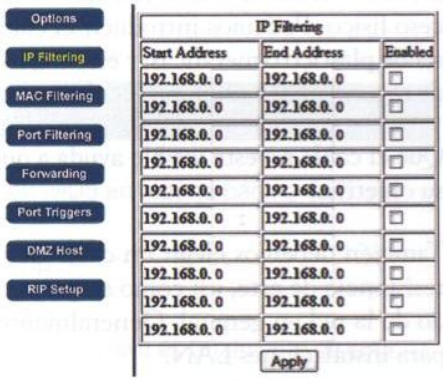
Pero, sobre todo, el cifrado de documentos es una garantía en caso de que un sniffer capte paquetes de información.



↑ Filtrado de direcciones Mac en el router.



↑ Cierre de puertos desde el router.



↑ Filtrado por IP.

5.2. Redes inalámbricas

caso práctico inicial

Si contamos con dispositivos móviles, las redes inalámbricas serán la única solución viable para la instalación de redes.

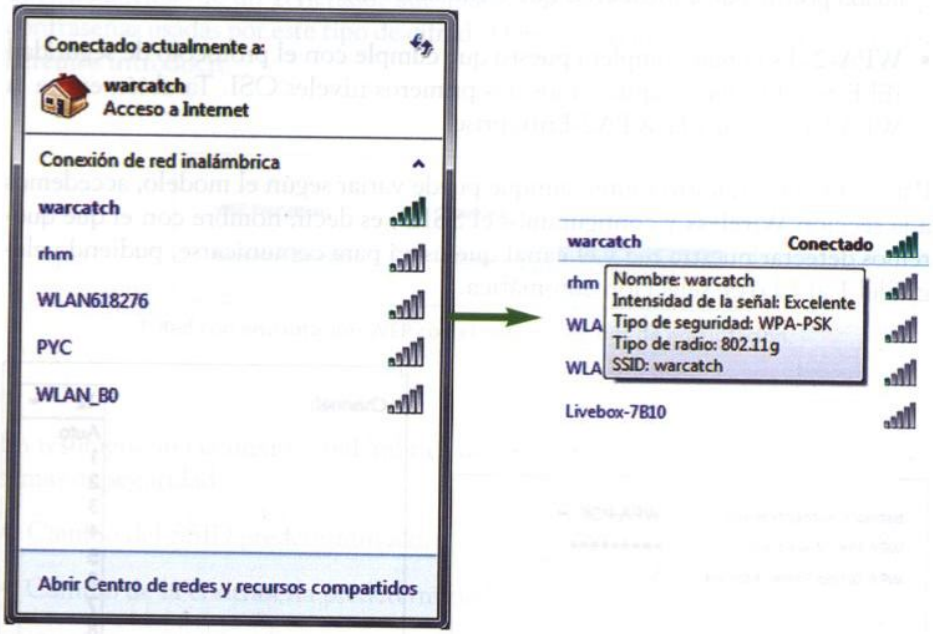
Todas las redes inalámbricas pierden la seguridad que ofrecen las LAN dado que es posible acceder a ellas sin necesidad de acceso al entorno físico.

El perímetro en el que se puede acceder sigue estando limitado, pero es mayor que el que brinda la seguridad de un edificio.

Cualquier equipo que se conecte a la red inalámbrica tendrá acceso al resto de la red, es decir, es equivalente a conectarse a través de una red LAN. Por esto es fundamental proteger los equipos para que, en caso de una intrusión, siga existiendo la máxima seguridad posible, pero además dedicaremos recursos para evitar que sistemas no autorizados rompan la seguridad inalámbrica y logren conectarse.

Debemos saber que si no utilizamos ningún protocolo de cifrado en nuestra conexión, cualquier persona dentro del alcance de nuestra red podrá conectarse y usar un sniffer para ver el tráfico, además de que podría usar nuestra conexión con fines delictivos a través de internet.

Existen una serie de pasos previos para conocer el tipo de cifrado que usamos en la conexión inalámbrica a la que nos conectamos. Cuando pulsamos sobre el icono para ver las redes disponibles, al pasar el ratón sobre alguna de ellas se muestra información relevante.



Lo más recomendable es utilizar algún tipo de encriptación en nuestra red, de este modo los paquetes viajan encriptados y será difícil para el intruso conectarse. Hay varios tipos de encriptación.

Los routers, accediendo como se indicó para el firewall por hardware, pueden configurarse con distintos tipos de encriptación. Las más importantes son WEP y WPA.

- **WEP.** Tradicionalmente es la encriptación que traen por defecto los routers, pero esta tendencia está cambiando debido a la facilidad con la que se puede romper la seguridad de esta encriptación.

  La longitud de la contraseña con la que encriptamos puede ser de 64 o de 128 bits, y de esta longitud dependerá la robustez de la contraseña, pero la mejor es la de 128.

  Sus siglas en inglés significan **Wired Equivalent Privacy,** es decir, Privacidad Equivalente a Cableado. Se basa en el algoritmo para cifrado RC4.

caso práctico inicial

El acceso no autorizado a la red puede evitarse, entre otras maneras, impidiendo la entrada de software espía y aplicando filtros en el propio router.

saber más

La mayoría de ISP (proveedores de internet) están cambiando las configuraciones por defecto de los routers que instalan puesto que han detectado un gran aumento en las conexiones no autorizadas a dispositivos configurados con encriptación WEP.

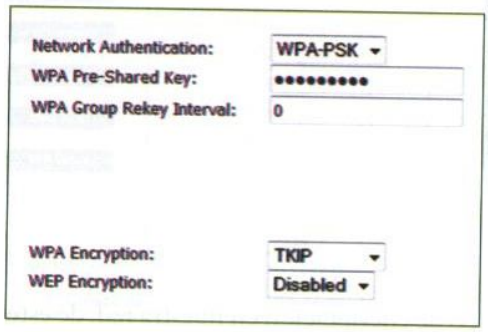
- **WPA.** WI-FI Protected Access. Este protocolo corrige los problemas que presenta WEP y permite la autentificación a través de un servidor, donde están guardadas las contraseñas y datos sobre los distintos usuarios de la red, aunque también se puede configurar para utilizar un sistema de claves compartidas, equivalente al de WEP, que se llama PSK *(Pre-Shared Key)*.

  Si el cifrado WPA usa una clave compartida, se denomina WPA-Personal y si usa un servidor para la clave, WPA-Enterprise.

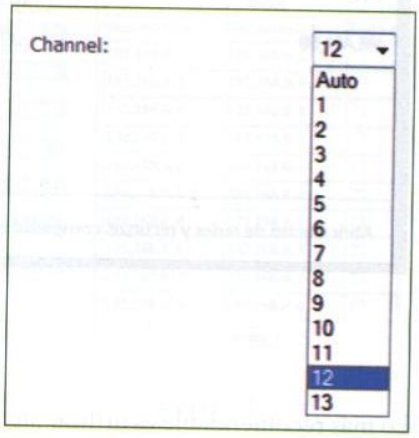
  Para acceder a estas redes rompiendo su seguridad se necesita un ataque por fuerza bruta a base de diccionarios, lo que podemos evitar utilizando la adecuada política de contraseñas que estudiamos anteriormente.

- **WPA-2.** Es la más completa puesto que cumple con el protocolo de seguridad IEEE 802.11, que se aplica a los dos primeros niveles OSI. También existe la WPA2-Personal y la WPA2-Entreprise.

Para configurar nuestro router, aunque puede variar según el modelo, accedemos a la sección **Wireless** y configuramos el **SSID,** es decir, nombre con el que queremos detectar nuestra red y el **canal** que usará para comunicarse, pudiendo elegir del 1 al 13 o de selección automática.

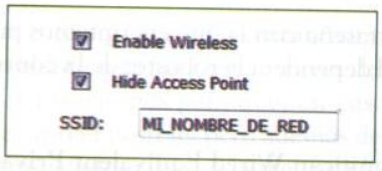


↑ Contraseña de red con encriptación WPA.



↑ Elección del canal de comunicación de la red configurado en el router.

Si no escribimos un nombre de red o SSID, nuestra señal inalámbrica no será visible, pero el tráfico seguirá siendo escaneado sin problemas por sniffers y analizadores de protocolo. También puede ocultarse el nombre, configurándolo de ese modo en el router, si admite esa opción.

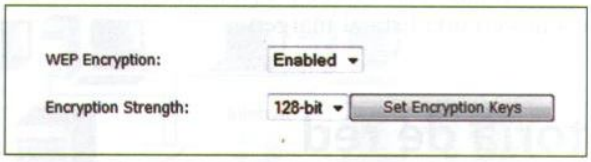


↑ Red Wireless habilitada, con nombre, pero escondido.

En la sección referida a seguridad podemos elegir utilizar cifrado WPA-PSK. PSK proviene de *Pre-Shared Key*, y en el lugar indicado podemos escribir la contraseña que deseemos usar, pero debemos recordar siempre elegir una contraseña segura para evitar ataques de diccionario.

Si en lugar de encriptación WPA queremos utilizar **WEP**, hemos de saber que nuestra red será menos segura y que los ataques pueden ser realizados por personas sin conocimientos especiales de informática.

Podemos elegir si deseamos una clave de 64 o de 128 bits. Siempre es recomendable utilizar el máximo tamaño permitido, por eso seleccionamos la de 128. Se dispone además de un generador automático de contraseñas hexadecimales (las contraseñas usadas por este tipo de cifrado) basadas en una palabra o frase que deberemos introducir.



↑ Red con encriptación WEP con el máximo de bits de encriptación.

En resumen, una conexión inalámbrica debe dotarse, como mínimo, de estos sistemas de seguridad:

- Cambio del SSID predeterminado.
- Cambio de la contraseña predeterminada de acceso al router.
- Cambios periódicos de contraseña de acceso al router.
- Cambio del número IP predeterminado del router.
- Contraseña de red cifrada en WPA o WPA-2.

ACTIVIDADES

39. ¿Cuál es la principal limitación que presenta una red LAN (cableada)?

40. ¿Para qué suelen utilizarse las redes LAN?

41. ¿Cuál es el ataque más común en una red LAN?

42. ¿Necesitan protección los equipos conectados a una red inalámbrica o es suficiente la que brinda la configuración predeterminada de la red?

43. ¿Qué tipos de encriptación de red conoces? ¿Cuál usas en casa? Compara tu respuesta con las de otras compañeras y compañeros.

44. ¿Por qué es mejor usar encriptación WPA en las redes inalámbricas?

6. NIDS

caso práctico inicial

A pesar de estar analizando todo el tráfico que circula por nuestra red, los sistemas de detección de intrusos (NIDS) no aumentan el flujo de tráfico.

Los IDS son **sistemas de detección de intrusos,** y en nuestro caso, los **NIDS** detectan intrusos dentro de una red (N de *Net*, red).

Se encargan de buscar patrones sospechosos, así como intentos de accesos al equipo o ataques de denegación de servicio, y todo esto, además, en tiempo real.

Estos sistemas no solo analizan el tráfico de red entrante, sino que también buscan en el tráfico saliente e incluso en el local, para así garantizar la máxima vigilancia. Para su óptima eficacia han de ser actualizados periódicamente.

Normalmente los NIDS **trabajan en equipo con los firewall** y cuentan con listas de ataques conocidos, para que estos sean reconocidos rápidamente.

Existen implementaciones tanto de software como de hardware de los IDS. Algunos ejemplos comerciales son **Snort** y **Symantec Intruder Alert.** Otros programas los mostramos en una lista al margen.

tripwire

INTRUSION

INTOUCH INSA

cisco

IBM

↑ Otras marcas con aplicaciones IDS.

7. Auditoría de red

caso práctico inicial

Para que el tráfico de documentos y datos a través de la red resulte seguro, se deberán aplicar todas las medidas posibles de seguridad que se han explicado en esta unidad.

En este punto conviene repasar el epígrafe correspondiente a la auditoría de la unidad 1. Recordamos que la auditoría puede hacerse tanto por personal especializado de la propia organización como por empresas externas que se dediquen a este fin.

La auditoría de la red equivale prácticamente a realizar un control de todos los activos del sistema de información, sus vulnerabilidades, amenazas, riesgos y soluciones empleadas, puesto que cualquier aspecto físico o lógico de los que hasta ahora se han estudiado en este libro tiene su influencia positiva o negativa sobre nuestra red.

Como mínimo, para realizar una auditoría de red es necesario:

- Conocer la topología de la red.
- Analizar los puntos vulnerables, tanto físicos como lógicos.
- Conocer las medidas de protección aplicadas a cada punto vulnerable.
- Señalar las deficiencias encontradas tras el análisis.
- Proponer las recomendaciones necesarias para subsanar cualquier anomalía.

ACTIVIDADES

45. Propuesta de actividad en grupo o para discusión global en el aula:

RedIris proporciona una muy buena información acerca de NIDS en la siguiente dirección:

http://www.rediris.es/cert/doc/unixsec/node26.html

(o, si lo deseas, puedes encontrar esa página escribiendo en el buscador las palabras **rediris sistemas detección intrusos).**

Lee el apartado final **«Algunas reflexiones»** y responde a las siguientes preguntas:

a) ¿Cuál es tu opinión acerca de la relación entre el hacker y el derecho a la libertad de información que se menciona en el apartado referido?

b) Personalmente, ¿consideras al hacker héroe o villano? Razona tu teoría.

PRÁCTICA PROFESIONAL

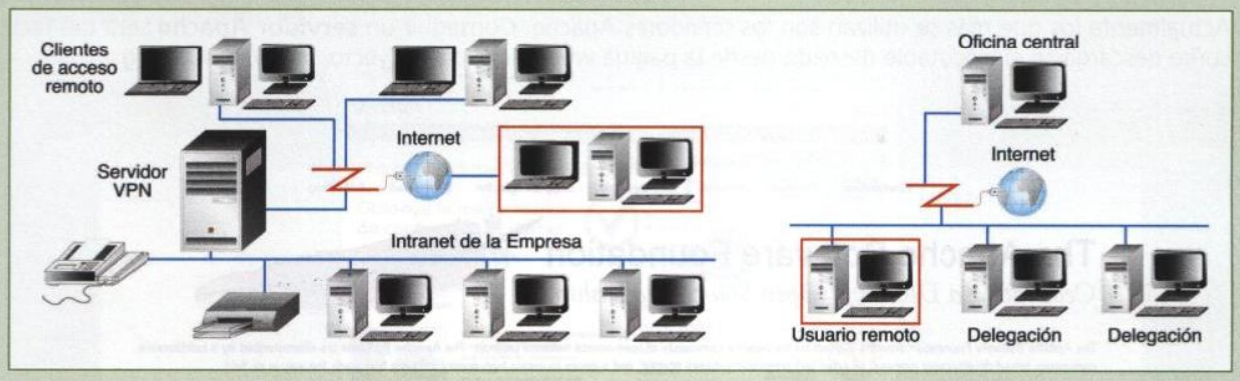
Comunicación segura en la red

1. Configuración mediante software de una red privada virtual

Siguiendo el ejemplo incluido en el epígrafe 2 y las indicaciones de tu profesor o profesora, de forma individual o en grupo, configura –mediante las herramientas propias del sistema operativo que estés usando o con otro software– un equipo como usuario remoto de una red privada virtual (VPN) cuyo servidor esté previamente configurado como tal y otorgue los datos de configuración de clientes.

La VPN puede ser mediante *tunneling,* de acceso remoto, de punto a punto o VLAN.

EJEMPLOS



2. Configuración de una web con el protocolo HTTPS

Una empresa para la que trabajas ha decidido crear una página web con el protocolo HTTPS. En esta unidad se ha visto que este tipo de páginas están cifradas y ofrecen seguridad a las personas que las visitan.

¿Qué pasos ha de seguir tu empresa para configurar su página web mediante el protocolo HTTPS?

3. Instalación y utilización de la criptografía

Descarga e instala **CryptoForge** y encripta un archivo que tengas en tu ordenador (puede ser un documento de texto, una fotografía o cualquier otro tipo de archivo). Introduce una contraseña que puedas recordar. Envía el archivo encriptado por correo electrónico o por mensajería a dos o tres personas, de las cuales alguna al menos tendrá instalado Cryptoforge en su ordenador y otras no. Indica que necesitas una respuesta de cada destinatario en donde se explique, para cada caso:

a) Con qué tipo de icono se le representa en el equipo el archivo recibido.

b) Qué mensaje recibe el destinatario cuando intenta abrir el archivo.

c) Comenta en clase las respuestas de quienes lo recibieron sin tener instalado el programa y de quienes sí lo tenían.

4. Cerrar paso a un programa mediante firewall software

En un equipo dotado de conexión inalámbrica utiliza un firewall software (puede ser un programa gratuito o incluido en el sistema operativo) para NO permitir la entrada de un programa determinado, por ejemplo la «detección de redes». Comprueba que las normas fijadas al firewall con respecto a ese programa se cumplen. Observa los avisos y las posibles respuestas que dejan al usuario. Después, vuelve al firewall y habilita de nuevo el programa.

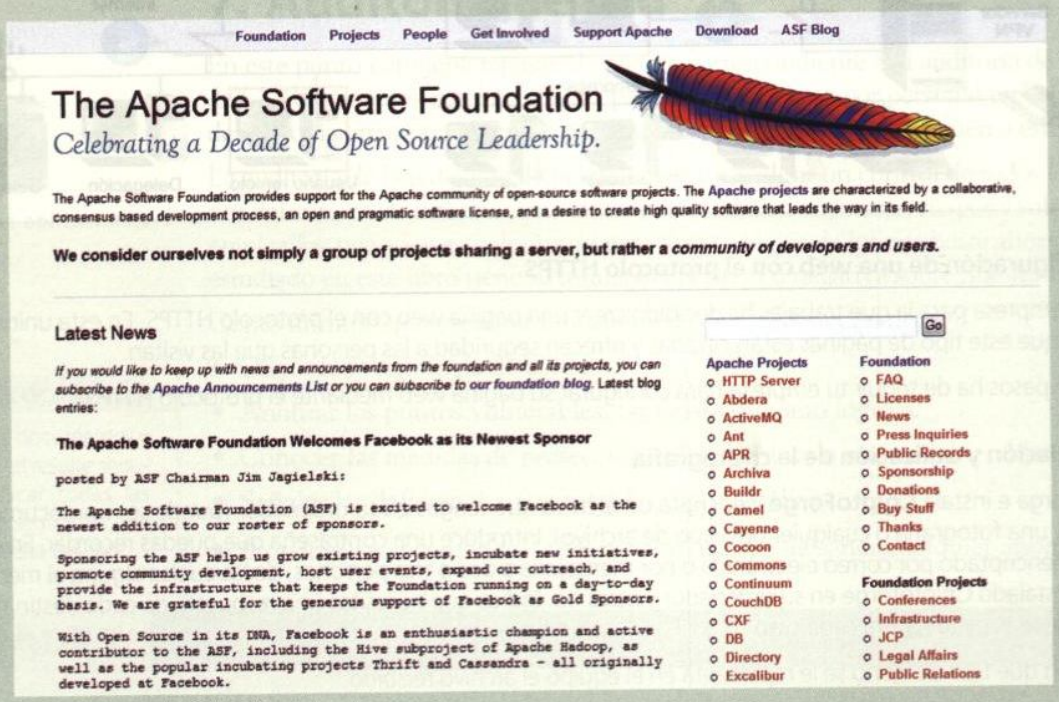
MUNDO LABORAL

El comercio electrónico desde el punto de vista de la empresa. Un ejemplo real

Desde el punto de vista del empresario, ofrecer un servicio web con la seguridad que brinda el protocolo SSL tiene múltiples ventajas, desde el aspecto legal y el propio de la seguridad en las transacciones, hasta la garantía que percibe el cliente por parte del empresario.

En consecuencia, es lógico que al instalar un servidor se adquiera un certificado SSL. Estos certificados no son parte de la programación de la página web, sino que deben ser instalados en el servidor.

Actualmente los que más se utilizan son los servidores Apache. Conseguir un **servidor Apache** será tan fácil como descargarse el ejecutable deseado desde la página web oficial del proyecto, www.apache.org



En caso de tener en el equipo un sistema operativo Windows, deberemos descargar la versión para Microsoft Windows con soporte para SSL. La instalación es sencilla, solo deberemos elegir los directorios de instalación y el nombre que tendrá nuestro servidor.

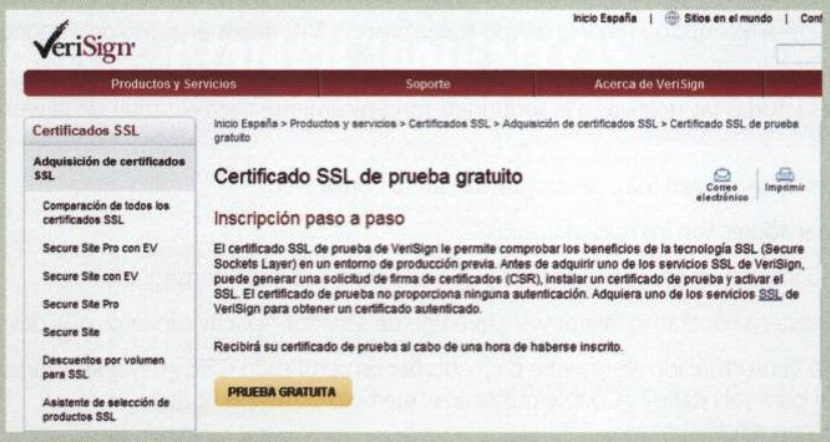
Una vez tengamos esto, debemos acudir a una autoridad certificadora para conseguir nuestro certificado SSL.

Para que la autoridad pueda comprobar nuestra actividad y los datos del servidor para el que solicitamos el certificado, debemos obtener un **CSR, *C*ertificate *S*igning *R*equest.**

Para ello podemos utilizar el **software del propio servidor,** pero en caso de no traerlo incorporado, existen **aplicaciones externas** que lo generan, como **OpenSSL,** que se descarga desde www.openssl.org

Al ejecutarlo, en el mismo directorio del servidor, nos hará una serie de preguntas sobre este, y generará el archivo CSR que enviaremos a la autoridad.

En nuestro caso usamos la **versión de prueba** del certificado digital de www.verisign.com, o la versión española en **www.verisign.es**

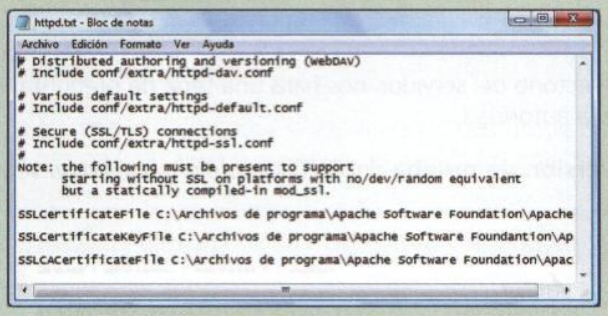


Una vez realizados todos los pasos, podremos descargar **el certificado para el servidor** y un **certificado intermedio,** necesario porque estamos usando una versión de prueba, pero que en su opción comercial de pago no es necesario.

