Seguridad Informática

MACMILLAN
Profesional

Seguridad Informática

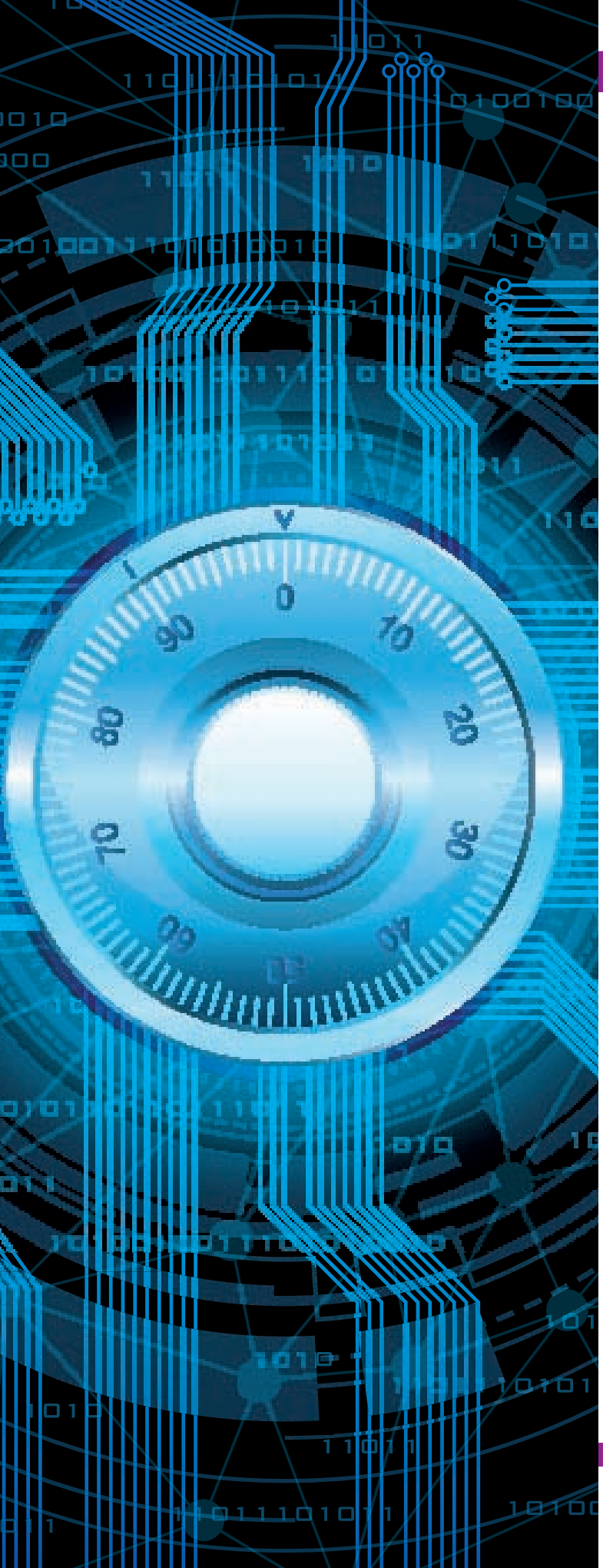
Gema Escrivá Gascó

Rosa Mª Romero Serrano

David Jorge Ramada

Ramón Onrubia Pérez

MACMILLAN
Profesional



unidad 1

Introducción a la seguridad informática

SUMARIO

- Seguridad de la información y seguridad informática
- Conceptos básicos relacionados con la seguridad informática
- Principios básicos de la seguridad informática
- Políticas de seguridad
- Planes de contingencia

OBJETIVOS

- Conocer las diferencias entre seguridad de la información y seguridad informática.
- Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
- Describir cuáles son los principios básicos de la seguridad.
- Conocer qué son y qué utilidad tienen las políticas de seguridad.
- Aprender en qué consisten los planes de contingencia.

1 >> Seguridad informática y seguridad de la información

Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma a la ruina. Extendiendo este concepto de seguridad al mundo de las telecomunicaciones y la informática, puede entenderse desde dos puntos de vista: **seguridad de la información y seguridad informática.**

La **seguridad de la información** es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información:

- **Integridad:** certificando que tanto la información como sus métodos de proceso son exactos y completos.
- **Confidencialidad:** asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados.
- **Disponibilidad:** permitiendo que la información esté disponible cuando los usuarios la necesiten.

Este término, por tanto, es un concepto amplio que engloba medidas de seguridad que afectan a la información independientemente del tipo de esta, soporte en el que se almacene, forma en que se transmita, etc.

La **seguridad informática,** por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida. Podemos distinguir los siguientes tipos:

- En función de lo que se quiere proteger:
  - **Seguridad física:** se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.
  - **Seguridad lógica:** mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.
- En función del momento en que tiene lugar la protección:
  - **Seguridad activa:** se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas). Por ejemplo, utilización de contraseñas.
  - **Seguridad pasiva:** comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras). Por ejemplo, las copias de seguridad.

Normas ISO/IEC 27000

Para gestionar de forma adecuada la seguridad de la información se han desarrollado un conjunto de estándares que se han convertido en el marco para establecer, implantar, gestionar y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Son las normas ISO/IEC 27000, desarrolladas por ISO *(International Organization for Standarization)* e IEC *(International Electrotechnical Commission)*.

Web

http://pwnies.com: página web de los premios Pwnies, distinción que reconoce lo mejor y lo peor de la seguridad informática durante el último año.

Actividades propuestas

1·· Debate con tus compañeros de clase: ¿a qué crees que se deben la mayoría de los fallos de seguridad?

2·· Realiza una