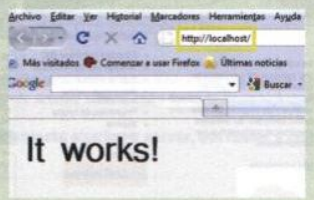
MUNDO LABORAL

Estos dos archivos, junto con la llave generada por el software **OpenSSL,** deberán ser indicados, con su ruta completa, en el archivo de configuración **http.conf** del servidor Apache.

Además, para que el servidor reconozca el protocolo SSL deberá «descomentarse» (eliminar la almohadillla) la línea que se encarga de cargar el modulo SSL/TLS.



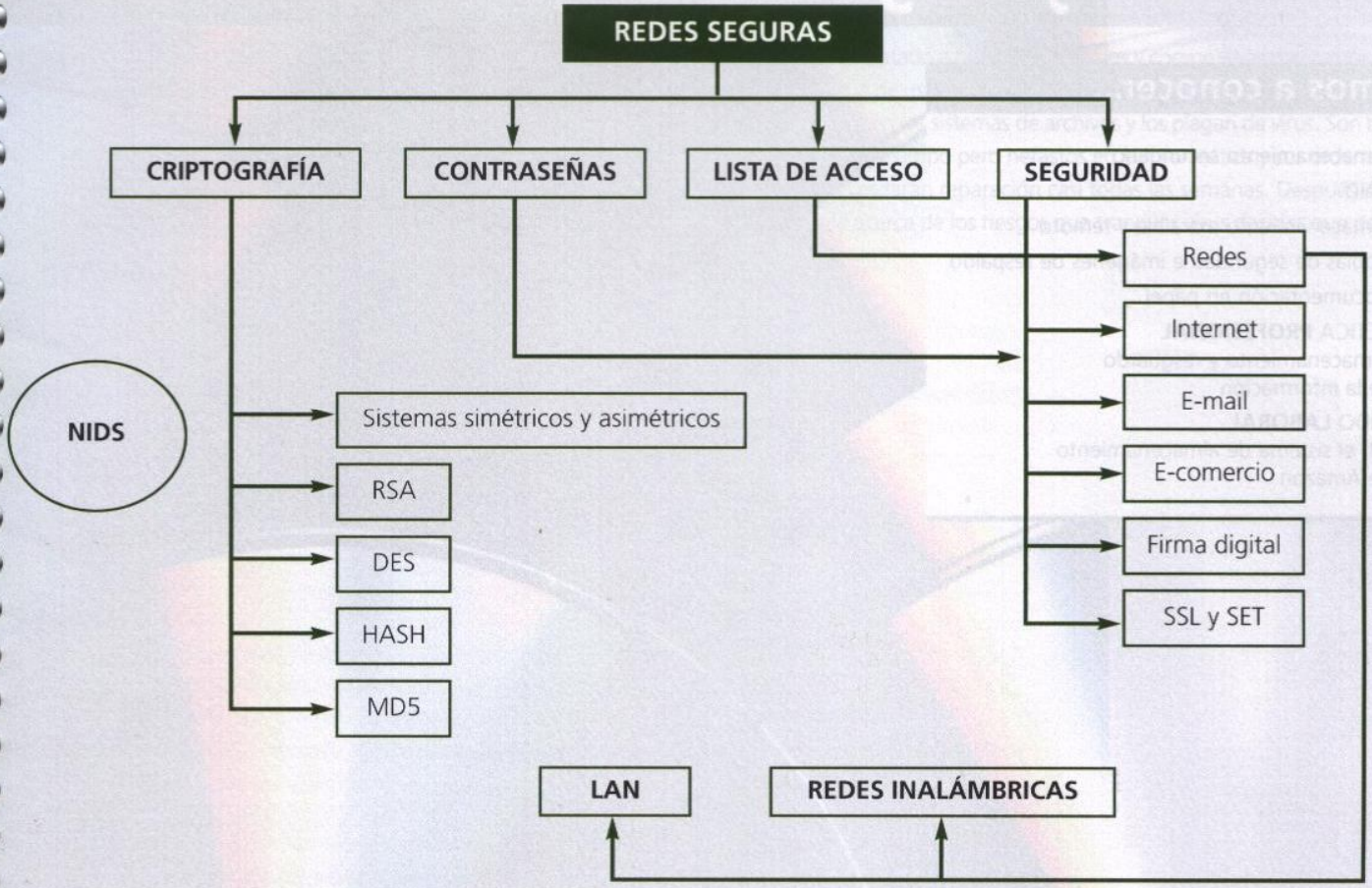
Una vez realizada toda la configuración, el servidor estará listo para servir páginas con certificación de seguridad SSL. Si hacemos una prueba local en nuestro servidor Apache con el modulo SSI, mostrará el resultado correcto.



Actividades

1. ¿Qué ventajas crees que aporta tener una web con protocolo SSL, desde el punto de vista legal, al titular de la web?
2. ¿Estas ventajas y todas las relativas a la seguridad son únicamente para el titular de la web? Razona la respuesta.
3. Los certificados de seguridad SSL, ¿se programan junto con la web?
4. ¿Qué tipo de servidores son los más utilizados?
5. ¿Es complicado instalar un servidor Apache? ¿Qué se debe hacer para conseguirlo?
6. Si tenemos un sistema operativo Windows, ¿qué tipo de servidor Apache tenemos que descargar e instalar?
7. Si el servidor no tiene instalado el software para obtener un certificado CSR, ¿hay aplicaciones externas que se puedan utilizar para solicitarlo? ¿Cuál se utiliza en el ejemplo de este artículo?
8. El certificado CSR de prueba que ofrece Verisign, ¿proporciona alguna autenticación real? ¿Qué habría que hacer para obtener esta autenticación?
9. Aplicar a la propia página web un certificado SSL, ¿convierte la página en una HTTPS?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. La VPN configurada mediante *tunneling:*
   a) No utiliza ningún protocolo de seguridad.
   b) Utiliza algún protocolo de seguridad.
   c) El túnel está lleno de antivirus cada cierto tramo.
   d) Ninguna de las tres anteriores.

2. De las siguientes respuestas una o varias son correctas. El protocolo HTTPS:
   a) Está basado en el uso de firewalls en cadena.
   b) Utiliza el cifrado SSL/TTL.
   c) Se aplica principalmente sobre la capa de transporte del modelo OSI.
   d) Constituye la garantía de una conexión segura.

3. ¿Cuál o cuáles de estas políticas no es utilizada por los firewalls?
   a) Expeditiva.
   b) Restrictiva.
   c) Inclusiva.
   d) Permisiva.

4. Una de las siguientes afirmaciones es correcta
   a) DES usa criptografía simétrica.
   b) Las funciones hash usan criptografía asimétrica.
   c) DSA usa criptografía simétrica.
   d) RSA usa criptografía simétrica.

Soluciones: 1b, 2b, 2c, 3a, 3c, 4a

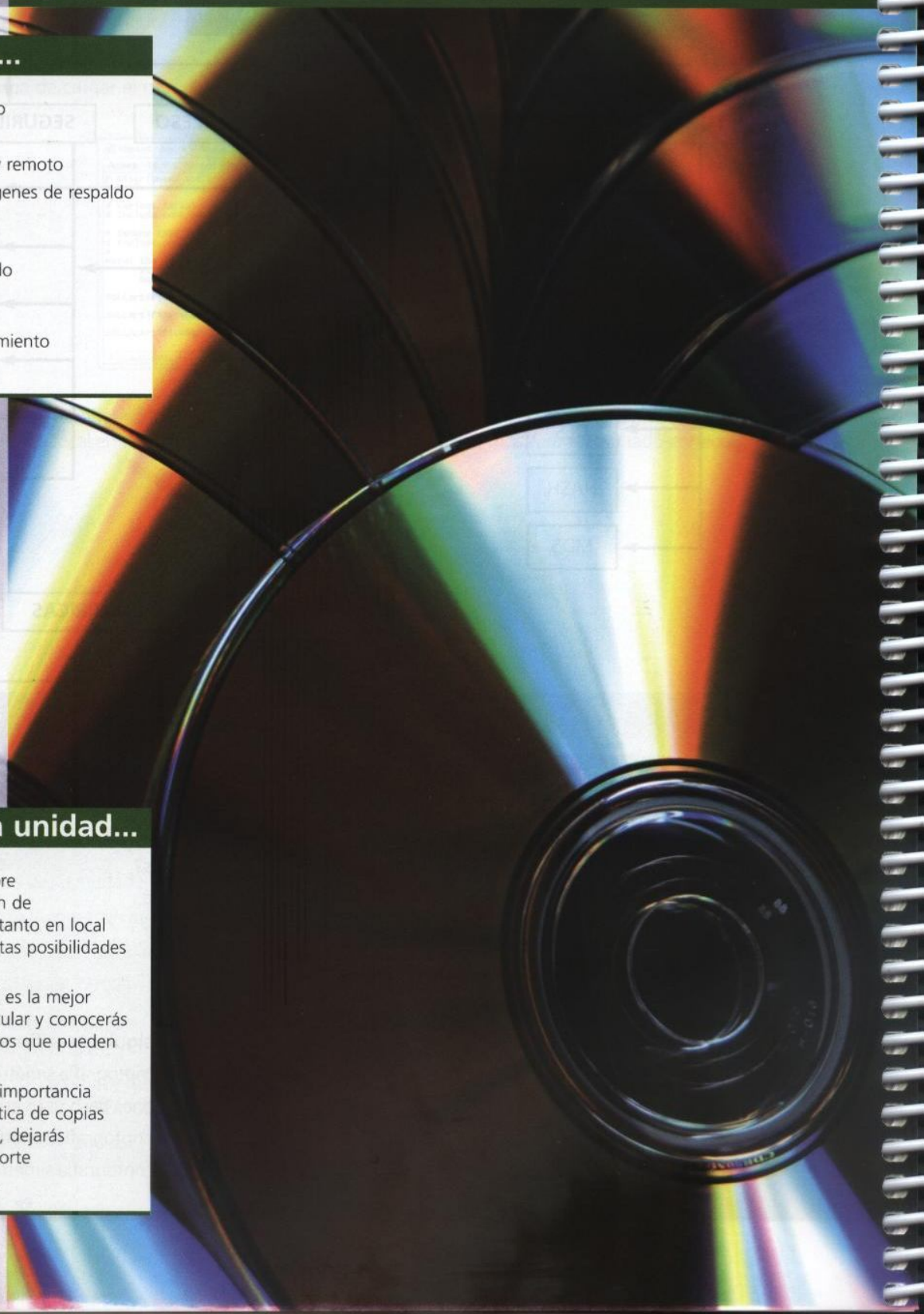
8 Políticas de almacenamiento y resguardo de la información

vamos a conocer...

1. Almacenamiento secundario
2. RAID
3. Almacenamiento extraíble y remoto
4. Copias de seguridad e imágenes de respaldo
5. Documentación en papel

PRÁCTICA **PROFESIONAL**
Almacenamiento y resguardo de la información

MUNDO **LABORAL**
S3, el sistema de almacenamiento de Amazon



y al finalizar esta unidad...

- Sabrás todo lo necesario sobre almacenamiento y protección de la información almacenada, tanto en local como en remoto, y las distintas posibilidades que se tienen.
- Serás capaz de discernir cuál es la mejor opción para cada caso particular y conocerás empresas que prestan servicios que pueden resultarte útiles.
- Tomarás conciencia sobre la importancia de seguir una adecuada política de copias de seguridad y, en lo posible, dejarás a un lado el papel como soporte para almacenar información.

CASO **PRÁCTICO** INICIAL

situación de partida

Tu empresa comienza a tener clientes y los contratos y datos privados aumentan. Necesitas garantizar que nadie tendrá acceso a esos datos o la Agencia de Protección de Datos te sancionará.

Rápidamente reconoces que el papel se pierde y estropea, y además, tienes miedo de que una catástrofe arruine tu trabajo y crees que debe de existir alguna empresa que salve tus datos de alguna forma.

Has contratado a nuevos empleados y compruebas con horror que la forma de usar los equipos y el software de terceros que instalan corrompen los sistemas de archivos y los plagan de virus. Son buenos en su campo pero nefastos en la informática y sus ordenadores necesitarán reparación casi todas las semanas. Después de la charla acerca de los riesgos que traen los virus decides que debes hacer algo.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

El técnico en seguridad informática te responderá en una reunión a las posibles dudas.

1. ¿Cómo puedo aumentar la capacidad de almacenamiento de mis discos duros?
2. ¿Puedo conseguir que los empleados menos hábiles solo vean un disco duro y no tengan que realizar ninguna tarea manual para duplicar datos?
3. ¿Qué tipo de dispositivo debo dar a los empleados para que tengan una copia de seguridad en el cajón del despacho y puedan pasársela entre ellos?
4. ¿Hay alguna forma más práctica de compartir información?
5. ¿Necesito internet en todos los ordenadores?
6. ¿Debería encriptar los datos sensibles?
7. ¿Hay empresas que me garanticen que mis datos están a salvo del fuego en otro lugar?
8. ¿Cómo hago para instalar un sistema operativo y 10 aplicaciones en 15 ordenadores todas las semanas, sin despedir a nadie?
9. En el fondo, ¿necesitamos tanto papel?

1. Almacenamiento secundario

Conocemos como almacenamiento secundario o periféricos de almacenamiento el conjunto de todos los dispositivos y soportes que se encuentren tanto dentro como fuera del ordenador y que constituyen un sistema de almacenamiento permanente de la información.

1.1. Soportes

En la actualidad se dispone de numerosos soportes donde almacenar la información, pero la mayoría puede englobarse dentro de tres categorías según la tecnología que usan.

- **Sistemas magnéticos.** Entrarían en esta categoría los discos duros actuales, los disquetes, aunque prácticamente en desuso, y las cintas magnéticas, un soporte completamente obsoleto.
- **Sistemas ópticos.** Formados principalmente por CD y DVD. Recientemente ha entrado en funcionamiento el Blu Ray, un disco óptico de última generación.
- **Sistemas de almacenamiento sólido.** Se utilizan en tarjetas de memoria flash. Destacan por su reducido tamaño y su principal aplicación es en cámaras de fotos y otros dispositivos ligeros y transportables. Recientemente han comenzado a usarse como disco duro de ordenadores portátiles.

El almacenamiento secundario, a pesar de tener velocidades de transferencia más lentas que el primario, sigue manteniendo altas velocidades y es necesario puesto que ofrece la posibilidad de almacenar grandes cantidades de información a un precio reducido, además de mantener la información guardada sin necesidad de estar permanentemente conectado a la corriente.

Repasando los dispositivos de almacenamiento y el soporte en el que guardan la información, uno de los más antiguos dentro de la historia reciente de la informática es la **disquetera,** que maneja disquetes de **3½" y 5¼".** Presentan bastantes problemas con el paso del tiempo, pudiendo perder información almacenada, además de su escasa capacidad de almacenamiento.

Los **discos duros** están presentes en la mayoría de los ordenadores convencionales. Dejando al margen los externos, cuya conexión puede ser USB, FireWire 800 o eSATA, nos centraremos a continuación en los internos. Aunque la clasificación suele hacerse en función del tipo de conexión que utilice, también puede hablarse de diferencias en lo que respecta al tamaño.

Atendiendo a su tamaño, lo que técnicamente se llama «**factor de forma**», podemos clasificar los discos duros en los tamaños de 8; 5,25; 3,5; 2,5; 1,8; 1 y 0,85 pulgadas, pero los principales en cuanto a frecuencia de compra y uso son los de 3,5; 2,5; 1,8 y 1 pulgadas.

Los discos de 2,5 pulgadas se usan principalmente en ordenadores portátiles.

Almacenamiento en discos duros externos

↑ Disco duro externo de la marca Woxter. Modelo iCUBE 35 USB.

↑ Disco duro externo con conexión USB, de la marca Western Digital, que tiene un tamaño de 2,5" para Windows y Mac. Además de su pequeñísimo tamaño ofrece almacenamiento de hasta 1TB y un software capaz de hacer copias de seguridad continuas sobre el soporte.

saber más

Existen actualmente disqueteras USB para conectar a equipos modernos.

Según su conexión con la placa base, los discos duros pueden ser **IDE, SATA** o **SCSI.**

- **Discos IDE** *(Integrated Disc Electronics)*. Los controladores del disco se encuentran incluidos en el mismo. Hace poco tiempo era el modelo más dominante, pero ha sido desbancado por los modelos SATA. Estos discos presentan una buena relación **calidad-precio** y aun hoy día son muy utilizados.
- **Discos SCSI** *(Small Computer System Interface)*. Son utilizados principalmente en servidores, aunque también se pueden encontrar en ordenadores personales. Su principal característica es la **velocidad** de acceso a los datos y transferencia. Para manejar este tipo de discos es necesario instalar un controlador especial.
- **Discos SATA** *(Serial Advanced Technology Attachment)*. El disco SATA, también llamado Serial ATA, utiliza un bus serie para transmitir los datos y es más rápido que los discos IDE, lo que le ha llevado a ser el estándar más utilizado hoy día.

Los discos duros externos se están usando cada vez más como un método de almacenamiento de bajo nivel (actualmente los más avanzados están en torno a 1 TB, aunque la tecnología aumenta capacidades en breve tiempo), principalmente entre particulares y pequeñas empresas. Normalmente se utilizan para almacenar carpetas con archivos que dejan de tener un uso frecuente y que ocupan demasiado espacio en el disco duro interno del equipo, así como archivos en vídeo y fotografía digital.

En cuanto al tamaño de los discos externos, si bien todos ellos son portátiles, los que llevan este sobrenombre son aquellos de muy pequeño tamaño que son muy cómodos de transportar en viajes o en maletines de trabajo.

Los multimedia tienen además la capacidad de ser reproducidos en monitores de televisión y equipos de música, mediante las conexiones adecuadas, generalmente USB o HDMI; esta última sustituye al euroconector y permite ver imágenes y vídeo en alta definición.

Conectores

↑ Euroconector.

↑ USB.

↑ HDMI.

↑ Conexiones HDMI y eSATA en un equipo portátil.

saber más

El Blu-Ray recibe su nombre de la tecnología de láser azul que utiliza, que permite almacenar más información gracias al aumento de precisión del láser.

Lectores y grabadores de discos ópticos

Los **lectores y grabadores de discos ópticos** son los dispositivos que trabajan con los distintos formatos de discos ópticos y sus variantes.

- **CD.** Disponible en distintas versiones, CD-ROM, CD-R, que se corresponde con un CD-ROM grabable y CD-RW, que es un CR-ROM regrabable.
- **DVD.** Al igual que el CD-ROM, el DVD es un disco óptico aunque de mayor capacidad y calidad. Resiste mejor el paso del tiempo y las condiciones climáticas. Existen distintos tipos de DVD: DVD±R, que es el DVD grabable y el DVD±RW, que es el DVD regrabable.
- **Blu-Ray.** Es el formato óptico de última generación, con una capacidad de almacenamiento y calidad muy superior a las del CD-ROM o el DVD.

↑ Evolución del CD al Blu-Ray de Sony. En un disco óptico de similares dimensiones se pasa de 700 MB de almacenamiento a 50 GB.

Por último, los **lectores de tarjetas** son los dispositivos encargados de leer **las tarjetas flash.** Las tarjetas flash ofrecen un bajo consumo, resistencia a golpes y, además, son silenciosas. Su precio en el mercado varía según su capacidad, pero por norma general el precio por MB es más elevado que el de un disco duro de los estudiados anteriormente y, además, no ofrecen capacidades de almacenamiento tan elevadas.

Existen lectores de tarjetas multiformato y lectores de discos ópticos que incluyen ranura para lectura de tarjetas.

ACTIVIDADES

1. ¿De qué tipo de almacenamiento secundario dispones en casa?
2. ¿Qué sueles guardar en cada tipo de soporte?
3. ¿Qué diferencia hay entre los dos tipos de disquetes disponibles?
4. Comprueba en casa qué tipo de disco duro usa el ordenador. ¿Cómo lo has sabido?
5. ¿Cuál crees que es el principal problema por el que el Blu-Ray no termina de integrarse en el mercado?
6. ¿Tiene tu PC disquetera? ¿Para qué crees que podría resultar útil?

2. RAID

En unidades anteriores ya hemos apuntado lo que es un RAID (*Redundant Array of Inexpensive Disks*), **grupo redundante de discos independientes**, y que se usan como una forma más de seguridad en hardware y para garantizar la protección de los datos almacenados.

En los sistemas RAID se emplean varios discos duros, en los que una vez configurados adecuadamente, se **distribuyen** y **replican** los datos que se almacenan.

En un principio, la tecnología RAID se usaba para conseguir mayores capacidades de almacenamiento y rendimiento a un menor coste, ya que se implementaba sobre discos de bajo precio.

Los RAID son utilizados principalmente en servidores u ordenadores personales cuyo uso requiere de un gran espacio de almacenamiento. A un nivel básico, el RAID reúne varios discos duros físicos en una misma unidad lógica, es decir, a los ojos del sistema operativo, nuestro equipo contará con un solo disco duro.

Existen diversas implementaciones de RAID, cada una con un propósito específico, y se clasifican siguiendo niveles.

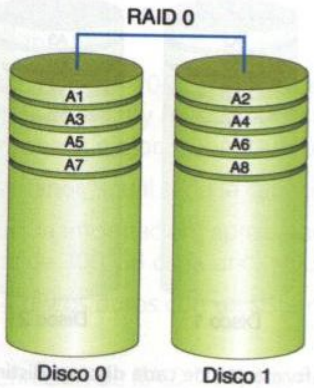
Las implementaciones pueden ser tanto por **hardware** como mediante **software,** y además existen alternativas que combinan ambas soluciones. En caso de que el control sea por hardware, será necesario disponer de una **controladora** integrada en la placa base o bien en una **tarjeta de expansión** independiente. Si la implementación es mediante software, será el propio sistema operativo el que gestione el RAID a través de una controladora convencional.

Atendiendo a los niveles de RAID, los más utilizados son RAID 0, RAID 1 y RAID 5.

- **RAID 0.** Este nivel, en según qué definiciones, no está considerado un RAID ya que no ofrece redundancia. La información almacenada se reparte entre todos los discos disponibles, y se puede leer y escribir simultáneamente en ellos. Esto ofrece un considerable aumento en la velocidad, aunque no garantiza una mayor seguridad ya que en caso de fallar un disco se pierde la información almacenada.

saber más

No se puede decir que un nivel de RAI sea mejor que otro. La elección de uno u otro nivel de RAI dependerá de las necesidades de la persona o empresa, en cuanto a capacidad de almacenamiento, coste, velocidad, seguridad, etc.

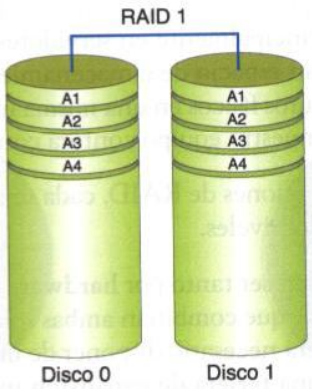


↑ Diagrama de un RAID 0. Hay dos discos pero la información que contienen no es la misma.

- **RAID 1.** Este RAID crea una copia de los datos almacenados en uno de los discos en el otro. La redundancia es total y garantiza la disponibilidad de la información en caso de fallo de uno de los discos. Este tipo de configuraciones reciben el nombre de **espejo,** y son muy utilizadas en servidores donde no prima la necesidad de espacio sino la **velocidad de lectura,** ya que se puede acceder a datos distintos en discos diferentes.

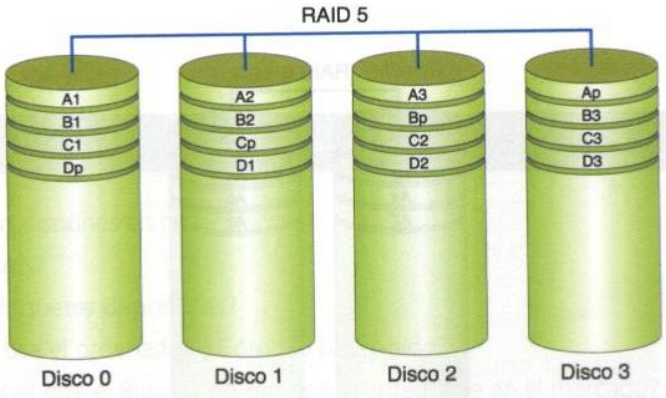
  Para perder la información almacenada en un RAID 1 tendría que darse el caso de que fallaran todos los discos de que dispone.

  La capacidad de almacenamiento no se ve aumentada y será igual al tamaño del más pequeño de los discos que formen el RAID.



↑ Diagrama de un RAID 1. La información se va almacenando en los dos discos a la vez, de modo que hay redundancia completa.

- **RAID 5.** Los RAID 5 cuentan con una gran popularidad gracias a su configuración que permite tanto redundancia como aumento de la capacidad de almacenamiento. Para construir este sistema serán necesarios un mínimo de 3 discos. En dos de ellos se almacenará la información de forma similar al RAID 0 explicado anteriormente. En el otro disco se guarda información de control, de forma que si falla alguno de los dos, no se pierde la información como en RAID 0, sino que esta se reconstruye a partir de lo guardado en el tercer disco.



↑ Diagrama de un RAID 5. La información de cada disco es distinta a la de otro, pero cada disco tiene un bloque de paridad –señalado con el subíndice «p»– que sirve para reconstruir sectores erróneos cuando se producen errores de redundancia.

Resulta especialmente interesante, además, el **RAID 0+1,** que combina la tecnología del RAID 0 con la del RAID 1. Básicamente, del espacio disponible, que será de un mínimo de cuatro discos, se obtienen dos RAID 0 y con estos dos se forman un RAID 1 que duplica la información para garantizar redundancia.

Además de las implementaciones mencionadas, existen otras versiones y siempre será conveniente revisar cuál es la que se adapta mejor a nuestras necesidades. El **RAID Z,** por ejemplo, es una implementación propietaria para el sistema de ficheros ZFS de Sun Microsystems y presenta un sistema de redundancia parecido al RAID 5.

saber más

En la propia web de Sun Microsystems dan información sobre el RAID-Z. Amplía tus conocimientos en el siguiente enlace:

http://docs.sun.com/app/docs/doc/820-2314/gamtu?l=es&a=view

ACTIVIDADES

7. ¿Qué significan las siglas RAID?

8. ¿Cuál es el uso principal de los RAID?

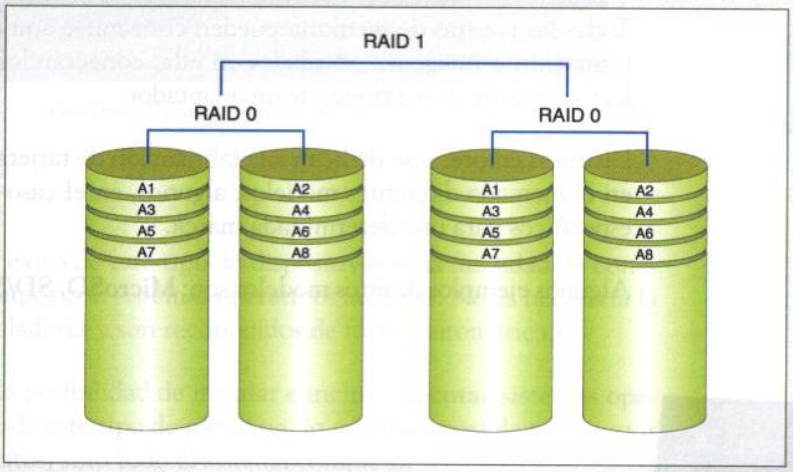
9. ¿Dónde suelen usarse con mayor frecuencia?

10. ¿Cuántos tipos de implementaciones existen y cuáles son?

11. ¿Cuáles son los niveles de RAID más utilizados?

12. ¿Por qué el RAID 0 a veces no se considera un RAID propiamente dicho?

13. ¿A qué nivel de RAID crees que corresponde este diagrama?



14. Usa internet para buscar más tipos de RAID. Selecciona uno, no explicado en esta unidad, que te resulte particularmente interesante.

15. Dispones de un disco duro de 100 GB y otro de 200 GB. Has diseñado un software que ocupa 50 MB y tiene una gran difusión por internet y no puedes permitirte perderlo. Instalas un servidor con un RAID para que la velocidad de lectura sea la mejor. ¿Qué RAID usarías?

16. Según el ejercicio anterior, ¿cuál sería la capacidad máxima de almacenamiento de tu servidor?

17. En casa guardas mucha información, aproximadamente 500 GB, pero esa información no es vital para ti. Dispones de dos discos de 300 GB cada uno. ¿Qué RAID montarías?

18. Si disponemos de 4 discos duros con un sistema de ficheros ZFS, ¿cuál será el mejor RAID que podemos implementar?

19. Atendiendo a la definición de RAID 0+1, ¿qué crees que es un RAID 1+0?

3. Almacenamiento extraíble y remoto

3.1. Almacenamiento extraíble

Ya adelantamos algo sobre almacenamiento extraíble cuando hablamos de **memorias flash,** y es que esta es la tecnología que se implementa en este tipo de dispositivos.

Se trata de hacer portátil, a un nivel físico, nuestra información. Usando los dispositivos adecuados podremos transportar de un equipo a otro los datos que usamos habitualmente y trabajar con ellos, garantizando tenerlos siempre actualizados.

Se ha popularizado mucho, además, el uso de estos dispositivos como **copias de seguridad** y para el intercambio de archivos.

Podemos asumir que los tres principales **dispositivos** utilizados como almacenamiento extraíble son las **tarjetas de memoria, memorias USB** y las **PC Card.**

- **Tarjetas de memoria.** Existen numerosos tipos de tarjetas de memoria, y la mayoría de ellas tienen aplicación como memoria para cámaras digitales, teléfonos o videoconsolas.

  Todas las tarjetas de memoria pueden conectarse a un PC para recoger la información o imágenes guardadas en ella, conectándolas directamente en un lector de tarjetas o a través de un adaptador.

  Distintas empresas se dedican a la fabricación de tarjetas de memoria y existen en el mercado diferentes modelos, algunos, en el caso de las cámaras de foto, específicos para una determinada marca.

  Algunos ejemplos de estos modelos son: **MicroSD, SD/MMC** y **CompactFlash.**

↑ Antigua tarjeta CompactFlash de 128 MB.

↑ Tarjetas de memoria de 8 y 4 GB de la marca SanDisk.

- **Memorias USB.** El nombre de USB procede de las siglas inglesas de **Universal Serial Bus.** En España, este tipo de dispositivos se conocen por su nombre inglés **Pen Drive,** el español **lápiz USB** o simplemente **USB,** aunque el uso de este último no sería técnicamente correcto.

  Una de las principales características de este dispositivo es su resistencia, lo que lo hace especialmente apto para el transporte de datos sin necesidad de prestar una especial atención al cuidado de este.

  Se alimenta sin necesidad de baterías, gracias a que se conecta a través de un bus USB y los tamaños de almacenamiento más usados actualmente comprenden desde 1 GB hasta 256 GB, dando un salto cuantitativo de precio a partir de los 16 GB.

↑ Pen Drive DataTraveler de 16 GB.

  Una de las claves de éxito de este tipo de dispositivos es la facilidad de conexión a los nuevos equipos con sistemas operativos actuales. No es necesaria la instalación de controladores y son reconocidos de forma automática.

  Actualmente existe la posibilidad de instalar e incluso **ejecutar sistemas operativos** completos desde este tipo de memoria, lo que hace posible transportar consigo no solo los datos, sino todo el sistema completo.

  Dado que hablamos de seguridad, debemos tener en cuenta que este tipo de memoria supone un sistema barato de almacenamiento para datos, pero su reducido tamaño hace que sea fácil perderlos, además de posibles **averías irreparables** sin motivos aparentes.

  También son frecuentes las infecciones por **virus** en este tipo de dispositivos dada la facilidad de conexión en otros equipos y el poco control que se tiene sobre la autoejecución de unidades extraíbles en algunos sistemas operativos de Microsoft, lo que puede provocar la pérdida de datos.

  Para implementaciones futuras de estos dispositivos se espera la utilización del USB 3.0, lo que supondrá un enorme avance en la velocidad de transferencia, pasando de los actuales 480 MB/s hasta los 4,8 GB/s.

saber más

En España es habitual llamar «pincho» a la memoria USB. ¿Tú qué nombre le das?

↑ Logotipo de una conexión USB.

↑ Disco duro PCMCIA Aska HD32F.

↑ *Collage* de tarjetas PC-Card de distintas marcas.

- **PC Card.** Las PC Card, en un principio llamadas PCMCIA (*Personal Computer Memory Card International Association*), están diseñadas específicamente para ordenadores portátiles.

  Puede que su uso principal fuera en un principio para expandir la memoria, pero en la actualidad cuentan con numerosos usos, desde disco duro hasta sintonizadores de televisión.

  El uso de las PC Card como memorias de almacenamiento extraíbles ha mejorado mucho desde su lanzamiento, aunque actualmente se encuentran prácticamente obsoletas. Usan tecnología flash y suelen tener una capacidad mayor que los *pen drive*.

3.2. Almacenamiento remoto

La tecnología avanza, y junto a la tecnología nuestra concepción de la informática debe evolucionar.

Actualmente, las empresas que desean garantizar la seguridad de sus datos y no cuentan con servidores externos propios, comienzan a usar la llamada ***cloud computing,*** en español **computación en la nube** o **nube de cómputo,** o una red de servicios accesibles a través de internet. Uno de esos servicios es el almacenamiento de la información.

saber más

Google ha revolucionado el concepto de *Cloud computing* con su sistema operativo «Google Chrome OS». Google Apps y Google Docs se basan en esta tendencia tecnológica.

Mediante la nube de cómputo, todos los programas y datos que manejamos están almacenados permanentemente en **servidores de internet,** normalmente situados en grandes centros de datos.

Usando este tipo de servicios garantizamos la disponibilidad de todos los datos en todas la máquinas que deseemos, con una **actualización inmediata** de los cambios que realicemos en cualquiera de los ordenadores. Normalmente se dispone de un acceso y control web de los datos almacenados.

Este tipo de almacenamiento favorece el denominado teletrabajo o trabajo a distancia, así como el desarrollo del trabajo en equipo ya que los cambios realizados serán actualizados prácticamente en tiempo real y no se producirán pérdidas de las copias de seguridad.

Para contar con este tipo de almacenamiento es necesaria una conexión de **banda ancha** a internet.

Aún existe reticencia por parte de los usuarios a usar este tipo de servicios, ya que se teme una pérdida de confidencialidad de los datos o un posible fallo en el servicio, pero la realidad es que muchos servicios Web 2.0 se apoyan en el *cloud computing* y se prevé que la Web 3.0 incrementará su uso, con lo que el futuro del almacenamiento en la informática tiene mucho que ver con este concepto.

Se deberá buscar un adecuado proveedor del servicio, que ofrezca las garantías necesarias y las condiciones de uso nos sean favorables, teniendo en cuenta que si dejamos nuestros datos en servidores de terceros, estos terceros deben ser confiables.

Actualmente hay multitud de empresas que ofrecen estos servicios, algunas tienen versiones gratuitas para usuarios particulares con una capacidad de almacenamiento muy limitada (generalmente entre 2 y 5 GB) y a veces temporal, si bien la mayoría ofrece muy buenas soluciones de almacenamiento para empresas.

Algunos ejemplos son **ADrive,** con 50 GB de almacenamiento para la versión gratuita y hasta 1 TB en la versión de pago, **Dropbox,** con 2 GB gratuitos y todas las herramientas de sincronización automática y guardado de *backups*, y **Amazon S3,** de la prestigiosa compañía Amazon, que lanza este servicio en sus servidores, preparados para atender una elevada demanda en un momento preciso, pero infrautilizados la mayoría del tiempo.

Las webs de estas compañías son:

- http://www.adrive.com
- http://www.dropbox.com
- http://aws.amazon.com/s3

↑ Algunas empresas que ofrecen servicios de copia de seguridad mediante pago o gratuitos.

ACTIVIDADES

20. ¿Cuál es el principal objetivo de los dispositivos de almacenamiento extraíble?

21. Nombra los tres tipos de dispositivos de almacenamiento extraíble más utilizados.

22. ¿Qué es una tarjeta MicroSD?

23. Responde verdadero o falso. Todas las tarjetas de memoria sirven para todas las cámaras y videoconsolas.

24. ¿Qué significan las siglas USB?

25. Responde verdadero o falso. Para que el sistema operativo reconozca el *pen drive,* se deben instalar controladores específicos de cada dispositivo.

26. ¿Conoces algún sistema operativo que funcione desde un *pen drive?* ¿Cuál?

27. Busca en internet algún dispositivo PCMCIA que no sea un disco duro y comenta sus características con tus compañeros.

28. ¿Qué es el *cloud computing?*

29. Nombra dos ventajas de la computación en nube.

30. Busca una pareja de trabajo. Registraros juntos en la web de Dropbox.com y descargad el software en su versión gratuita. Conectad ambos equipos y cread una carpeta para compartir que no contenga datos importantes. Probad las funciones y comprobad que la actualización es inmediata y la sincronización y guardado de *backups* es automática.

31. En Dropbox, ¿qué ocurre si creas una carpeta y dentro documento nuevo?

32. ¿Qué sucede al borrar ese archivo en uno de los ordenadores?

33. ¿Sabrías restaurar una versión anterior de un documento? ¿Cómo?

4. Copias de seguridad e imágenes de respaldo

saber más

Aunque las empresas son las que más realizan copias de seguridad de su información, debería ser también práctica común entre particulares.

Toda empresa que maneje sistemas informáticos y almacene datos debe seguir una estricta política de copias de seguridad y de creaciones de imágenes de respaldo.

Las copias de seguridad son duplicados de toda la información o parte de ella que se desee conservar y almacenar en algún medio independiente del que se encuentran normalmente, ya sea a través de internet, en otro disco duro o en un medio extraíble.

En caso de que se produjera un fallo en el sistema o un borrado accidental de la información, si se ha creado copia de seguridad no habrá problemas para restaurar la información.

Hay que tener en cuenta, además, que en nuestro país, la Agencia Española de Protección de Datos obliga a las empresas a realizar copias de seguridad de los datos que poseen.

No se producen solamente pérdidas de datos, sino también de las aplicaciones y configuraciones de los equipos; por ello existen las imágenes de respaldo, donde se guarda toda la información del disco duro, incluyendo el sistema operativo, para que al restaurarse todo siga funcionando como antes del incidente que hizo necesario utilizar la imagen.

4.1. Tipos de copias de seguridad

Cualquier empresa que realice copias de seguridad debe seguir una **estricta política** a la hora de **almacenar** sus copias, ya que de lo contrario podría darse el caso de restaurar una versión muy antigua, produciéndose pérdidas importantes de información.

Cuando nuestros datos se almacenen de una forma desorganizada, o con la mínima información para saber al momento qué se ha copiado y cuándo, diremos que usamos un modelo **desestructurado.**

Si se realiza una copia de todos los archivos cada cierto tiempo, estamos hablando de copia **completa o total.** Es el sistema más recomendable cuando el volumen de datos guardados no es demasiado alto, por ejemplo, inferior a 100 MB.

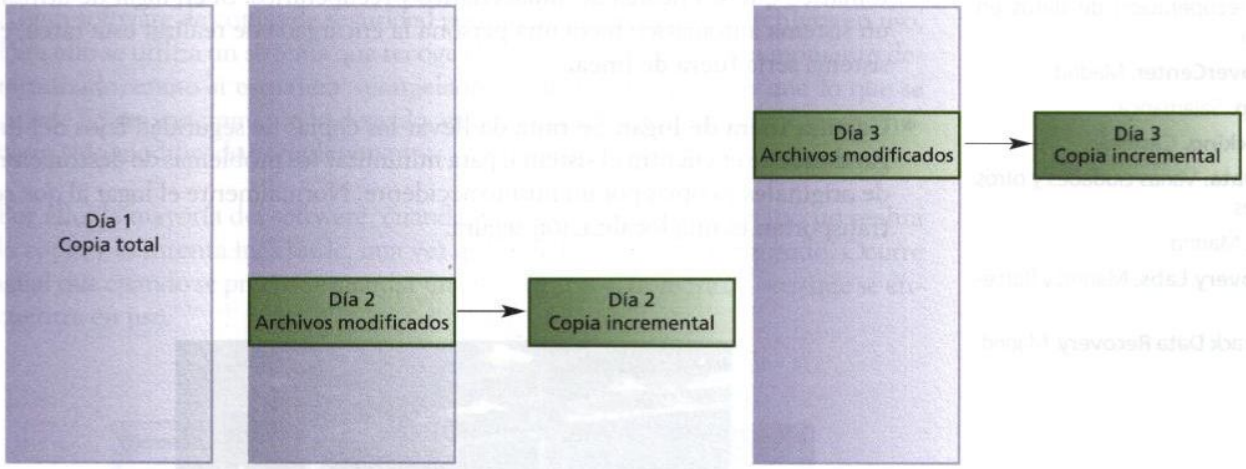
En lugar de hacer una copia completa cada vez, es posible hacer una primera y luego, cada cierto tiempo que se determine, copia únicamente de los archivos que se han modificado y a continuación cada día –o cada cierto tiempo– llevar a cabo una nueva copia de todo lo que se ha modificado desde la última vez. Este tipo de copia es **incremental** y para restaurarla se requiere la copia total y todas y cada una de las copias incrementales que se hayan ido realizando.

También puede decidirse hacer una copia **diferencial.** En este caso se ejecuta una primera copia total, y a continuación, cada cierto tiempo, se hará una copia de los archivos modificados desde la copia completa. Cada copia diferencial

se superpone a la anterior, de modo que para restaurar el sistema son necesarias la copia completa y la copia diferencial. Pueden comprenderse mejor los conceptos de copia incremental y diferencial en las imágenes que aparecen a continuación.

Las empresas y organizaciones con mucho volumen de datos y con una buena gestión de copias de seguridad, suelen optar por un sistema mixto

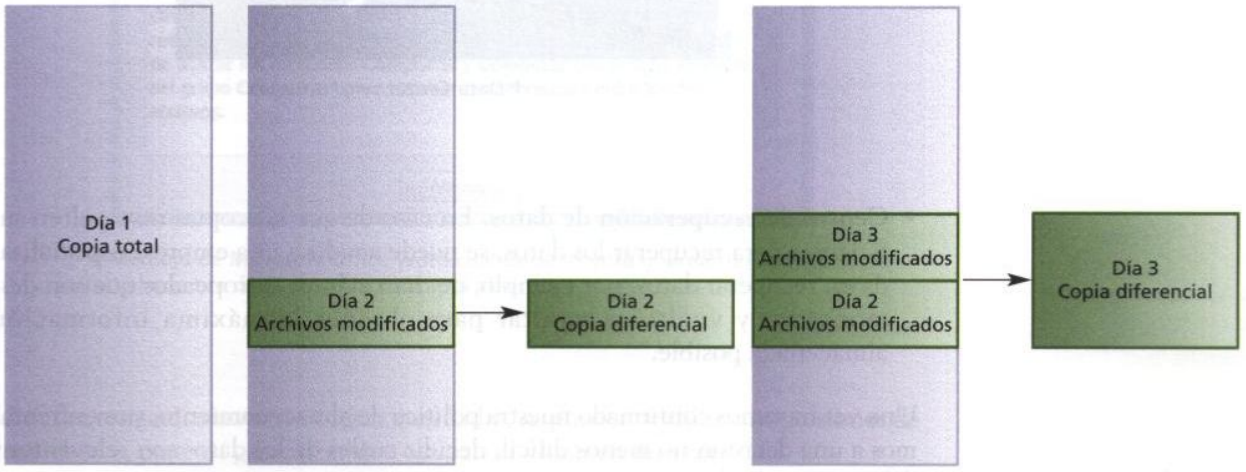
Un modelo de copias de seguridad con **protección continua de datos** es aquel que no realiza copias cada cierto tiempo, sino inmediatamente después de detectar un cambio en el fichero, consiguiendo que se reduzcan al mínimo los daños en caso de fallo. Puede hacerse tanto de forma incremental como diferencial.



↑ Cada día (o semana o mes, según se establezca) se compara **lo que hay ese día con lo que había la última vez que se hizo una copia incremental** y se realiza una nueva copia incremental con esa diferencia encontrada.

Restaurar copia: la restauración comprende la copia total + todas las copias incrementales que se hayan realizado:

$$R = C_T + I_1 + I_2 + \ldots + I_N$$



↑ Cada día (o cada semana o mes, según se tenga planificado), **se comparará lo que hay ese día con la copia total** que se hizo al principio. Esa diferencia se guarda como copia diferencial.

Restaurar copia: la restauración comprende la copia total + la última copia diferencial, ya que contiene todas las modificaciones que se han realizado desde la copia completa:

$$R = C_T + C_D$$

Ya hemos aprendido diferentes formas de ordenar y almacenar las copias de seguridad, pero también es necesario saber **administrar** ese almacén de datos.

- **En línea.** Las copias de seguridad se almacenan en el propio disco o en un RAID. Es uno de los sistemas más utilizados aunque cuenta con grandes inconvenientes, como que la localización de los archivos de respaldo es próxima a los originales, por lo que una destrucción de estos puede implicar destrucciones de las copias, bien sea por un desastre o por la acción de un virus en el sistema.
- **Cerca de línea.** En este caso los datos de respaldo se almacenan fuera del propio sistema al que se le realiza las copias, y son transportados por un sistema automático que se encarga de almacenarlos y recuperarlos. Si en lugar de utilizar un sistema automático fuera una persona la encargada de realizar esta tarea, el sistema sería **fuera de línea.**
- **Cámara fuera de lugar.** Se trata de llevar las copias de seguridad lejos del lugar donde se encuentra el sistema, para minimizar los problemas de destrucción de originales y copias por un mismo accidente. Normalmente el lugar al que se transportan es una localización segura.

↑ *Data Center.*

- **Centro de recuperación de datos.** En caso de que las copias no resulten suficientes para recuperar los datos, se puede acudir a una empresa especializada en recuperar datos, por ejemplo, de discos duros estropeados que son desmontados y vueltos a montar para obtener la máxima información almacenada posible.

Una vez hayamos confirmado nuestra política de almacenamiento, nos enfrentamos a una decisión no menos difícil, decidir cuáles de los datos son relevantes y deben ser incluidos en la copia.

Como norma general debemos saber que hay que guardar copias de seguridad de aquellos ficheros que nos sería imposible recuperar, o supondrían un fuerte impacto sobre la empresa en caso de perderlos.

saber más

Algunas empresas especializadas en la recuperación de datos en España:

- **RecoverCenter.** Madrid.
- **Adap.** Salamanca.
- **ITBacking.** Castellón.
- **OnData.** Varias ciudades y otros países.
- **RSE.** Madrid
- **Recovery Labs.** Madrid y Barcelona.
- **OnTrack Data Recovery.** Madrid.

saber más

Ante la duda sobre la relevancia de un archivo, se debe tomar una actitud conservadora y crear una copia de seguridad.

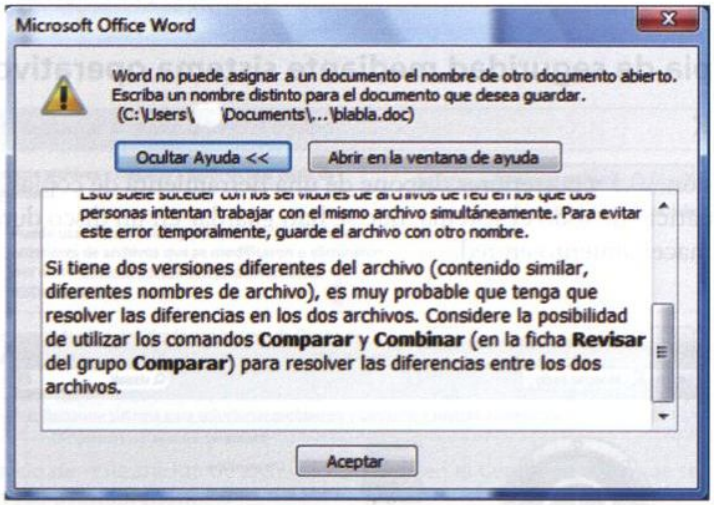
4.2. Copia de seguridad mediante software

También debemos guardar en las nuevas copias posteriores solo aquellos datos que hayan sido modificados con respecto a alguna copia anterior, ya que de otra forma podríamos alcanzar la capacidad máxima de almacenamiento de los equipos.

La mejor forma de gestionar las copias de seguridad es utilizando un **software específico.** Cada software tendrá unas características propias, aunque la mayoría comparte unos rasgos principales, como son el **rastreo** en busca de **ficheros modificados,** que son detectados basándose en la última fecha de modificación, o por un bit que indica si el fichero ha sido modificado.

Algún software de copias de seguridad permite realizar copias de archivos en uso. Para ello se utiliza un sistema que recoge el estado del fichero en un momento determinado, como si estuviera «congelado». Esto puede provocar que lo que se guarde no sea exactamente lo deseado, ya que es posible que el archivo aún no hubiera sido modificado completamente.

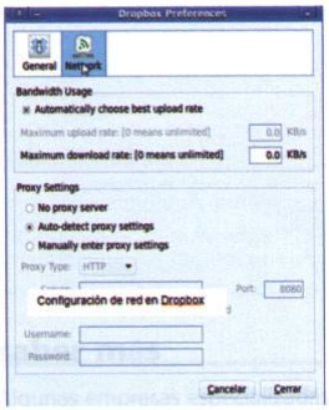
Por ello, la mayoría del software, cuando encuentra un archivo en uso no realiza la copia y lo intenta más tarde, una vez que el fichero no está bloqueado. Ocurre igual que cuando se pretende guardar un archivo con el nombre de otro que se encuentra en uso.



↑ Mensaje de Microsoft Office Word cuando se intenta guardar un archivo con el nombre de otro archivo que está abierto.

Una vez tengamos nuestras copias guardadas, se pueden realizar compresiones de los ficheros, para así garantizar que ocupan el volumen mínimo.

Tanto si usamos un software que automatice la tarea como si se realiza de forma manual, deberemos tener en cuenta el **horario,** ya que realizar copias de archivos consume recursos que no estarán disponibles durante un uso normal del equipo.



↑ Configuración de red en Dropbox.

Las tareas de copia de archivos deberán ser realizadas con permisos de **administrador** para poder acceder a los archivos de todos los usuarios del equipo sin restricciones, ya que de otra manera podríamos dejar información importante sin copiar.

Una vez realizadas todas las copias podremos hacer **verificaciones** mediante *hashes*, estudiados anteriormente, u otros mecanismos que garanticen que la copia se corresponde fielmente con la información original.

Una vez más, es conveniente recordar lo estudiado hasta el momento, ya que será fundamental realizar **duplicados** de nuestras copias de seguridad y, según el lugar donde se almacenen, sería conveniente realizar un **cifrado** sobre los datos de las copias.

↑ Página de descarga de Acronis, incluida la versión *Trial*.

4.3. Copia de seguridad mediante sistema operativo

Mac OS X

En su versión 10.5 y posteriores dispone de una herramienta de copias de seguridad automáticas de todo el sistema, que se han guardar en un disco duro distinto o en almacenamiento en red.

↑ Inicio de copia de seguridad en Time Machine. «Copia más reciente» da error cuando no se ha conectado al equipo el volumen de copia de seguridad.

saber más

Otros programas de creación de backups locales que se pueden descargar con licencia gratis:

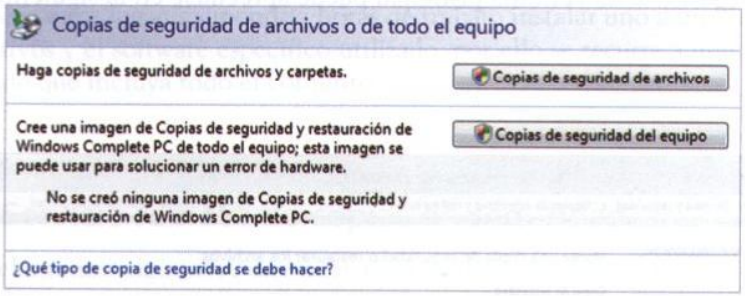
- **AutoVer.** Copias con versión de cambios.
- **Fab's AutoBackup.** Archivos y correo electrónico.
- **Macrium Reflect.** Copia local o en red.
- **JaBack.** Con copia programable.
- **EASEUS Todo Backup.** Imágenes de disco bit a bit.
- **Comodo Backup.** Modo local y remoto.
- **USB Image Tool.** Crea imágenes de unidades flash USB.

Linux

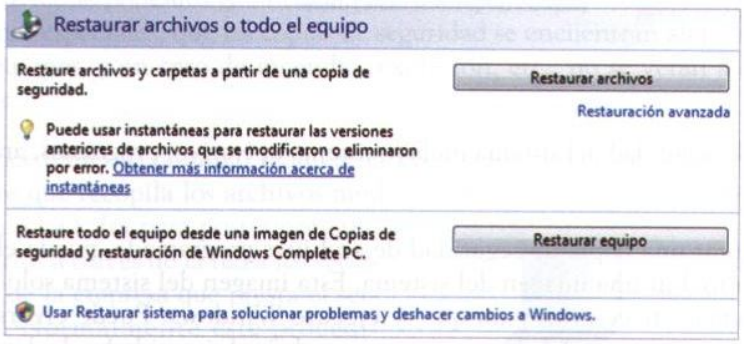
Las copias de seguridad de ficheros se pueden realizar mediante comandos del sistema operativo o mediante las herramientas Tar, Gzip o Bzip, que producen copias comprimidas que pueden enviarse a un almacenamiento remoto vía FTP o por correo electrónico.

Windows Vista

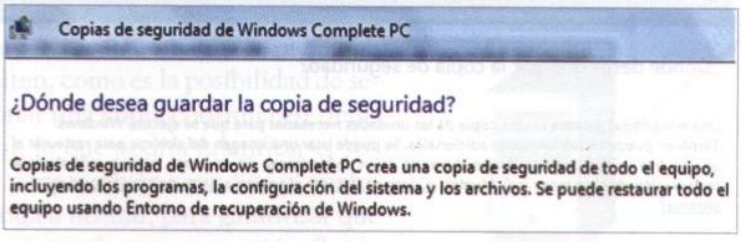
Se accede mediante el Panel de control al Centro de copias de seguridad y restauración, que ofrece la copia de seguridad de archivos y de todo el equipo, así como la restauración de copias realizadas con anterioridad.



↑ Inicio de copia de seguridad del sistema o de archivos en el Centro de copias de seguridad y restauración.



↑ Inicio de restauración de archivos o sistema en el Centro de copias de seguridad y restauración.



↑ Inicio de Windows Complete PC para copia de seguridad del sistema. Se puede optar por enviarla a un disco duro o a uno o varios DVD.

saber más

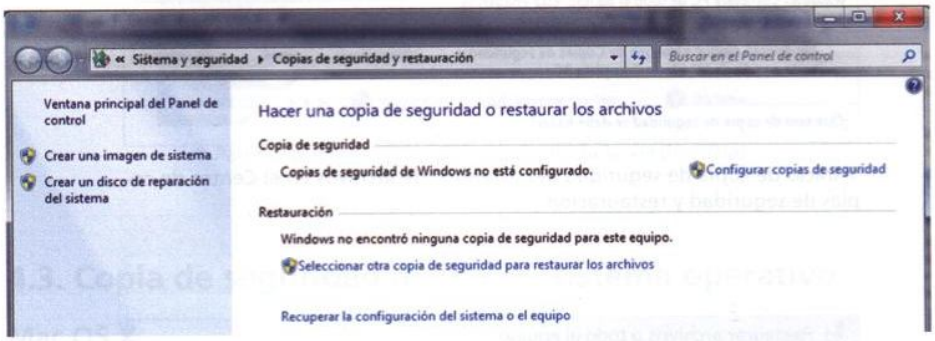
Quien no esté muy familiarizado con Linux para usar las herramientas del sistema, puede utilizar programas comerciales para Linux (BRU, Backup Professional, PCParachute...) o no comerciales (Amanda, Burt, AfBackup...).

Windows 7

Se accede a **Copias de seguridad y restauración** desde el **Panel de control → Sistema y seguridad.**

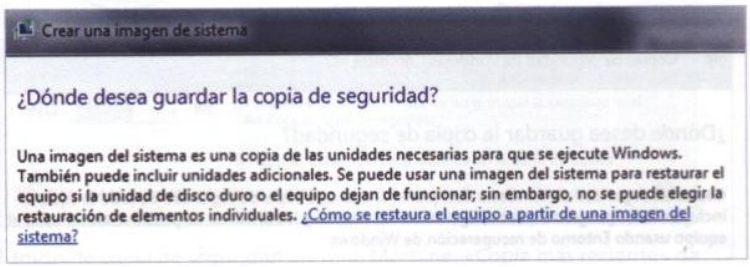
Puede optarse por configurar las copias de seguridad de archivos contenidos en el equipo, por realizar una imagen del sistema o por crear un disco de recuperación del sistema.

Una vez configurada la copia de seguridad de archivos, las copias se crean periódicamente de forma predeterminada. Puede cambiarse la programación y realizar manualmente una copia de seguridad en cualquier momento. Después de configurar Copias de seguridad de Windows, el sistema operativo realiza un seguimiento de las carpetas y archivos nuevos o modificados y los agrega a la copia de seguridad. La ventana principal puede apreciarse en la siguiente imagen.



La copia de seguridad del sistema incluye sistema operativo, programas, archivos y configuración.

Al configurar una copia de seguridad de archivos programada, puede elegirse si se desea incluir una imagen del sistema. Esta imagen del sistema solo incluye las unidades necesarias para que se ejecute Windows. Puede crearse manualmente una imagen del sistema si se pretende incluir unidades de datos adicionales.



↑ Inicio de creación de imagen del sistema. Se puede optar, como destino, un disco duro o uno o varios DVD.

4.4. Imágenes de respaldo

Son copias de seguridad de **todo el sistema.** En las imágenes no solo se copian los archivos modificados últimamente, sino todo el contenido del disco duro, al que se le hace una «fotografía», de ahí su nombre de imagen, y se almacena para posteriormente ser repuesta en caso de fallo.

Las imágenes de respaldo se realizan cuando todo el sistema funciona perfectamente, y de ese modo, en caso de que comience a fallar por infección de virus o algún problema similar, se pueda utilizar la imagen para restaurar el equipo.

Las imágenes de respaldo son muy utilizadas en lugares donde hay multitud de equipos susceptibles de fallar con frecuencia, como centros educativos, locutorios, etc.

En todos estos lugares supondría horas de trabajo instalar uno a uno los sistemas operativos y el software específico utilizado, por ello se recurre a una imagen de respaldo que incluya todo el conjunto.

saber más

La mayoría de sistemas operativos modernos traen la opción de crear una imagen de respaldo y un punto de restauración.

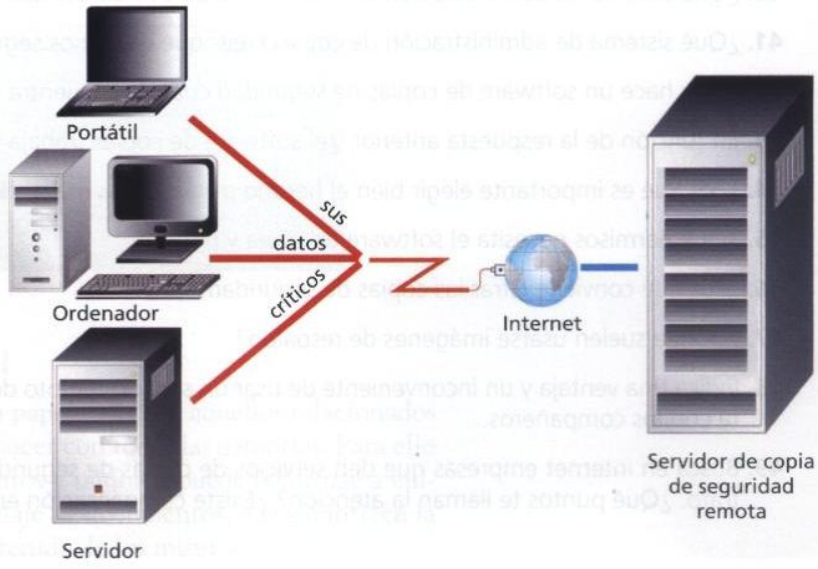
4.5. Servicio remoto de copias de seguridad

Ya adelantamos algo sobre este aspecto al hablar sobre almacenamiento remoto.

Siguiendo esa misma línea, si nuestro equipo está conectado a la red podemos contratar un servicio remoto que gestione todo lo relacionado con las copias de seguridad.

De este modo podemos garantizar, a un módico precio y sin necesidad de instalaciones especiales, que las copias de seguridad se encuentran alejadas de nuestros equipos, y en caso de incendio, explosión, etc., no se verán afectadas las copias.

El procedimiento habitual requiere la instalación de un software en el equipo cliente que recopila los archivos modificados que van a ser salvados, los comprime y los cifra para posteriormente enviarlos a través de la red a los servidores de la empresa que presta el servicio. Normalmente este procedimiento se ejecutará una vez al día, y en un horario que no interfiera con el uso normal del equipo, aunque estos parámetros son configurables en la mayoría de proveedores remotos.



Hay algunas características típicas que se repiten, como es la posibilidad de seleccionar una copia continua en tiempo real, lo que podría ralentizar el sistema, pero también se indica el ancho de banda a utilizar, para garantizar que siga existiendo comunicación fluida para el resto de aplicaciones instaladas.

La mayoría de proveedores ofrecen servicios que varían según lo contratado. Existen tarifas en función de los equipos de los que se salven datos o en función del volumen guardado. Es habitual, además, encontrar limitaciones en el número de copias de un mismo archivo, o mínimo en la antigüedad máxima permitida de un fichero que ya ha sido modificado.

Al contratar un servicio remoto de copias de seguridad se debe tener en cuenta que nuestros datos, al igual que ocurría en el almacenamiento remoto mediante *cloud computing*, quedan en manos de **terceras empresas.** Por ello conviene realizar una buena elección de una empresa **estable** que garantice la seguridad de los datos, ya que si se da el cierre de dicha empresa podría resultar imposible la recuperación de las copias.

saber más

En la mayoría de ocasiones, las compensaciones son de tipo económico o prestación de servicios gratuitos, aunque a veces los conflictos acaban en los tribunales.

Debemos asegurar, mediante **contrato,** que si se produce un fallo o pérdida de las copias de seguridad por parte del proveedor, debe realizarse una **indemnización** del tipo pactado, para compensar, en la medida de lo posible, el daño causado.

ACTIVIDADES

34. ¿En qué consiste una copia de seguridad?

35. ¿Para qué sirven las copias de seguridad?

36. Amplía tus conocimientos buscando información sobre la Agencia Española de Protección de Datos. Comenta lo aprendido con los compañeros

37. ¿Cuál es la diferencia, a grandes rasgos, entre una copia de seguridad y una imagen de respaldo?

38. ¿Qué modelos de almacenamiento existen?

39. ¿Qué modelo de almacenamiento te parece más completo?

40. ¿Qué sistema de administración de copias consideras más barato?

41. ¿Qué sistema de administración de copias crees que es menos seguro?

42. ¿Qué hace un software de copias de seguridad cuando encuentra un archivo en uso?

43. En función de la respuesta anterior, ¿el software de copias trabaja siempre de ese modo?

44. ¿Por qué es importante elegir bien el horario para realizar copias de seguridad?

45. ¿Qué permisos necesita el software de copia y por qué?

46. ¿Por qué conviene cifrar las copias de seguridad?

47. ¿Dónde suelen usarse imágenes de respaldo?

48. Indica una ventaja y un inconveniente de usar un servicio remoto de copias de seguridad. Debate tu respuesta con los compañeros.

49. Busca en internet empresas que den servicios de copias de seguridad remotas y lee las condiciones del contrato. ¿Qué puntos te llaman la atención? ¿Existe compensación en caso de fallo del servicio?

5. Documentación en papel

Hoy día todas las empresas siguen teniendo gran cantidad de documentación en papel.

Contratos, libros con cuentas, documentos antiguos, etc. Todos estos papeles también necesitan copias de seguridad; antiguamente se fotocopiaban y eran almacenados en cajas fuertes.

No es necesario decir el gran volumen que podían llegar a ocupar estos documentos, por lo que últimamente se tiende a su digitalización. No obstante, continúa siendo necesaria la conservación en papel de determinados documentos importantes, que deberán custodiarse con todas las medidas de seguridad tradicionales y que se contemplan en las unidades relativas a seguridad física.

Lo más fácil es escanear el documento en sí para poseer una versión digital del mismo, y una vez en nuestro equipo se procede a almacenar y se copia siguiendo los pasos habituales.

Existen también dispositivos, como las tabletas digitalizadoras, que permiten recoger una firma, evitando así imprimir innecesariamente un documento.

↑ Tableta LCD para firmas STU-500.

↑ Escáner EPSON Perfection v750 PRO.

Hacer esto evita perder información debido al deterioro del papel y de la tinta con que se imprima, además de ayudar a la conservación del medio ambiente.

Atención: Si no es imprescindible, no imprima ni fotocopie este documento. Ahorrar papel y energía es cosa de todos.

Destrucción de documentos en papel

La destrucción de archivos importantes en papel, máxime aquellos relacionados con la privacidad de las personas, se debe hacer con todas las garantías. Para ello existen máquinas destructoras de documentos y también puede recurrirse a empresas especializadas en destrucción y reciclaje de documentos, que garanticen la confidencialidad presente y futura del contenido de los mismos.

PRÁCTICA PROFESIONAL

Almacenamiento y resguardo de la información

Ahora que has terminado la unidad sobre políticas de almacenamiento y resguardo de la información, te pedimos que vayas más allá y entres en la realidad del mundo laboral.

Estás trabajando y tu jefe te pide que realices varias tareas. Puede que nunca antes las hayas hecho, pero tendrás que aprender practicando.

OBJETIVOS

- Comprobar la necesidad de un buen ancho de banda para almacenar copias de seguridad y datos en remoto.
- Familiarizarse con el uso de software de propósito específico, en este caso de almacenamiento remoto.
- Aprender a crear imágenes de respaldo e instalarlas.
- Familiarizarse con el software propio para crear imágenes.
- Familiarizarse con el manejo de almacenamiento secundario, en este caso, un DVD.

INSTRUCCIONES

Junto con un compañero o compañera realiza la siguiente práctica.

Primera parte

- Descarga, si aún no lo tienes, el software en su versión gratuita de **Dropbox** y sigue los pasos que se indican para su instalación.
- Descarga una imagen del sistema operativo Guadalinex, disponible en http://www.guadalinex.org/descargador/index.php?nombre=guadalinex-v6-desktop-cd.iso
- Comparte la imagen **.iso** con tu compañero a través de Dropbox.
- Aprende todas las opciones de las que dispone Dropbox mientras se realiza todo el proceso. No tengas miedo de practicar con el software.

Segunda parte

- Descarga el software de evaluación Image for Windows desde alguna web. Nosotros te proponemos la descarga gratuita desde Softonic: http://image-for-windows.softonic.com/
- Instálalo y crea una imagen de alguna partición de tu disco duro que no estés utilizando pero que contenga algún archivo.
- Grábala en un DVD y vuelve a restaurarla con el software mencionado.
- Dispones de 30 días desde que instales el software para usarlo.

Resuelve

1. Realiza los pasos comentados anteriormente y redacta un informe con tu compañero o compañera. El informe debe tratar al menos tu experiencia sobre los puntos fijados en los objetivos.
2. Se deberán presentar capturas de pantallas que demuestren las actividades realizadas así como el DVD con la imagen.

MUNDO LABORAL

S3, el sistema de almacenamiento de Amazon

Una de los grandes problemas a los que nos enfrentamos los desarrolladores a la hora de lanzar un gran proyecto que incluya el almacenamiento y servicio de una gran cantidad de datos es el de conseguir un sistema rápido, con alta disponibilidad y, además, económico.

La mayoría de proveedores de *hosting* nos ofrecen la posibilidad de contratar servidores con gran capacidad de almacenamiento, pero suelen ir ligados una tarifa de pago por transferencia de datos, por lo que si lo que buscamos es servir archivos de gran tamaño como fotos o vídeos, nos encontraremos con que la factura a final de mes será más alta de lo que nos imaginábamos al principio.

Justo en esta época en la que las nuevas conexiones de banda ancha nos permiten acceder a contenidos cada vez más pesados, y la demanda de servicios de publicación y reproducción online de contenidos multimedia se ha visto incrementada, Amazon ha desarrollado AWS *(Amazon Web Services),* un conjunto de servicios que ha hecho la vida un poco más fácil y economizada a los desarrolladores que se han propuesto lanzar proyectos de este tipo, como es el caso de minube.com.

Dentro de AWS encontramos S3 *(Simple Storage Service),* un servicio de almacenamiento masivo, totalmente transparente, que nos permite colgar todos nuestros datos en los *Data Center* de Amazon sin preocuparnos por ningún tipo de límite. Fotos, vídeos...

Capacidad, seguridad y disponibilidad

Uno de los puntos fuertes de S3 es su transparencia a la hora de alojar nuestros datos. Nunca tendremos que preocuparnos por la capacidad de almacenamiento que tiene nuestra cuenta, ya que dispondremos de un único contenedor con una capacidad virtualmente ilimitada. Cuanto más almacenemos, más pagaremos.

Físicamente, nuestros datos estarán distribuidos por los *Data Center de Amazon,* pero es algo que permanece ajeno a nosotros y de lo que jamás tendremos que preocuparnos. La escalabilidad es un concepto que con S3 se vuelve superfluo. Amazon ya se encarga por nosotros de disponer de nuevas máquinas y más unidades de almacenamiento, y de hacer que todo funcione sin que estemos al tanto de ello.

Para la organización de nuestros archivos, Amazon ha creado tres conceptos:

- ***buckets:*** son algo parecido a un directorio o carpeta de nuestro sistema operativo, donde colocaremos nuestros archivos. Los nombres de los *buckets* están compartidos entre toda la red de Amazon S3, por lo que si creamos un *bucket,* nadie más podrá usar ese nombre para un nuevo *bucket.*
- ***objects:*** son las entidades de datos en sí, es decir, nuestros archivos. Un *object* almacena tanto los datos como los metadatos necesarios para S3, y pueden ocupar entre 1 byte y 5 gigabytes.
- ***keys:*** son una clave única dentro de un *bucket* que identifica a los *objects* de cada *bucket.* Un object se identifica de manera unívoca dentro de todo S3 mediante su *bucket* + *key.*

En cuanto a seguridad, Amazon ha implementado un sistema de permisos de acceso a archivos por usuario (un poco simple pero suficiente para cualquier propósito), a los que podremos dar capacidad de «Lectura», «Escritura» o «Control Total».

Por defecto tendremos tres usuarios: ***Owner*** (referente al usuario que alojó el archivo), ***Authenticated Users*** (referente a usuarios autenticados en Amazon), ***Everyone*** (referente a todos los usuarios no autenticados, es decir, cualquier cliente en todo internet), aunque podremos añadir nuevos usuarios de S3 con permisos específicos para nuestros datos.

Amazon nos asegura un 99,9 % de disponibilidad, lo que iguala cualquier sistema de alta disponibilidad que podamos contratar, y nos llegaría a devolver hasta un 25 % de lo facturado en caso de una disminución de disponibilidad por debajo del 99 %.

MUNDO LABORAL

Tarifas y servicios

El servicio S3 se factura de cuatro maneras distintas, y conjuntas:

- **Almacenamiento mensual:** cuanto más almacenemos en S3, más pagamos. Se trata de una tarifa por GB almacenado/mes.
- **Transferencia de datos:** una tarifa decreciente en la que cada GB transferido nos costará más barato cuanto más transfiramos.
- **Accesos GET:** solicitudes de archivos. Se paga por cada acceso a un archivo..
- **Accesos PUT/LIST:** solicitudes de envío o solicitud de listados.

A pesar de todo el desglose de facturación, que nos pueda parecer que nos cobran por todo, los servicios de Amazon son ridículamente baratos. Para que os hagáis una idea, unos 2,5 GB de datos almacenados y una transferencia de 15 GB al mes, no llegará a los 4 dólares (2,69 €) mensuales.

Podéis hacer el cálculo de cuánto nos podría costar esto, o una cantidad mayor proporcional, en un servicio de *hosting* tradicional.

Adaptado de **Maestros del Web**
4 de marzo de 2008
http://www.maestrosdelweb.com/editorial/por-que-utilizar-s3-el-sistema-de-almacenamiento-de-amazon/

Actividades

1. Maestros del Web publicaba en **marzo de 2008** este artículo en el que informaba de las características y los precios de almacenamiento remoto ofrecidas por la compañía Amazon (www.amazon.com).

- ¿Existe en la actualidad ese servicio S3 de Amazon?

2. En caso negativo:

- ¿Qué servicio de *hosting* ofrece actualmente Amazon que tenga parecidas características?

3. El artículo habla del cobro de algunos *hosting* por tasa de transferencia.

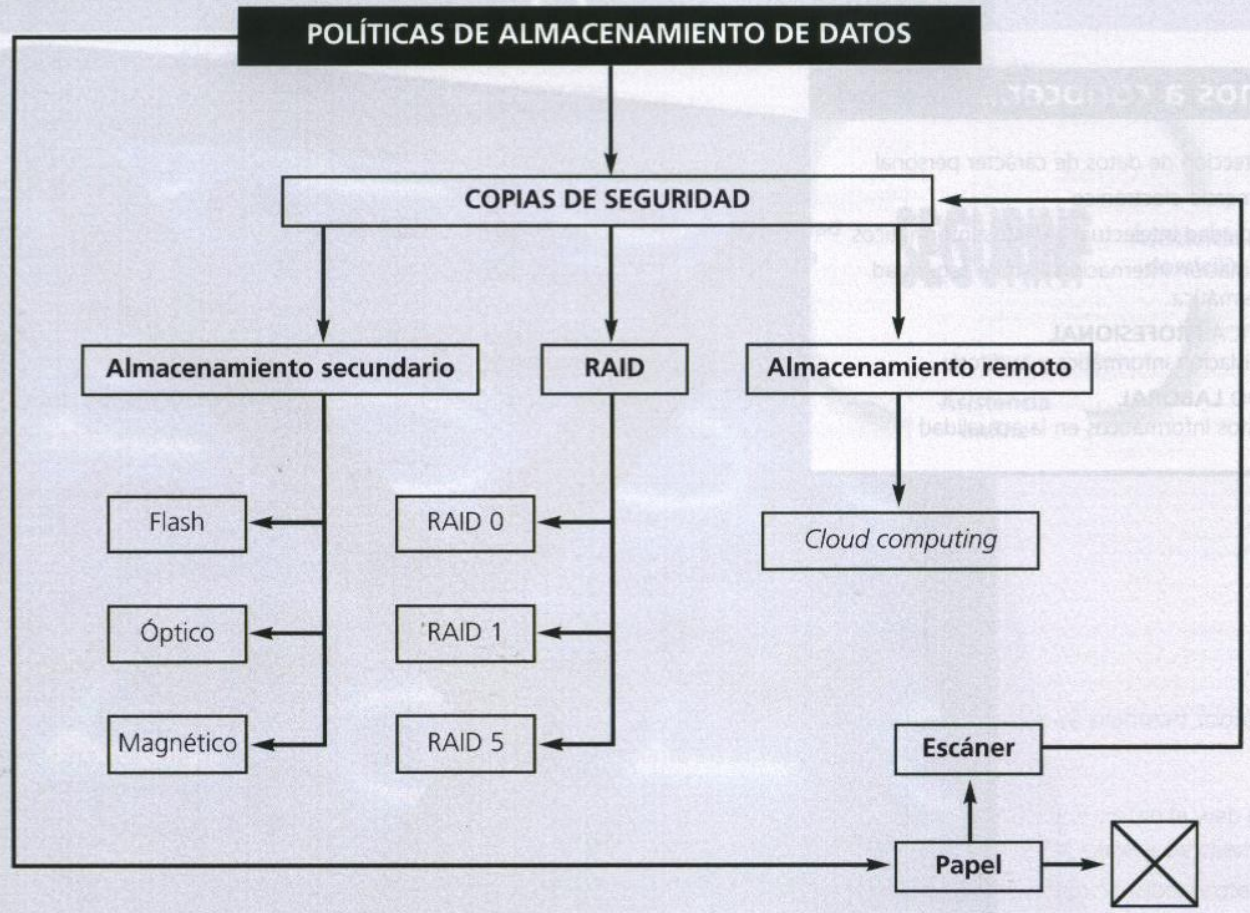
- ¿Puedes explicar en qué consiste la tasa de transferencia de alojamiento?
- ¿Si se cobra por tasa de transferencia y tenemos alojada una web que ofrece visualización de vídeos o películas, nos saldrá más cara que si ofrecemos servicios de mudanzas?
- En cuanto a Accesos GET, ¿en cuál de los dos casos del punto anterior crees que nos saldría más cara la tarifa?

4. Unas consideraciones más:

- ¿Podríamos decidir no alojar en esos espacios nuestra web sino solamente una copia de seguridad de nuestros archivos más importantes o más voluminosos?
- ¿Qué tarifa nos resultaría más interesante en el caso del punto anterior?

En el mundo en evolución permanente de la informática, lo que es noticia un día, en pocos meses deja de ser actualidad. Recuerda que **siempre hay que estar al día.**

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. **Marca las respuestas que sean válidas si hablamos de los RAID que se han estudiado:**
   a) El RAID 0 necesita como mínimo 5 discos.
   b) En el RAID 1 se perdería toda la información si fallasen todos los discos que lo componen.
   c) El RAID 5 necesita un mínimo de 3 discos.
2. **El almacenamiento remoto es el que se hace:**
   a) En un disco duro externo.
   b) En un CD, DVD o Blu-Ray.
   c) En el exterior de la empresa, probablemente en una empresa externa.
   d) El que se guarda en cajas fuertes de la propia empresa.
3. **Para restaurar una copia de seguridad incremental, es necesario restaurar:**
   a) La copia completa.
   b) La copia completa más todas las copias incrementales.
   c) La copia completa más la última copia incremental.
4. **¿Windows y Mac tienen herramientas para crear copias de seguridad de todo el sistema?**
   a) Solamente Windows 7.
   b) Eso solamente puede hacerlo Mac.
   c) En Windows era posible hasta la versión XP.
   d) Windows Vista, Windows 7 y Mac Os a partir de la versión 10.5.

Soluciones: 1b, 1c, 2c, 3b, 4d

9 Legislación sobre seguridad informática y protección de datos

vamos a conocer...

1. Protección de datos de carácter personal
2. Comercio electrónico
3. Propiedad intelectual y delitos informáticos
4. Legislación internacional sobre seguridad informática

PRÁCTICA **PROFESIONAL**
Legislación informática y auditoría

MUNDO **LABORAL**
Delitos informáticos en la actualidad

y al finalizar esta unidad...

- Conocerás la normativa que rige los datos de carácter personal, el comercio electrónico y la propiedad intelectual.
- Sabrás detectar los delitos informáticos y las normas que los regulan en distintas leyes españolas.
- Sabrás qué son los *Common Criteria* y las Directivas europeas en materia de seguridad informática.
- Aplicarás tus conocimientos técnicos y legales sobre seguridad informática para realizar auditorías.

CASO **PRÁCTICO** INICIAL

situación de partida

Al terminar los estudios, tú y un grupo de estudiantes de tu curso habéis decidido crear una empresa de servicios y productos para la seguridad informática.

Además de los trámites administrativos necesarios para su creación, incluida una subvención que vais a solicitar en vuestra Comunidad Autónoma, hay una serie de factores que necesitáis analizar y decidir de qué forma vais a gestionar el trabajo, quién se encargará de cada cometido, cómo haréis la publicidad de vuestra empresa, la forma de recibir pedidos y de atender dudas o reclamaciones de clientes, los medios y gastos de envío de productos, la gestión de presupuestos y, sobre todo, cómo tener la seguridad de que todo se está haciendo dentro de la legalidad.

estudio del caso

Antes de comenzar a leer esta unidad de trabajo, podrás realizar algunas de las actividades que se plantean sobre este caso. Una vez que hayas completado el estudio detenidamente serás capaz de realizarlas todas.

1. Habéis decidido insertar publicidad de vuestra empresa en páginas web relacionadas con la informática.
   - ¿Qué requisitos legales debe cumplir vuestra publicidad?
2. Una vez que habéis puesto en funcionamiento vuestra actividad económica, vais creando un fichero de clientes, que contiene todos los datos de los mismos necesarios para la facturación de productos y servicios. Dicho fichero se conserva en el disco duro de un ordenador, pero también se realiza copia en papel de cada registro
   - ¿Será necesario aplicar medidas de seguridad a estos ficheros?
   - ¿Hay que hacer algún trámite con la Agencia Española de Protección de Datos?
   - ¿A qué nivel de seguridad pertenece nuestro fichero de clientes?
3. Habéis decidido crear una página web para vuestra empresa, no solo para dar a conocer vuestros productos y servicios, sino también para contratar su venta con los potenciales clientes que visiten la web o con los que ya pertenecen a vuestra cartera de clientes.
   - ¿Hay que hacer alguna advertencia sobre protección de datos para clientes que solicitan presupuestos o contratan la compra de alguno de vuestros productos y servicios?
   - ¿Qué normativa sobre comercio electrónico deberéis conocer bien para no cometer errores que puedan causaros problemas legales?
   - ¿Tendréis la obligación de realizar auditorías de seguridad de la información periódicamente?
   - ¿Quién puede hacer una auditoría informática?
4. Si no queréis que nadie copie el diseño de vuestra página web, ni utilice las imágenes que habéis colgado para cada producto en venta, o que copie artículos informativos:
   - ¿Qué tendréis que hacer?
   - ¿Podríais decidir que cualquiera pueda publicar en otro sitio parte de vuestra web siempre que indique la fuente de la información y ponga un enlace a la misma?

1. Protección de datos de carácter personal

1.1. Origen del derecho a la protección de datos personales


Constitución
Título Preliminar
Artículo 1
1. España se constituye en un Estado social y democrático de Derecho, que propugna como valores superiores de su ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político.
2. La soberanía nacional reside en el pueblo español, del que emanan los poderes del Estado.
3. La forma política del Estado español es la Monarquía parlamentaria.
Artículo 2
La Constitución se fundamenta en la indisoluble unidad de la Nación española, patria común e indivisible de todos los españoles, y reconoce y garantiza el derecho a la autonomía de las nacionalidades y regiones que la integran y la solidaridad entre todas ellas.

↑ El derecho a la intimidad es uno de los derechos fundamentales de las personas que ampara la Constitución Española de 1978.

En la presente unidad estudiaremos la legislación relativa a seguridad de la información y de protección de datos de carácter personal.

Haremos un análisis de las disposiciones nacionales vigentes en materia de protección de datos. En los laterales de las páginas se reflejarán las directivas del Parlamento Europeo y del Consejo que se incorporan a la legislación española, así como una referencia a las Comunidades Autónomas que tienen sus propias agencias de protección de datos y normativa al respecto.

El derecho a la protección de datos de carácter privado y personal es un **derecho fundamental recogido en la Constitución** para su desarrollo legislativo posterior.

La Constitución española de 1978, como carta magna, no puede ser contradicha por ninguna otra ley o normativa de rango inferior, y es ahí donde se determinan los derechos fundamentales de las personas.

Concretamente en su **artículo 18** queda claro el derecho a la intimidad y en su favor requiere, en el apartado 4, la limitación por ley del uso de la informática:

1. Se garantiza el derecho al **honor,** a la **intimidad personal y familiar** y a la **propia imagen.**
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el **secreto de las comunicaciones** y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. **La Ley limitará el uso de la informática** para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En el **artículo 20,** apartado 4, vuelve a mencionar el **derecho al honor, a la intimidad y a la propia imagen** como límite a las libertades.

1.2. Agencia Española de Protección de Datos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) es un ente independiente de derecho público, cuya función general es la de **velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.**

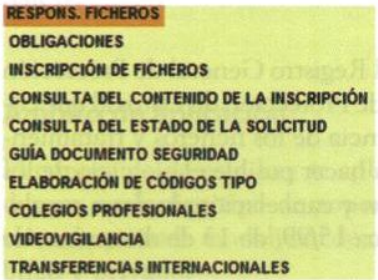
La AEPD fue configurada en la **Ley Orgánica 5/1992,** de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter personal. Poco después, el **Real Decreto 428/1993,** de 26 de marzo, aprobó su **Estatuto** regulador, que establece, entre otras cosas, las normas por las que la Agencia se ha de regir y las funciones que debe realizar.

Principales funciones por ámbitos y materias

1. **En relación con los afectados:**
   - Tutelar y garantizar el derecho de las personas en el ámbito de las comunicaciones telemáticas, incluido el spam.
   - Atender y resolver sus peticiones y reclamaciones, sin perjuicio de las vías de recurso procedentes.
   - Informar a las personas de los derechos que la Ley les reconoce en relación con el tratamiento automatizado de sus datos de carácter personal.
   - Promover campañas de difusión a través de los medios de comunicación social, con el fin de información referido en el punto anterior.

↑ Imagen en la portada de la web de la AEPD.

2. **En relación con quienes custodian datos de carácter personal:**
   - Dictar normas para que los ficheros de datos sean tratados de acuerdo con la legislación vigente.
   - Emitir recomendaciones de seguridad sobre el tratamiento y control de acceso a los ficheros.
   - Requerir medidas de corrección.
   - Ordenar la cancelación de los datos si se incumple la legalidad.
   - Sancionar a quienes traten con datos de carácter personal sin atenerse a la legislación vigente.
   - Autorizar o denegar las transferencias internacionales de datos.



← Información de la Agencia Española de Protección de Datos para los responsables de ficheros con datos de carácter personal.

saber más

LORTAD y LOPD

La primera norma con rango de Ley que regula el tratamiento de datos de carácter privado es la llamada **LORTAD,** o Ley Orgánica 4/1992 de Regulación del Tratamiento **Automatizado** de los Datos de Carácter Personal.

Actualmente se encuentra derogada y está en vigor la **LOPD,** o Ley Orgánica 15/1999 de Protección de Datos, que ya no se refiere –como su antecesora– únicamente a los datos automatizados, sino a los datos personales en **cualquier tipo de soporte.**

saber más

Organismos y normativa autonómica de protección de datos

Cataluña. Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.

Galicia. Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica.

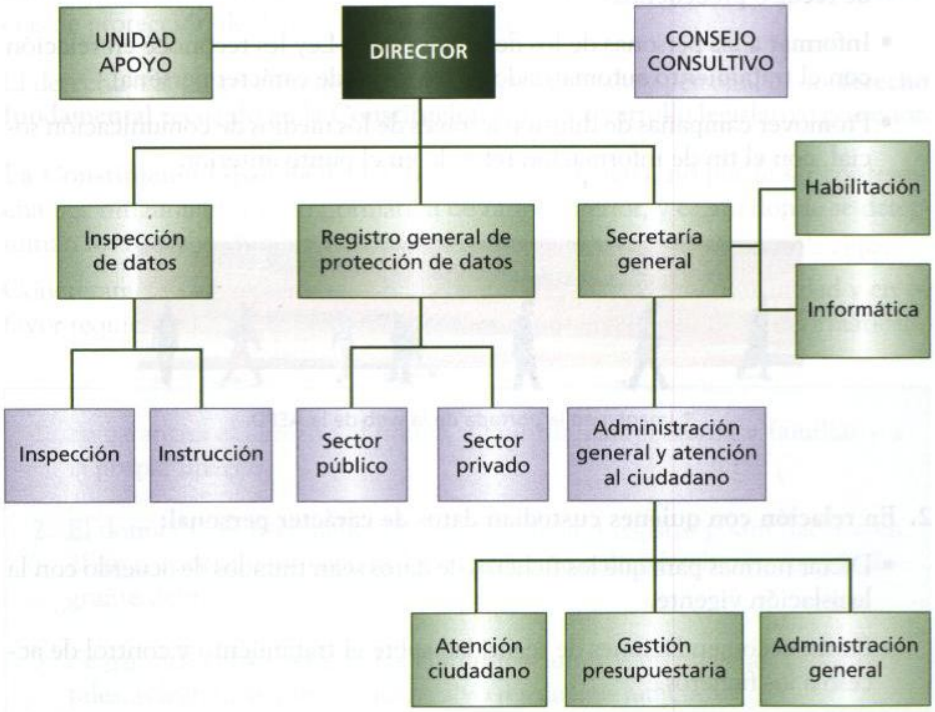
Madrid. Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

País Vasco. Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

↑ Animación de la 31 Conferencia Internacional de Autoridades de protección de datos y privacidad.

3. **En la elaboración y cumplimiento de normas:**
   - Colaborar con los órganos competentes en materia de desarrollo normativo relativo a protección de datos.
   - Colaborar con los organismos competentes en materia de control de cumplimiento de la normativa vigente en cuanto a protección de datos.

4. **En relación con otros países:**
   - Cooperación con otros organismos internacionales y órganos de la Comunidad Europea en materia de protección de datos.
   - Representación de España en los foros internacionales en la materia.



↑ Organigrama de la AEPD.

recuerda

Registro General de Protección de Datos

Tanto las Administraciones públicas como las empresas privadas tienen obligación de inscribir en el Registro General de Protección de Datos todos sus ficheros que contengan datos de carácter personal, ya sea de clientes, socios, proveedores, personal en plantilla, etc.

Asimismo tendrá obligación de notificar las modificaciones que se produzcan en dichos ficheros, para constancia del Registro General.

A continuación indicamos las funciones de algunos de los órganos de la Agencia Española de Protección de Datos.

- **Director.** Los actos dictados por el director de la AEPD se consideran actos de la Agencia y agotan la vía administrativa, dejando abierto solamente el recurso contencioso-administrativo.

- **Registro General de Protección de Datos.** El Registro General de Protección de Datos es el órgano de la Agencia Española de Protección de Datos al que corresponde velar por la publicidad de la existencia de los ficheros y tratamientos de datos de carácter personal, con miras a hacer posible el ejercicio de los derechos de información, acceso, rectificación y cancelación de datos regulados en los artículos 14 a 17 de la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Serán objeto de inscripción en el Registro General de Protección de Datos:

- Los ficheros de las Administraciones públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones de **transferencias internacionales** de datos de carácter personal con destino a **países** que no presten un nivel de protección equiparable al que presta la LOPD a que se refiere el artículo 33.1 de la citada Ley.
- Los **códigos tipo,** a que se refiere el artículo 32 de la LOPD, que serán los que se establezcan en las organizaciones de titularidad pública o privada en cuanto a régimen de funcionamiento, normas de seguridad del entorno, programas o equipos, obligaciones en el tratamiento de información de carácter personal y garantías que se ofrecen a las personas para ejercer los derechos que la Ley y su desarrollo les otorgan.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

- **Inspección de datos.** Comprueba la legalidad de los tratamientos.
- **Secretaría General.** Apoya a la Agencia para el correcto desempeño de sus funciones.

1.3. Ley Orgánica de Protección de Datos (LOPD)

La Ley Orgánica 15/1999, de **Protección de Datos de Carácter Personal,** fue publicada en el BOE del 14 de diciembre de 1999. Mediante esta Ley quedó derogada la LORTAD (Ley Orgánica 5/1992).

Uno de los objetivos de la **LOPD** fue adaptar el ordenamiento español a la **Directiva 95/46/CE** del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La LOPD tiene por objeto «garantizar y proteger las libertades públicas y los derechos fundamentales de las personas –en especial el derecho al honor y la intimidad personal y familiar– en lo que concierne al tratamiento de los datos personales».

Ámbito de aplicación

El contenido de esta Ley se aplicará a los **datos de carácter personal** registrados en **cualquier tipo de soporte físico,** que los haga **susceptibles de tratamiento,** y a toda modalidad de **uso posterior** de estos datos por los **sectores público y privado.**

Código de conducta de protección de datos personales en la Universidad de Castilla-La Mancha

↑ En la actualidad, una decena de **códigos tipo** han sido inscritos en el Registro General de Protección de Datos, entre ellos el de la Universidad de Castilla-La Mancha.

saber más

Datos personales

La LOPD y su Reglamento definen los datos personales como ***«Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables».***

Identificadas hace referencia a datos que por sí mismos identifican a la persona.

Identificables serían aquellos que con un poco de investigación llevarían a identificar a un individuo.

saber más

Guías telefónicas

Cualquier persona tiene derecho a que sus datos no figuren en las guías telefónicas y a que, si figuran, no sean utilizados con fines comerciales. Para ello, lo deberá comunicar a su proveedor de servicios telefónicos.

Se regirá por la LOPD **todo tratamiento de datos de carácter personal** en los siguientes casos:

- Cuando el tratamiento sea efectuado en **territorio español** en el marco de las actividades de un establecimiento del responsable del tratamiento.
- Cuando al responsable del tratamiento **no establecido en territorio español, le sea de aplicación la legislación española** en aplicación de normas de Derecho internacional público.
- Cuando el responsable del tratamiento **no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español,** salvo que tales medios se utilicen únicamente con fines de tránsito.

↑ Diagrama del ámbito de aplicación de la LOPD en todo el mundo.

Exclusión del ámbito de la LOPD

El régimen de protección de los datos de carácter personal que se establece en la LOPD **no será de aplicación:**

- A los ficheros mantenidos por **personas físicas** en el ejercicio de actividades exclusivamente **personales o domésticas.**
- A los ficheros sometidos a la normativa sobre protección de **materias clasificadas.**
- A los ficheros establecidos para la **investigación del terrorismo** y de formas graves de **delincuencia organizada.**

No obstante, en estos supuestos el **responsable del fichero comunicará previamente la existencia del mismo a la Agencia de Protección de Datos,** así como sus características generales y su finalidad.

saber más

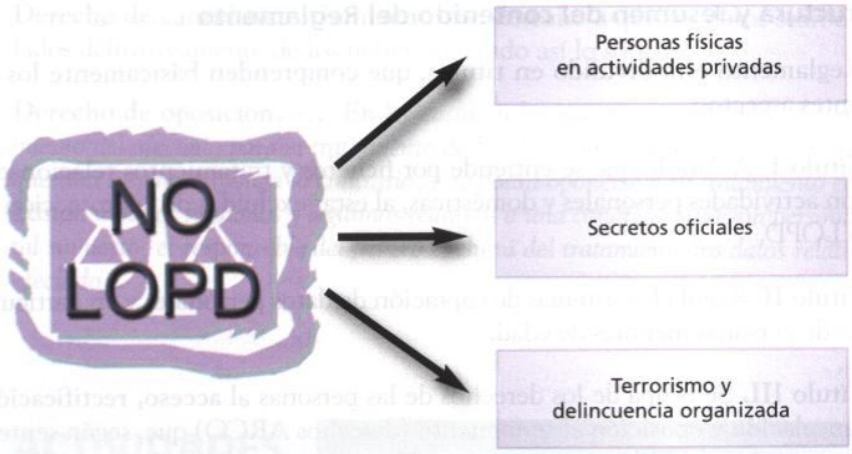
Directiva europea que incorpora la LOPD:

- **Directiva 95/46/CE,** relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

saber más

Materias clasificadas

En Derecho se llaman materias clasificadas los asuntos declarados como secretos oficiales.



↑ Situaciones que no se rigen por lo dispuesto en la Ley Orgánica de Protección de Datos de Carácter Personal.

Disposiciones específicas

Determinados tratamientos de datos personales tendrán **sus propias disposiciones reguladoras,** además de las que prevé la LOPD. Serán los siguientes:

- Los ficheros regulados por la legislación de régimen electoral.
- Los que sirvan a fines exclusivamente estadísticos y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
- Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
- Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

1.4. Reglamento de desarrollo de la LOPD (RLOPD)

El 19 de enero de 2008 se publicaba en el BOE el **Real Decreto 1720/2007** en el que se aprobaba el **Reglamento de desarrollo de la LOPD.**

El Reglamento nace, entre otros motivos, con el objeto de desarrollar procedimientos concretos de aplicación de las leyes vigentes bajo la competencia de la AEPD. No trata de repetir los contenidos de la Ley, sino de desarrollar contenidos de la misma que a lo largo de su tiempo de vigencia han demostrado necesitar ampliaciones y aclaraciones para dotar a la normativa de una mayor seguridad jurídica.

Estructura y resumen del contenido del Reglamento

El Reglamento está dividido en títulos, que comprenden básicamente los siguientes aspectos:

- **Título I.** Aclara lo que se entiende por ficheros y tratamientos relacionados con actividades personales y domésticas, al estar excluidos de la protección de la LOPD.
- **Título II.** Regula los sistemas de captación de datos personales y en particular los de personas menores de edad.
- **Título III.** Se ocupa de los derechos de las personas al **acceso, rectificación, cancelación** y **oposición** al tratamiento (derechos ARCO) que, según sentencia 292/2009 del Tribunal Constitucional, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y *«sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer»*.
- **Títulos IV a VII.** Regulan los criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían: los relativos a la **solvencia patrimonial y crédito** y los utilizados en actividades de **publicidad y prospección comercial,** así como las obligaciones que deben cumplir quienes manejen ficheros con este tipo de datos y la forma de transferirlos a otros países. Además definen el llamado **«código tipo»,** que son los instrumentos y procedimientos mediante los cuales cada organización garantizará el cumplimiento de la normativa vigente en cuestión de protección de datos.
- **Título VIII.** Atribución de **niveles** de seguridad y de las medidas que se tienen que tomar en cada uno de ellos.
- **Título IX.** Se refiere a los procedimientos tramitados por la Agencia de Protección de Datos.

saber más

ARCO son las siglas que corresponden a las iniciales de:

- **A**cceso.
- **R**ectificación.
- **C**ancelación.
- **O**posición.

saber más

Derechos ARCO

Artículos de la LOPD y su Reglamento regulador que hacen referencia a los derechos ARCO:

- **Acceso.** Artículo 15 LOPD y artículos 27 a 30 del Reglamento.
- **Rectificación y cancelación.** Artículo 16 LOPD y artículos 31 a 33 del Reglamento.
- **Oposición.** Artículos 35 y 36 del Reglamento.

caso **práctico** inicial

Cualquier empresa social, autónoma, pública o privada que trate ficheros con datos de carácter personal, tiene la obligación de registrarlos en el Registro General de Protección de Datos.

Derechos ARCO

Con estas siglas hacemos una abstracción del conjunto de derechos ciudadanos en relación con los datos personales registrados en el **Registro General de Protección de Datos,** para conocer quién los tiene y qué uso se está haciendo de ellos.

- **Derecho de acceso.** Tanto la LOPD como el Real Decreto 1720/2007 reconocen expresamente el derecho de las personas a tener acceso a sus datos de carácter privado que se encuentren en ficheros de empresas y entidades, y conocer el tratamiento al que están sometidos esos datos, la fuente de donde fueron obtenidos y las comunicaciones que se realicen o prevean realizarse de los mismos a otras organizaciones.
- **Derecho de rectificación.** Cuando los datos incluidos en cualquier fichero, automatizado o no, son inexactos, incompletos o excesivos, el ciudadano tiene derecho a solicitar su rectificación y a que su petición sea atendida.

- **Derecho de cancelación.** También tiene derecho a que sus datos sean cancelados definitivamente de los ficheros cuando así lo solicite.
- **Derecho de oposición.** *«... En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado».*

ACTIVIDADES

1. ¿En qué ley de rango superior se determinan las bases del derecho a la protección de datos de carácter personal?
2. ¿Cuál es la función principal de la Agencia Española de Protección de Datos?
3. Si no se está de acuerdo con los actos dictados por el director de la APDE, ¿qué se puede hacer?
4. Probablemente mantienes en tu ordenador un fichero de contactos de las personas con las que mantienes correspondencia por correo electrónico.
   a) ¿Es necesario que des de alta tu fichero en el Registro General de Protección de Datos?
   b) ¿Por qué?
   c) Si no tuvieras que darlo de alta, ¿eso significaría que puedes utilizar esa información de carácter personal para cualquier finalidad?
5. Indica cuáles son los derechos ARCO y especifica en qué consiste cada uno de ellos.
6. ¿Dónde se regulan los derechos ARCO?
7. En el sitio web de la Agencia Española de Protección de Datos, existe el **Canal del ciudadano,** que informa de los derechos ARCO y otros que le amparan.
   a) ¿Qué dice acerca del derecho a no recibir publicidad no deseada?
   b) ¿Están incumpliendo las empresas con la LOPD si envían publicidad no solicitada ni deseada?
   c) ¿Qué se puede hacer si aun así se recibe?
8. Señala cuáles de los siguientes casos están excluidos del ámbito de aplicación de la LOPD:
   a) Las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al que presta la LOPD a que se refiere el artículo 33.1 de la citada Ley.
   b) Los ficheros de datos personales, cuando al responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público.
   c) Los ficheros relativos a terrorismo.
   d) Los ficheros que contienen materias clasificadas.
   e) Aquellos cuyo tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
   f) Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Formulario establecido en nuestro Documento de Seguridad para el cumplimiento de los derechos ARCO de titulares de datos de carácter personal, según LOPD.

EJERZA SU DERECHO de acceso, rectificación, cancelación u oposición, de acuerdo con la Ley Orgánica de Protección de Datos

D/Dª ..... DNI .....

Domicilio ..... Localidad ..... C.P. .....

Provincia ..... Teléfono* ..... E-mail .....

**Campo no obligatorio*

SOLICITA *(Marque el derecho que desea ejercitar)*

☐ Ejercitar el **derecho de acceso** a sus datos de carácter personal

☐ Solicitando que se le remita dicha información a su dirección postal

☐ Solicitando que se le remita dicha información a su dirección de correo electrónico

☐ Ejercitar el **Derecho de Rectificación** de los siguientes datos de carácter personal en el sentido que se indica a continuación:

.....

.....

☐ Ejercitar el **Derecho de Cancelación** de los datos de todos los archivos/ficheros de los dominios asociados a ***nombre_de_responsable_del_fichero***.

☐ Ejercitar el **Derecho de Oposición** al tratamiento sus datos para las siguientes finalidades *(marque o enumere las finalidades objeto de la oposición)*:

☐ Remitirle información o comunicaciones sobre productos, servicios, eventos o actividades de ***nombre_de_responsable_del_fichero***.

☐ Otras (indicar)

.....

.....

Se deberá entregar el formulario debidamente cumplimentado y adjuntando una fotocopia de DNI (adjuntar escaneada si utiliza como medio el email – xxx@xxxxx.com) o documento equivalente, que acredite la identidad del interesado y sea considerado válido de acuerdo al ordenamiento jurídico Español. Si actúa en representación de un tercero deberá aportarse DNI del representante y documento acreditativo de la representación de interesado. El siguiente formulario deberá remitirse por correo a ***nombre_de_responsable_del_fichero***, Dirección: *xxxxxxxxxxxxxx*

Por favor, indique el fichero o ficheros donde cree que pueden encontrarse sus datos:

☐ **Usuarios Web** ☐ **Clientes** ☐ **Contactos**

↑ Un modelo-ejemplo de formulario para que las personas puedan solicitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, que les reconoce la Ley.

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos serán incorporados a un fichero con datos de carácter personal denominado **"xxxxx"**, cuya finalidad es **"xxxxxxxxxxx"**. Le informamos asimismo que los datos podrán ser comunicados a otras Administraciones públicas en el ámbito de competencias semejantes o materias comunes en cumplimiento de la legislación aplicable. Podrá comunicarnos su **oposición** a este tratamiento de datos así como ejercer sus derechos de **acceso, rectificación y cancelación** dirigiéndose al responsable del fichero, **"nombre_de_la_empresa_u_organismo"**, siempre acreditando su identidad en la comunicación conforme a Derecho.

↑ Modelo de información que debe mostrarse en cualquier formulario de recogida de datos de carácter personal, ya sea en papel, web o mediante comunicación electrónica.

Niveles de seguridad y medidas asociadas

El Real Decreto 1720/2007 establece qué tipos de datos se consideran de nivel básico, medio y alto. Los de nivel alto son los que más protección requieren y para ello el Real Decreto establece unas medidas mínimas de seguridad que son de obligado cumplimiento para las personas y organizaciones que manejen o custodien los datos.

En la siguiente tabla puede verse de forma resumida qué datos son de cada nivel y cuáles son las medidas mínimas que les corresponde adoptar a los responsables de los ficheros de datos personales.

Hay que observar que al nivel medio le corresponden sus propias medidas además de las que se deben adoptar para el nivel básico, y que el nivel alto tendrá las suyas propias además de las de los dos niveles inferiores.

caso práctico inicial

Si el fichero contiene datos relativos a salud, origen racial, creencias religiosas, ideología política, violencia de género y otros especialmente sensibles, pertenece al nivel alto.

NIVELES	TIPO DE DATOS	MEDIDAS
Básico	**Personales, como:** • Nombre y apellidos • Números de teléfono fijos y móviles • Dirección postal y electrónica • Profesión • Fecha y lugar de nacimiento • Otros datos personales	• Documento de seguridad • Formación y responsabilidad del personal encargado del manejo de datos • Registro de incidencias • Control de acceso • Gestión de soportes de los datos • Copias de respaldo y recuperación
Medio	**Relativos a:** • Infracciones administrativas o penales • Solvencia patrimonial y crédito • Los que permitan deducir aspectos o comportamientos de la persona **O que manejen para sus servicios:** • Las entidades financieras • La Seguridad Social, entidades gestoras y mutuas • La Administración tributaria	Las medidas de nivel **básico** y además: • Designación de personal responsable de seguridad • Auditoría de seguridad cada dos años • Exigencia de identificación y autenticación para acceso a datos • Control de acceso físico solo para personal autorizado
Alto	**Relativos a:** • Religión • Ideología • Afiliación sindical • Creencias • Origen racial • Salud • Vida sexual • Violencia de género • Recabados para fines policiales sin consentimiento de la persona afectada	Las medidas de nivel **básico y medio** y además: • Registro pormenorizado de accesos a los datos • Medidas adicionales de seguridad en copias de respaldo y recuperación • Cifrado de datos para telecomunicaciones

↑ Después de haber estudiado el contenido de las anteriores unidades, no te resultará desconocido el lenguaje que se emplea en la tabla en cuanto a medidas de seguridad que se han de tomar para velar por la **integridad, confidencialidad** y **disponibilidad** de la información.

caso **práctico** inicial

Si el fichero contiene datos sometidos por ley a un nivel de seguridad medio o alto, la empresa titular del fichero tendrá que pasar auditorías bianuales.

Soporte no automatizado

De la tabla anterior podríamos deducir que solamente hay que preservar los datos en soporte informático, pero en las empresas también se encuentran datos no automatizados, normalmente en papel, que pueden contener datos de carácter personal y que deben contar con el mismo nivel de protección que si estuviesen almacenados en discos duros u otros soportes digitales y en función del tipo de datos que contengan.

De ese modo, para el **nivel 1,** se deberá:

- Conservar los documentos en ubicaciones seguras, garantizando a los titulares de los datos conservados el ejercicio de los derechos ARCO.
- Establecer medidas de seguridad activa para impedir el acceso de personas no autorizadas a las ubicaciones en donde se encuentren los archivos en soporte papel.
- Establecer medidas de seguridad para los documentos que, por motivos cualesquiera, tuviesen que permanecer fuera de sus ubicaciones seguras, como por ejemplo para realizar trámites o consultas.

saber más

Artículos del RLOPD sobre medidas asociadas a niveles de seguridad

Nivel 1

Ficheros automatizados: artículos 88 a 94.

No automatizados: artículos 105 a 108.

Nivel 2

Ficheros automatizados: artículos 95 a 100.

No automatizados: artículos 109 y 110.

Nivel 3

Ficheros automatizados: artículos 101 a 104.

No automatizados: artículos 111 a 114.

En lo relativo al **nivel 2,** se tendrán en cuenta las medidas que se establecen para los que están en soporte digital.

En cuanto al **nivel 3,** se debe:

- Destruir el material que contenga datos de carácter personal cuando no se necesite más.
- Destruir las copias que se realicen para gestiones diversas cuando se hayan finalizado.
- Tomar todas las medidas de seguridad que garanticen la confidencialidad de la información en los traslados de documentos.
- Además del control de acceso, es necesario llevar un sistema de identificación de las personas que acceden a este tipo de información.

↑ Trituradora de papel Destroylt.

↑ Mini destructora de papel USB.

Infracciones

Cuando el obligado a la custodia de datos de carácter personal incumpla lo establecido por la Ley, puede ser objeto de sanciones económicas desde 600 hasta 600.000 euros o incluso a la inmovilización de ficheros o el cese de la actividad, en función del tipo de infracción cometida. A continuación mostramos algunos **ejemplos** de infracciones leves, graves y muy graves:

a) **Leves:**

- No atender en el plazo reglamentario de 10 días las solicitudes de los usuarios en cuanto a sus derechos ARCO.
- Incumplir de forma leve el deber de secreto (no transmisión a terceros) de datos personales.
- Recoger datos personales de usuarios sin informar previamente de la existencia de un fichero en donde se conservarán o de las consecuencias de no responder a las preguntas formuladas.
- No colaborar con la AEPD en materia de protección de datos.

b) **Graves:**

- No observar las medidas de seguridad que se establecen en lo relativo a la conservación de los datos.
- Recoger datos personales sin consentimiento expreso del titular de los mismos, salvo en los casos que contempla la Ley.
- La no actualización de los datos cuando se haya producido y comunicado un cambio de los mismos.
- Incumplir el deber de secreto cuando se trate de datos de nivel medio.

c) **Muy graves:**

- La obtención de datos personales de forma engañosa o fraudulenta.
- Desatender sistemáticamente u obstaculizar el ejercicio de los derechos ARCO.
- La transferencia de datos personales a países cuya legislación no aplique medidas de seguridad equivalentes a las españolas.
- El incumplimiento del deber de secreto en el caso de datos de nivel alto.

saber más

Sanciones

Las sanciones económicas que puede imponer la AEPD por incumplimiento de la Ley en materia de protección de datos de carácter personal se establecen en función de la gravedad de las infracciones.

En números redondos:

- **Leves:** de 600 a 60.000 €.
- **Graves:** de 60.000 a 300.000 €.
- **Muy graves:** de 300.000 a 600.000 €.

ACTIVIDADES

9. De las siguientes medidas, indica cuáles son obligatorias en el caso de una empresa que trabaje con datos de nivel medio:

a) Cifrar los datos en las telecomunicaciones.

b) Llevar un registro de incidencias.

c) Hacer copias de respaldo y recuperación de los datos.

d) Tener redactado un documento de seguridad.

e) Realizar una auditoría de seguridad bianual.

f) Llevar un control de acceso físico solo para el personal autorizado.

EJEMPLO

Documento de seguridad

Como hemos visto en la tabla de medidas obligatorias para los tipos de datos de cada nivel, es obligatorio disponer de un documento de seguridad, que será redactado por la empresa en función de sus características y de los tipos de datos que maneje y deba custodiar.

La Agencia Española de Protección de Datos ha elaborado un modelo de documento de seguridad adaptable a todo tipo de empresas. En el mismo indica el carácter de guía y no de norma de ese modelo, que divide en siete apartados, de los que haremos un corto resumen:

I. Ámbito de aplicación del documento

- Se nombrará a la persona responsable de los ficheros y se enumerarán los ficheros que maneja la empresa y a qué niveles pertenecen.

II. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

- Medidas de identificación y autenticación del personal con permiso de acceso a los ficheros.
- Control de acceso físico o lógico. Relación de personas que tienen acceso parcial o completo a los ficheros.
- Gestión de soportes. Normas de etiquetado y almacenamiento de los soportes que contienen los ficheros con datos de carácter personal.
- Gestión de acceso a través de las redes de comunicaciones.
- Procedimientos para las copias de respaldo y recuperación de la información.

III. Procedimiento general de información al personal

- Funciones de cada persona que tiene acceso a los datos y procedimientos seguidos para la formación del personal en lo que respecta a la normativa legal y los procedimientos de seguridad fijados por la empresa.

IV. Funciones y obligaciones del personal

- Obligaciones generales de las personas que accedan a los datos de carácter personal en cuanto a medidas, normas, procedimientos y estándares que corresponden a las funciones que desarrollan.
- Obligaciones particulares de cada persona con acceso a los datos: administradores, responsables de seguridad física o lógica, etc.

V. Procedimiento de notificación, gestión y respuestas ante las incidencias

- Identificar las posibles incidencias de seguridad y la persona o personas a las que tienen que notificarse, así como el método a seguir para la notificación.
- Indicar los procedimientos manuales o informáticos por los que se gestionará el registro de incidencias.

VI. Procedimientos de revisión

- Cómo y cuándo se deberá revisar el documento de seguridad y a qué personas compete proponer modificaciones y aprobar su contenido, de modo que siempre esté conforme a la realidad de la empresa y a la normativa vigente. Indicar los procedimientos de auditoría para los niveles que la requieren legalmente.

VII. Consecuencias del incumplimiento del documento de seguridad

- Indicación de la norma vigente por la que se aplicarán sanciones por incumplimiento del contenido del documento de seguridad.

Completo en

https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

1.5. Software para la protección de datos

El Real Decreto 1720/2007, en el que se aprueba el Reglamento de desarrollo de la LOPD, expone en su **Disposición adicional única que «Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento».**

A partir de la publicación de la LOPD y, sobre todo, después de la publicación del Reglamento que la desarrolla, las empresas productoras de software de gestión han comenzado a crear versiones de sus productos adaptadas a los requerimientos de nuestra legislación, como es la conocida SAGE SP, creadora de ContaPlus, NominaPlus y FacturaPlus. Algunas de ellas, como Artico SLL, ofrecen productos de **gestión online.**

Estas aplicaciones están desarrolladas para grandes empresas y también hay versiones más sencillas para pymes. Están construidas para entornos específicos o mixtos, aunque la mayoría se basa en entornos bajo Windows. Básicamente contienen las siguientes herramientas de gestión de datos de carácter personal:

- Inscripción de los ficheros de datos en la Agencia Española de Protección de Datos.
- Plantillas para la cumplimentación de la documentación legal necesaria, como contratos de cesión de datos, solicitud de derechos ARCO, contratos de prestación de servicios, etc.
- Plantilla para la elaboración del documento de seguridad obligatorio para cualquier nivel de seguridad de datos.
- Mantenimiento del documento de seguridad.
- Mecanismos para gestionar los informes de incidencias y las entradas y salidas de información.
- Mecanismos o pautas para gestionar los soportes de datos.
- Gestión y realización de auditorías periódicas o extraordinarias.

recuerda

El **título VIII** del Reglamento de desarrollo de la LOPD establece los niveles de seguridad de los datos y las medidas que se tienen que tomar en cada uno de ellos.

GESDATOS SOFTWARE DE PROTECCIÓN DE DATOS
proyectopyme
i latina
Conecta-lopd.es
DataPro
LOPDGEST
Protección de Datos El software de protección de datos para la LOPD

↑ Algunas marcas de software de gestión adaptado a la LOPD.

ACTIVIDADES

10. Busca en internet algunas de las marcas de software indicadas al margen u otras que faciliten el cumplimiento de lo establecido por la LOPD y completa con una X la columna de la derecha si ofrece la herramienta o servicio indicados en la columna de la izquierda.

Nombre de la empresa o del software:	
Inscripción de los ficheros en el Registro General de Protección de Datos	
Plantilla para la elaboración del documento de seguridad	
Herramientas de mantenimiento del documento de seguridad	
Gestión y realización de auditorías, periódicas o no	

2. Comercio electrónico

2.1. Ley de Servicios de la sociedad de la información y de comercio electrónico (LSSI)

La **Ley 34/2002,** de 11 de julio, se creó con objeto de incorporar las Directivas Europeas **2000/31/CE** sobre comercio electrónico, y **98/27/CE** sobre cesación de servicios por conductas contrarias a los derechos del consumidor.

Básicamente, la LSSI describe aspectos de internet y las nuevas tecnologías que otras leyes no definen o que suscitan incertidumbre, y que resume en el concepto de «servicios de la sociedad de la información».

Servicios de la sociedad de la información

La LSSI se refiere a los que prestan los operadores de telecomunicaciones, los proveedores de acceso a internet (ISP), portales, motores de búsqueda o las personas o empresas que ofrecen alguno de estos servicios a través de internet, incluido el comercio electrónico. En concreto, la ley describe el marco de obligaciones y derechos que comportan los siguientes servicios, siempre que constituyan una **actividad económica** directa o indirecta:

- Contratación de bienes y servicios por vía electrónica.
- Suministro de información por vía electrónica.
- Actividades de intermediación relativas a la provisión de acceso a la red.
- Transmisión de datos por redes de telecomunicaciones.
- Realización de copia temporal de las páginas de internet solicitadas por los usuarios.
- Alojamiento en servidores propios o de terceros.
- Provisión de instrumentos de búsqueda o de enlaces a otros sitios de internet.
- Cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...), siempre que represente una actividad económica para el prestador.

Exclusiones de la libre prestación

Están excluidos de la libre prestación aquellos servicios que atenten contra el orden público, la salud y la dignidad de las personas o la protección de la juventud y la infancia.

Ámbito territorial

La LSSI se aplica sobre las personas físicas o jurídicas prestadoras de esos servicios, que estén establecidas:

recuerda

La LSSI se refiere a servicios de la sociedad de la información que constituyan una **actividad económica directa o indirecta,** es decir, que proporcionen beneficio económico a quien la ejerza. Ejemplo de actividad económica indirecta: páginas web de acceso gratuito que, sin embargo, muestran publicidad por la que el titular de la página recibe una compensación dineraria. En tal caso, se han de someter a la LSSI.

↑ Google AdSense ofrece insertar publicidad en sitios web a cambio de dinero para sus titulares.

saber más

Se considera que un prestador de servicios está **establecido en España** si desde este país dirige y gestiona su actividad económica, es decir, el lugar en que el prestador tiene su domicilio fiscal.

- En España.
- En un Estado miembro de la UE, sobre el que se aplicarán restricciones si los servicios que ofrecen atentan contra ciertos valores, como el mantenimiento del orden público, la salud pública, la protección de menores o que incumplan la legislación española.
- En cualquier país fuera de la UE, que preste servicios de la sociedad de la información a través de algún establecimiento permanente situado en España o dirija estos servicios al territorio español, siempre que las normas internacionales no establezcan otra cosa.

Obligaciones que impone la LSSI

Los sujetos que se ven afectados por el contenido de la LSSI son los que indicamos a continuación junto con sus obligaciones.

A) Empresas que realizan comercio electrónico

La empresa incluirá en su web la siguiente información:

- Denominación social, domicilio fiscal, dirección de correo electrónico y números de teléfono o fax.
- Datos de inscripción en el Registro Mercantil u otro.
- Códigos de conductas a los que se encuentra adherida la empresa y la forma de acceder a ellos de forma electrónica.
- Precios de los productos o servicios que ofrecen, así como el importe de los impuestos y gastos de envío.
- Indicación de ofertas y plazo de vencimiento.
- En su caso, datos relativos a la autorización administrativa necesaria para ejercer su actividad, datos de colegiación y datos profesionales de quienes ejerzan una actividad regulada, así como la información clara y necesaria para las empresas que se acojan a servicios telefónicos de facturación adicional.

Además, será obligatoria la explicación en la web de lo relativo al contrato de compraventa online:

- Trámites necesarios para la contratación online.
- Si el contrato será archivado y accesible por el usuario.
- Idioma o idiomas en que será formalizado el contrato.
- Herramientas para detectar y corregir errores al introducir los datos en el contrato.
- Condiciones generales a las que está sujeto el contrato.
- Confirmación de la formalización del contrato mediante el envío de acuse de recibo.

saber más

Directivas europeas que incorpora la LSSI:

- **Directiva 2000/31/CE,** sobre comercio electrónico.
- **Directiva 98/27/CE,** relativa a las acciones de cesación de servicios por conductas contrarias a las leyes.
- **Directiva 2000/31/CE,** sobre internet y la sociedad de la información.

caso práctico inicial

Además de cumplir con lo establecido por la **LSSI,** las empresas que realicen contratos (de compraventa u otros) a través de internet pondrán en su web una cláusula informativa sobre el tratamiento al que se someterán los datos personales introducidos por los usuarios, que deberá ser aceptada antes de formalizar el contrato, cumpliendo así lo que establece la **LOPD** y su **Reglamento.** Además, la página debería ser segura **(protocolo https).**

saber más

El spam está regulado por la LOPD y por la LSSI.

↑ SMS que informa de un contenido publicitario.

B) Páginas web con publicidad

- Identificación clara del anunciante.
- Información inequívoca de que se trata de un mensaje publicitario.
- Cuando realicen ofertas, concursos o juegos promocionales, deberá quedar claro en la publicidad el carácter de tales y las condiciones de participación.
- En la publicidad mediante SMS es obligatorio haber obtenido la autorización expresa del destinatario para recibirla, estar indicados con las palabras «publicidad» o «publi» y establecer procedimientos sencillos para la revocación del consentimiento de recepción. (*Más adelante veremos que este aspecto se modifica en la Ley General de Telecomunicaciones, de 2003*).

C) Empresas intermediarias de la sociedad de la información

Son los operadores de telecomunicaciones, los proveedores de internet y las empresas de alojamiento de datos, enlaces y buscadores.

Aunque no son responsables directos de los contenidos que alojan o a los que permiten el acceso, sí lo son desde el momento en que tienen conocimiento de que se trata de material ilícito, si no lo retiran de inmediato. En función de esta responsabilidad tienen las siguientes obligaciones:

- Informar a sus clientes de medidas **y herramientas para aumentar la seguridad de la información,** tales como antivirus, cortafuegos o antispam, de las herramientas de filtro y control de acceso a contenidos, y en el caso de los ISP, de las posibles responsabilidades derivadas del uso de internet con fines ilícitos.
- **Colaborar con los órganos públicos** para la ejecución de resoluciones que no pudieran cumplirse sin esa ayuda.

D) Usuarios de internet

Son **responsables frente a la LSSI de los contenidos de sus espacios en internet** (foros, páginas web, blogs, etc.) siempre que contengan **publicidad de terceros por la que perciban ingresos.** En tal caso deben dejar de sí mismos una información básica como nombre, apellidos, dirección, teléfono y correo electrónico, y **respetar las normas que marca la Ley en lo que respecta a la publicidad:**

- Que el mensaje publicitario lo sea de forma inequívoca.
- Que se puede identificar a la empresa anunciante.

caso práctico inicial

La publicidad que hacemos de nuestros productos en otras páginas web, debe cumplir los requisitos que exige la LSSI.

saber más

La LSSI habla en su texto de «autorización expresa», lo que no quiere decir necesariamente escrita. Por ejemplo, entregar una tarjeta de visita en un contexto comercial ya implica una autorización expresa a recibir publicidad de quien la recibió, como queda recogido en la Jurisprudencia tras una sentencia de la Audiencia Nacional.

↑ Enlaces publicitarios en una página web.

ACTIVIDADES

11. Si una empresa u organismo ofrece servicios (como por ejemplo información), a través de internet, de forma gratuita, ¿está sujeta a la LSSI?

12. Las personas particulares que tienen una página web, un blog o un foro en internet con acceso al público general:

a) ¿Deben someterse a lo establecido por la LSSI?

b) Si contestaste sí, ¿en qué casos?

13. ¿Qué condiciones debe cumplir la publicidad insertada en un espacio web personal, si se reciben ingresos por ella?

2.2. Otras leyes

Otras leyes españolas y sus reglamentos regulan el tratamiento electrónico de la información en lo relativo al derecho a la privacidad y la intimidad, en el tratamiento de datos de carácter personal y a la publicidad. No obstante, suelen remitirse a lo establecido por la LOPD y por la LSSI, aunque maticen algunos aspectos particulares.

Ley General de Telecomunicaciones

La **Ley 32/2003,** de 3 de noviembre, General de Telecomunicaciones y el **RD 863/2008,** de 23 de mayo, por el que se aprueba el Reglamento de desarrollo, tienen por objeto la regulación de las telecomunicaciones, que comprenden la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas y los recursos asociados. En lo relativo a los derechos de los usuarios que tienen que ver con la materia que estamos estudiando, se refiere a ellos como señalamos a continuación a modo de resumen:

- Presta especial atención al derecho a la **intimidad de los usuarios de telefonía.**
- Establece que los datos aportados por los usuarios para la facturación, **no puedan utilizarse con fines comerciales.**
- Determina el derecho a **impedir, si se desea, la identificación de las llamadas** efectuadas por teléfono mediante algún procedimiento simple y gratuito.
- Protege a los usuarios frente a **publicidad no deseada** realizada mediante llamadas telefónicas o mensajes de fax, salvo consentimiento previo.
- En cuanto a los **derechos de los usuarios frente al spam,** se garantizan en los mismos términos en que lo hace la LSSI, aunque la LGT excluye la necesidad de un consentimiento expreso cuando ya existe una relación contractual entre el emisor y el receptor del mensaje publicitario, lo que, según la LGT, ya hace presumir que existe ese consentimiento.

saber más

Directivas Europeas incorporadas a la Ley General de Telecomunicaciones:

- Directiva 2002/19/CE
- Directiva 2002/20/CE
- Directiva 2002/21/CE
- Directiva 2002/22/CE
- Directiva 2002/58/CE
- Directiva 2002/77/CE

Ley de Firma Electrónica

La Ley 59/2003**, de 19 de diciembre, de Firma Electrónica se creó para otorgar confianza y garantías a las transacciones realizadas por vía telemática, fomentando la incorporación de las nuevas tecnologías** de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. En la LFE se desarrolla un marco legal para tres importantes conceptos que ya hemos estudiado en la **unidad 7:**

- Certificado electrónico.
- Firma electrónica.
- DNI electrónico.

saber más

Directiva Europea incorporada a la Ley de Firma Electrónica:

- **Directiva 1999/93/CE** del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

3. Propiedad intelectual y delitos informáticos

3.1. Introducción

El Ministerio de Cultura describe la propiedad intelectual como **«el conjunto de derechos que corresponden a los autores y otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación».**

La propuesta de medidas, normativas o no, para lograr la adecuada protección de la propiedad intelectual, es competencia del Ministerio de Cultura.

En España, todo lo referente a la propiedad intelectual está recogido principalmente por:

- **Real Decreto Legislativo 1/1996,** de 12 de octubre, por el que se aprueba el texto refundido de la **Ley de Propiedad Intelectual** (LPI).
- **Ley 19/2006,** de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios
- **Ley 23/2006,** de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual.

En enero de 2010, el Consejo de Ministros aprobó el texto del anteproyecto de **Ley de Economía Sostenible,** que también está muy relacionado con la sociedad de la información y que ha suscitado acalorados debates entre internautas, juristas expertos en derechos digitales y de autor y colectivos de creadores y productores.

La propiedad intelectual afecta directamente al campo de la informática y a la sociedad de la información, máxime desde que internet se convirtió en un medio de difusión de la cultura.

3.2. Conceptos

Derechos de autor. Les corresponden a quienes realizan creaciones originales de obras literarias, pictóricas, arquitectónicas, escultóricas, cinematográficas, musicales, etc., por cualquier medio y sobre cualquier tipo de soporte.

Derechos afines a los de autor. Los que corresponden a intérpretes, ejecutantes, entidades de radiodifusión, productores, etc.

Copyright. Es la expresión utilizada para indicar que una obra está sujeta a derechos de autor.

Copyleft. Alternativa a las restricciones que imponen en cualquier parte del mundo las leyes sobre derechos de autor en cuanto al uso, la distribución y la modificación de copias de una obra. Se considera lo opuesto al *copyright*, como lo son los símbolos que representan a ambos.

saber más

El **Registro General de la Propiedad Intelectual** es único en todo el territorio nacional y está integrado por los Registros Territoriales y el Registro Central, además de una Comisión de Coordinación como órgano colegiado de colaboración entre los Registros.

saber más

Directivas europeas

Directiva 2004/48/CE

Incorporada al ordenamiento jurídico español por la Ley 19/2006, por la que se amplían los medios de tutela sobre los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios.

Directiva 2001/29/CE

Incorporada por medio de la Ley 23/2006, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información.

↑ *Copyright.*

↑ *Copyleft.*

3.3. Delitos contra la propiedad intelectual

Delitos informáticos

Antes de hablar específicamente de la propiedad intelectual, podemos hacer un repaso de los delitos informáticos más frecuentes, que ya hemos estudiado en unidades anteriores.

Algunos de ellos se tramitan y resuelven según el Código Penal. Los que no entran en ese campo del Derecho –al menos todavía– deberán denunciarse, tramitarse y resolverse por las vías que les correspondan. Por ejemplo, en materia de protección de datos, las denuncias se elevan a la Agencia Española de Protección de Datos:

- Contra la disponibilidad, confidencialidad e integridad de la información. Por ejemplo, la alteración deliberada de la información, el robo de identidad, el *cracking*, *spyware* y *keylogger*.
- Relacionados con el sexo, principalmente corrupción de menores y pornografía infantil a través de páginas web, P2P o mensajería, o posesión de ese tipo de material.
- Estafas. Por ejemplo, el *phishing*.
- Contra el derecho a la intimidad, no haciendo uso de la obligación de secreto de datos de carácter personal como pueden ser fotografías, direcciones o datos médicos.
- Contra el mercado y los consumidores; por ejemplo, haciendo publicidad engañosa.
- Amenazas, injurias y calumnias propagadas a través de internet.
- Otros delitos, como la apología de la violencia, la xenofobia, el racismo o el terrorismo.
- Contra la propiedad intelectual, en especial la copia y distribución no autorizada de programas informáticos, música y películas, o la manipulación de la protección anti copia.

Las infracciones contra los derechos que confiere la LPI pueden ser castigadas mediante el ejercicio de acciones **civiles, penales** y **administrativas.**

- Las sanciones varían en función del daño que causen las infracciones y pueden ser, entre otras:
- Suspensión de la actividad de la organización que ha infringido la Ley.
- Prohibición de reanudación de la actividad.
- Inutilización, precintado o destrucción del material, incluido software y hardware o web, utilizado para reproducir contenidos sin derecho.
- Intervención de los ingresos obtenidos con la actividad ilícita.

saber más

SGAE - Sociedad General de Autores y Editores

Es una sociedad privada de gestión colectiva, que se dedica a gestionar los derechos de autor de sus socios, principalmente artistas y empresarios del negocio de la cultura.

sgae.es

saber más

Brigada de Investigación Tecnológica (BIT)

http://www.policia.es/bit/

Grupo de Delitos Telemáticos de la Guardia Civil (GDT)

https://www.gdt.guardiacivil.es/

caso **práctico** inicial

Si deseamos que nadie pueda copiar los contenidos de nuestra página web, tendremos que incluir una cláusula de ***copyright.***

Si los contenidos pudieran ser copiados, podemos incluir una cláusula ***Creative Commons*** con la modalidad de licencia elegida.

Piratería informática

Es uno de los términos más conocidos en el campo de los delitos telemáticos y afecta directamente a la propiedad intelectual. Ya dijimos en su momento que a los *hackers* se les suele llamar «piratas» sin ser correcta esta utilización del término aplicado al intrusismo informático, ya que **por piratería informática se entiende la distribución o reproducción ilegal de software comercial para su utilización empresarial o particular.**

saber más

En el nuevo proyecto de Código Penal se excluye al *hacker* como criminal informático.

recuerda

Se llama *hacker* a una persona experta en informática, redes y programación que pone a prueba los sistemas, con frecuencia para detectar y aportar soluciones a los errores de seguridad.

Se llama *cracker* a quien utiliza esos conocimientos para causar daño en sistemas informáticos.

También se incluye en el concepto la copia no autorizada de material literario, musical, grafico o audiovisual para su distribución a través de internet. Sea deliberada o no, la piratería informática es ilegal y está castigada por la ley al considerarse un atentado contra los derechos de la propiedad intelectual o industrial.

Tipos de piratería

Los sistemas más usados de piratería informática, tanto para software como para archivos literarios o de audio y vídeo, son los siguientes:

- Distribución gratuita de copias por internet, principalmente mediante P2P.
- Venta ilegal de copias.
- Creación de programas para conseguir claves de activación de productos.
- Creación de programas para activar la licencia completa de un producto demo o de licencia limitada por tiempo.

ACTIVIDADES

14. Analiza la disposición final primera del texto del **anteproyecto de Ley de Economía Sostenible** *(puedes poner en el buscador* ***meh.es anteproyecto economía sostenible,*** *para observarlo en la página del Ministerio de Economía y Hacienda)* o si ya está publicada la Ley, consúltala y responde a las siguientes preguntas:

a) ¿En qué leyes, de las que hemos estudiado en esta unidad, se producen cambios con la entrada en vigor de la Ley de Economía Sostenible?

b) ¿Qué Comisión se crea que tiene potestad para interrumpir la prestación de un servicio de la sociedad de la información o para retirar los contenidos que vulneren la propiedad intelectual por parte de un prestador con ánimo de lucro, directo o indirecto, o de quien pretenda causar un daño patrimonial?

ACTIVIDADES

15. Analiza los siguientes mensajes que aparecieron en periódicos digitales en enero de 2010. A continuación responde a las preguntas que se formulan:

Periódico ABC. Copyright © ABC (...) Reservados todos los derechos. Queda prohibida la reproducción, distribución, comunicación pública y utilización, total o parcial, de los contenidos de esta web, en cualquier forma o modalidad, sin previa, expresa y escrita autorización, incluyendo, en particular, su mera reproducción y/o puesta a disposición como resúmenes, reseñas o revistas de prensa con fines comerciales o directa o indirectamente lucrativos, a la que se manifiesta oposición expresa.

Periódico El Plural. El Plural publica todos sus contenidos bajo licencia Creative Commons. Esta licencia permite que el autor fije las condiciones con las que distribuye su obra en soporte digital.

Se permite:

- Copiar, citar y distribuir cualquiera de los contenidos de elplural.com.
- La utilización de los contenidos de elplural.com en cualquier otra publicación, sea o no de carácter comercial.
- La creación y distribución de obras derivadas de los contenidos de elplural.com.

Bajo las siguientes condiciones:

- En cualquiera de los tres casos deberá reconocerse y citarse la autoría de elplural.com y, si la obra se distribuye por internet, incluir un enlace con la URL original.
- Los contenidos creados a partir de la modificación de informaciones originales de elplural.com deberán publicarse bajo este mismo sistema de licencia.

La elección del sistema de licencias Creative Commons forma parte del compromiso con el progreso de elplural.com y de la apuesta de este periódico por la libre distribución de contenidos en internet.

Periódico El País. Todos los derechos reservados. En virtud de lo dispuesto en los artículos 8 y 32.1, párrafo segundo, de la Ley de Propiedad Intelectual, quedan expresamente prohibidas la reproducción, la distribución y la comunicación pública, incluida su modalidad de puesta a disposición, de la totalidad o parte de los contenidos de esta página web, con fines comerciales, en cualquier soporte y por cualquier medio técnico, sin la autorización de EDICIONES EL PAÍS. El USUARIO se compromete a respetar los derechos de Propiedad Intelectual e Industrial titularidad de EDICIONES EL PAÍS. Podrá visualizar los elementos del Site e incluso imprimirlos, copiarlos y almacenarlos en el disco duro de su ordenador o en cualquier otro soporte físico siempre y cuando sea, única y exclusivamente, para su uso personal y privado. El USUARIO deberá abstenerse de suprimir, alterar, eludir o manipular cualquier dispositivo de protección o sistema de seguridad que estuviera instalado en el las páginas de EDICIONES EL PAÍS.

a) Indica el nombre o nombres de periódicos, de los arriba reseñados, que contienen la cláusula de *Copyright*.

b) ¿De cuál o cuáles de ellos se deduce que puede copiarse contenido si no es con ánimo de lucro?

c) ¿Qué periódico parece indicar que no puede copiarse contenido alguno ni siquiera sin ánimo de lucro?

16. Investiga qué es una licencia Creative Commons y responde a las siguientes cuestiones:

a) Indica las modalidades de licencias Creative Commons.

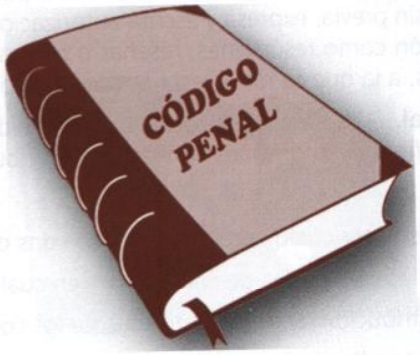
b) Explica qué modalidad de licencia Creative Commons utiliza el periódico El Plural.

17. Busca información sobre las siguientes **operaciones** del Grupo de Delitos Telemáticos de la Guardia Civil e indica a continuación qué tipo de delito se cometió en cada una de ellas:

PIOLÍN	RONNIE
GALA	CLON
POLICARBONATO	PHESCA
PAMPA	SANTIAGO

Código Penal

El Código Penal recoge varios delitos que pueden cometerse en internet. En algunos casos deja explícita la relación entre las telecomunicaciones y los delitos y en otros casos se trata de delitos generales que también pueden cometerse usando las tecnologías de la información y la comunicación.



a) **Estafas.** Artículo 248

«Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

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 terceros.

La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas previstas en este artículo».

b) **Delitos sexuales relacionados con menores de edad.** Artículos 185 a 189

En estos artículos se señalan las penas que se aplican en casos de corrupción de menores o personas con incapacidad.

c) **Delitos contra la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos**

- El artículo 197 contempla las penas con las que se castigará:
  - A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.
  - A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.

– Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.

En el mismo artículo se señala la mayor gravedad de las infracciones cuando quien las cometa fuese responsable de los ficheros cuyos secretos se revelen.

- En el artículo 278.1 se hace referencia a las penas con las que se castigará a quien realice las mismas acciones que explica el artículo 197, siempre que sea con el fin de descubrir secretos de empresa.
- El artículo 264.2 trata de las penas que se impondrán 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.

d) Delitos contra la propiedad intelectual y derechos afines

- El artículo 270 establece el castigo para quienes reproduzcan, distribuyan o comuniquen públicamente, en su totalidad o en parte, una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.
- El artículo 273 trata las penas que se impondrán a quienes, sin consentimiento del titular de una patente, fabriquen, importen, posean, utilicen, ofrezcan o introduzcan en el comercio objetos amparados por tales derechos, con fines comerciales o industriales.

e) Falsedad

En los artículos 386 y siguientes se enumeran los casos de falsedad de documentos, moneda y tarjetas, y se explica en concreto la creación o la tenencia de programas de ordenador orientados a cometer delitos de falsedad.

f) Amenazas, calumnias o injurias

Los artículos 169 y siguientes se refieren a las amenazas por cualquier medio de comunicación, lo que incluye la telemática. Asimismo, el artículo 205 y siguientes se refieren a las calumnias e injurias proferidas por cualquier medio equivalente a la imprenta o la radiodifusión, lo que incluye internet.

ACTIVIDADES

18. Localiza el Código Penal e indica de qué tratan los artículos 206 y 209 y qué tipo de sanciones se aplicarán a quienes procedan con las conductas que en ellos se especifican. ¿Tienen estos artículos algo que ver con internet?

19. El artículo 215 se refiere a las personas que hayan sido víctimas de calumnias e injurias. ¿Tienen que hacer algo estas personas o la sanción se producirá de forma automática sobre quien las haya proferido?

20. Explica qué entiendes del contenido del artículo 212.

4. Legislación internacional sobre seguridad informática

4.1. Directivas Europeas

Una Directiva de la Unión Europea es un acuerdo vinculante tomado por los Estados miembros. Básicamente consiste en una exposición de objetivos que se deben conseguir, dejando en libertad a los países miembros para que establezcan libremente los medios que lleven a la consecución de los objetivos. Por ese motivo la legislación española en materia de seguridad informática está en constante evolución, con el fin de incluir las Directivas europeas en nuestra normativa.

En el desarrollo de esta unidad didáctica, en los márgenes, se han incluido las directivas europeas que se han ido incorporando a nuestras leyes.

4.2. Criterios comunes

↑ Logo de Common Criteria.
http://www.commoncriteriaportal.org/

Son certificados internacionales que miden la fiabilidad de todo tipo de productos de las tecnologías de la información y la comunicación, ya sean software o hardware. Son más conocidos por su nombre en inglés **Common Criteria** y son emitidos por organismos de certificación de varios países.

Fue a principios de la década de 1980 cuando se empezaron a desarrollar en Estados Unidos unos criterios de seguridad para las tecnologías de la información, recogidos bajo el nombre de **TCSEC** *(Trusted Computer System Evaluation Criteria)*, que se publicaron en el llamado *Libro Naranja* y que siguieron desarrollándose posteriormente en todo el mundo, adaptándose constantemente a la evolución de las tecnologías de la información.

Esa evolución llegó hasta el establecimiento de los certificados internacionales Common Criteria, también conocidos como **ISO-IEC 15408,** reconocidos en casi todo el mundo y emitidos por 14 países, entre ellos España. En nuestro país el organismo que emite certificaciones Common Criteria es el **Centro Criptológico Nacional,** dependiente del **Centro Nacional de Inteligencia,** actualmente dentro del Ministerio de Defensa.

↑ Centro Criptológico Nacional, emisor de certificados de seguridad para las tecnologías de la información.
https://www.ccn.cni.es/

Para llevar a cabo la evaluación de los productos de las tecnologías de la información, existen laboratorios acreditados por el CCN que cumplen con los requisitos que determina el Organismo de Certificación, tras someterse al plan de seguimiento y auditorías.

PRÁCTICA PROFESIONAL

Legislación informática y auditoría

En esta unidad hemos conocido la legislación sobre seguridad informática, tanto a nivel de protección de datos de carácter personal como sobre derechos de autor y delitos informáticos.

Prácticamente viene a ser un compendio de lo que se ha aprendido a lo largo del libro, por lo que esta práctica profesional servirá para evaluar los conocimientos adquiridos y su aplicación en el campo de la legalidad.

OBJETIVOS

- Reconocer las medidas de seguridad que se tienen que aplicar a ficheros que contienen datos de carácter personal.
- Demostrar los conocimientos sobre las exigencias legales que comporta el comercio electrónico en supuestos concretos.
- Recordar los conceptos de política de seguridad y plan de contingencias.
- Realizar una auditoría completa de un pequeño sistema de información.

INSTRUCCIONES

1. Análisis de medidas de seguridad exigidas por la LOPD

En primer lugar presentamos una tabla con una serie de medidas de seguridad que deben cumplirse obligatoriamente cuando se tratan ficheros con datos de carácter personal, como ordena la LOPD y su Reglamento.

Marca con una X, en las columnas de la derecha, a qué nivel o niveles hay que aplicar las medidas indicadas en la columna de la izquierda.

Medidas de seguridad	Nivel básico	Nivel medio	Nivel alto
Cifrado de datos para telecomunicaciones			
Registro de incidencias			
Formación y responsabilidad del personal			
Auditoría de seguridad			
Responsable de seguridad			
Copias de respaldo y recuperación			
Identificación y autenticación para acceso a datos, de forma obligatoria			
Documento de seguridad			
Gestión de soportes de los datos			
Medidas adicionales de seguridad para copias de respaldo y recuperación			

PRÁCTICA PROFESIONAL

2. Comercio electrónico

Una empresa que ha decidido vender sus productos a través de internet, te consulta sobre las medidas que debe cumplir la página web a través de la cual se realizarán los pedidos. Ten en cuenta que para realizar un pedido se solicitarán ciertos datos imprescindibles del cliente. El sistema de cobro, en principio, se realizará solamente contra reembolso.

Explícales cuáles deben ser las medidas necesarias para estar dentro de la legalidad en nuestro país y cuáles son las principales leyes que deben respetarse en este supuesto.

3. Un supuesto concreto de fichero de datos de carácter personal

- Un trabajador autónomo, que no tiene a nadie contratado, realiza determinados trabajos para los que necesita tener un fichero que contiene los siguientes datos de sus clientes:
  - Nombre y apellidos
  - Dirección, localidad y provincia
  - DNI
  - Estatura
  - Peso
  - Raza

  a) Al ser autónomo y trabajar solo, ¿tendrá que cumplir lo establecido por la LOPD y por el RLOPD?

  b) ¿A qué nivel de seguridad pertenece el fichero de datos que maneja este trabajador autónomo?

- Después de realizar unas consultas legales, le han comunicado a este trabajador que tiene que acogerse a lo establecido por la LOPD.

  c) ¿Deberá tener un documento de seguridad? ¿Qué apartados imprescindibles debería contener dicho documento?

- Si tiene que enviarle a un cliente, por correo electrónico, su propio registro de datos para que compruebe y realice modificaciones si las hubiera:

  d) ¿Debería cifrarlos para enviarlos? ¿Por qué? Indica un sistema de cifrado de datos que conozcas.

- El empleado guarda su fichero de datos en su propia oficina.

  e) ¿Necesita utilizar algún control de acceso a dicho local? Si consideras que es necesario, ¿qué mecanismo de control de acceso al entorno físico propondrías?

4. Proyecto: auditoría informática

Hasta el momento presente, no hay nada legislado en cuanto a quién puede realizar una auditoría informática en España ni qué sistemas debe utilizar para llevarla a cabo. Por lógica se entiende que ha de ser una persona con conocimientos informáticos suficientes para ejecutarla. Tienes los conocimientos necesarios para realizar una auditoría a una pequeña organización. Sabes que la auditoría se tiene que hacer obligatoriamente, como mínimo cada dos años, en organizaciones públicas o privadas que traten datos de carácter personal de nivel medio y alto. En todo caso, cualquier empresa, aunque no maneje este tipo de datos, puede solicitar una auditoría de seguridad informática.

Sigue las indicaciones de tu profesor o profesora sobre una empresa ficticia a la que tienes que realizar una auditoría.

Para ponerte manos a la obra, puedes comenzar por la parte exterior del sistema de información, es decir, el entorno físico. Para terminar, puedes hacer un análisis de la seguridad del software y de las comunicaciones. En medio hay varios temas que debes incluir en tu auditoría, como es la seguridad del hardware y el personal que pertenece a dicho sistema de información.

A modo de esquema orientativo, te dejamos una lista de pasos a seguir:

a) Comprobar si existe una **política de seguridad** en la empresa. De no existir, puedes recomendar una política mínima adecuada a la actividad que realiza.

b) Verificar si la política de seguridad está en conocimiento de todas las personas que pertenecen al sistema. En caso contrario, recomendar su puesta en conocimiento.

c) Confirmar si existe un **plan de contingencias.** En caso contrario, puedes redactar y recomendar un pequeño plan para recuperación en caso de desastre.

d) Realizar una **auditoría de seguridad** en todos los niveles del sistema de información, tal y como hemos estudiado a lo largo de este libro **(entorno físico, hardware, red, software, personal, comunicaciones...),** indicando para cada nivel:

- **Puntos fuertes.** Qué medidas de seguridad, que resultan efectivas, se están aplicando sobre ese nivel.
- **Puntos débiles.** Normas de seguridad que no están establecidas y deberían estarlo, o existen pero no se practican.
- **Sistema de auditoría.** Qué método has utilizado para localizar los puntos débiles y fuertes. Por ejemplo: inspección visual para la seguridad del entorno físico, programas que has utilizado para la monitorización del hardware, del software o de las comunicaciones, etc.
- **Recomendaciones de seguridad.** Si sobre algún nivel existen puntos débiles, redacta las recomendaciones que consideres oportunas para resolver las vulnerabilidades existentes.

Ejemplo:

a) Entorno físico

Puntos fuertes: puerta metálica con cerradura de seguridad. Alarma contra intrusos.

Puntos débiles: no hay extintor de incendios en el local.

Sistema de auditoría: control visual.

Recomendaciones de seguridad: instalación de un extintor de incendios adecuado a equipos electrónicos e informáticos.

b) Seguridad del hardware

Puntos fuertes, puntos débiles, sistema de auditoría, recomendaciones...

c) Otros

MUNDO LABORAL

Delitos informáticos en la actualidad

Resumen de la charla de Juan Rodríguez, jefe del Equipo de Investigación Tecnológica de la Policía Judicial de Huesca, dirigida al alumnado del IES Sierra de Guara:

En primer lugar, Rodríguez informó a los alumnos de la legislación española en este ámbito e hizo hincapié en el **Tratado de Lisboa,** que supondrá una unificación de la legislación penal y procesal a nivel europeo. A continuación desgranó las peculiaridades de cada delito y las técnicas para detenerlos, englobados en los cuatro grandes bloques del **Convenio sobre la Ciberdelincuencia de Budapest.**

El primer apartado comprende los delitos contra la **propiedad intelectual,** como son las descargas ilegales. El siguiente bloque encierra los delitos contra la **confidencialidad y la disponibilidad de datos** en los sistemas informáticos, el denominado «hacking». El tercero contiene los delitos relacionados con la **falsificación y los fraudes,** como el «phishing» y todo tipo de **timos y estafas,** por ejemplo los portales de subastas o las páginas falsas que reclaman ayudas para catástrofes como la de Haití.

El último bloque engloba los **delitos de contenido,** la violencia, el «bullying», los distintos tipos de provocación sexual, las amenazas o la pedofilia. Rodríguez advirtió en este punto del peligro de las redes sociales, ya que si antes este tipo de conductas se desarrollaban principalmente en el chat, ahora se van desplazando hacia esta otra forma de establecer contacto.

Juan Rodríguez reveló que no existe un perfil definido del delincuente y que es «laborioso luchar contra este tipo de delitos». «Internet es un sistema global y la investigación es complicada, pero hemos desarrollado equipos y programas muy avanzados para luchar contra este tipo de delincuencia, y aunque las técnicas que usan los delincuentes también avanzan muy rápidamente, nosotros contamos con la experiencia y el personal que se dedica exclusivamente a esto y que hace todo lo posible», subrayó.

Alba Aguilón. Diario del Alto Aragón

http://www.diariodelaltoaragon.es/NoticiasDetalle.aspx?Id=615059

Actividades

1. ¿En qué año se celebró en Budapest el Convenio sobre la Ciberdelincuencia?

2. ¿A qué cuatro grandes bloques del Convenio sobre Ciberdelincuencia se refiere?

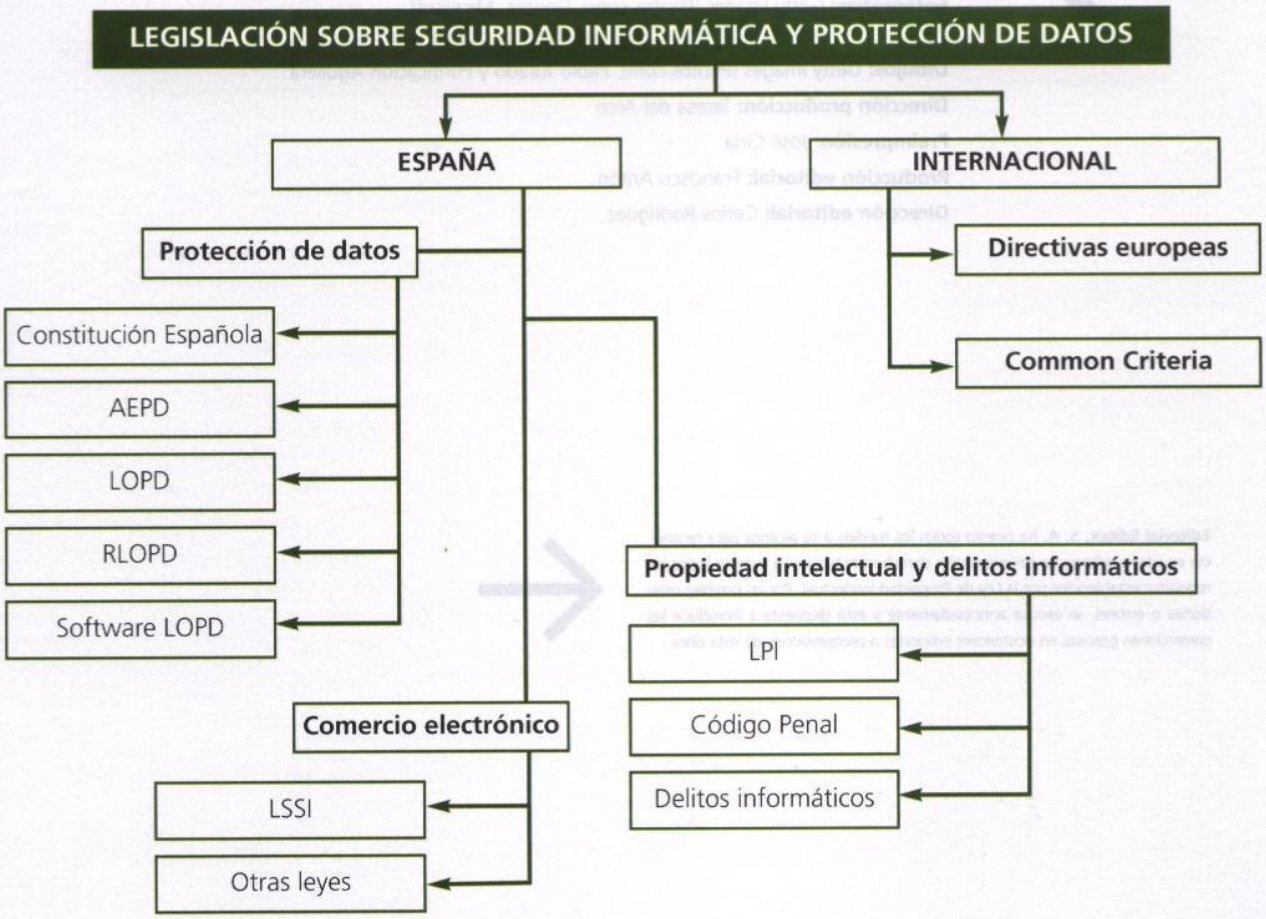
3. Cuando se descarga música, películas u otro material de internet, ¿se está realizando una descarga ilegal?

4. ¿Qué es el *bullying?*

5. ¿En qué entorno afirma que se desarrollan principalmente en la actualidad comportamientos de *bullying?*

6. Según Juan Rodríguez, ¿existe un perfil definido del ciberdelincuente?

EN **RESUMEN**



EVALÚA TUS **CONOCIMIENTOS**

1. En la legislación española, ¿dónde está el origen del derecho al respeto de los datos de carácter personal?
   a) En la LOPD.
   b) En la costumbre.
   c) En la LSSI.
   d) En la Constitución.
2. ¿Qué ente se encarga de velar por el cumplimiento de la ley en materia de protección de datos?
   a) El Ministerio de Interior.
   b) La SGAE.
   c) La AEPD.
   d) El Registro General de Protección de Datos.
3. Señala qué tipos de datos requieren llevar un registro de incidencias en la empresa.
   a) Nombre y apellidos.
   b) Solvencia, patrimonio y crédito.
   c) Salud.
   d) Vida sexual.
4. La SGAE se ocupa de velar por los derechos con los que ampara la Ley de Propiedad Intelectual a:
   a) Todos los autores y editores españoles.
   b) Los internautas.
   c) Sus socios.
   d) Los titulares de páginas web con *copyright*.

Soluciones: 1d, 2c, 3a, 3b, 3c, 3d, 4c

Edición: Gonzalo Morlanes

Diseño de cubierta: Paso de Zebra

Fotocomposición, maquetación y realización de gráficos: Fer Fotocomposición

Fotografías: Getty Images (Photos.com), Google, Microsoft, Purificación Aguilera, Softrónica, Youtube, fuentes citadas y archivo Editex

Dibujos: Getty Images (Photos.com), Pablo Jurado y Purificación Aguilera

Dirección producción: Teresa del Arco

Preimpresión: José Ciria

Producción editorial: Francisco Antón

Dirección editorial: Carlos Rodríguez

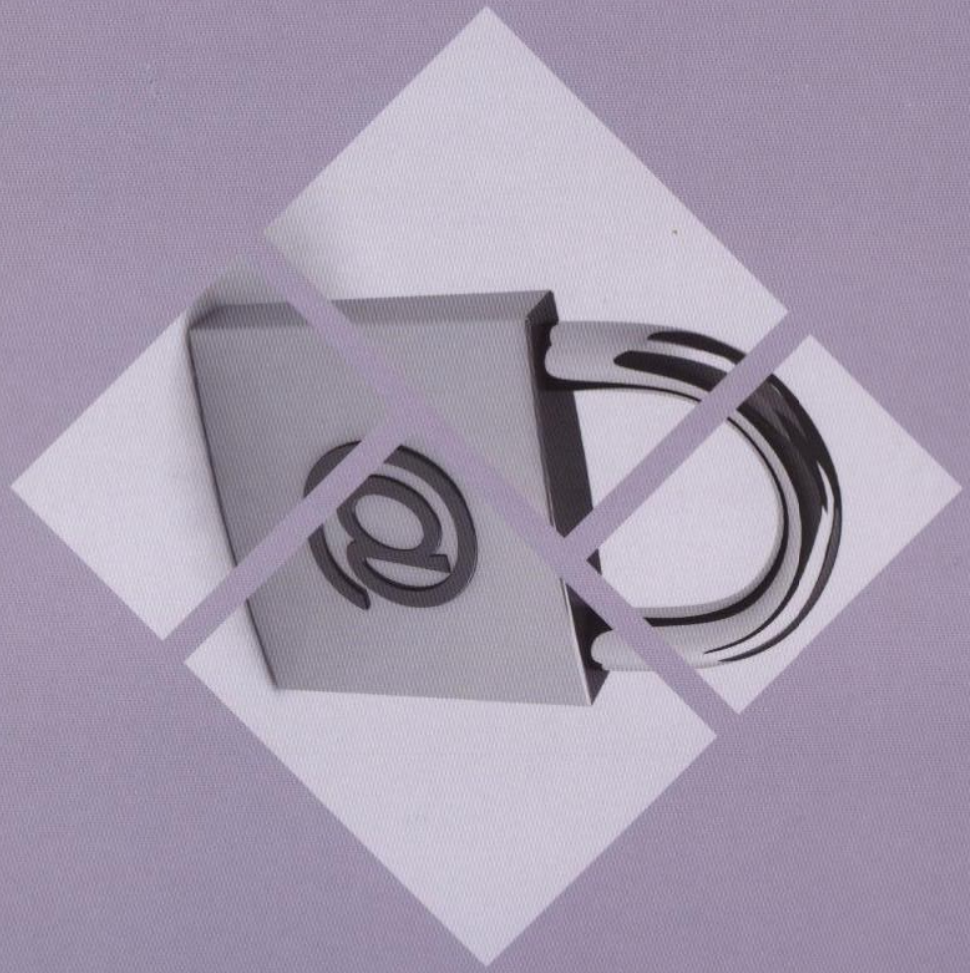
El presente material didáctico ha sido creado por iniciativa y bajo la coordinación de **Editorial Editex, S. A.**, conforme a su propio proyecto editorial.

Vía Dos Castillas, 33. C.E. Ática 7, edificio 3, planta 3ª, oficina B
28224 Pozuelo de Alarcón (Madrid)
ISBN: 978-84-9771-657-4
Depósito Legal: M-3171-2010
Imprime: Gráficas Rógar
C/ Mina del Cotorro - Parcela 59
Polígono Industrial Alparrache
28600 Navalcarnero (Madrid)
Impreso en España - Printed in Spain

EDITEX

Seguridad informática

INFORMÁTICA Y COMUNICACIONES



ISBN 978-84-9771-657-4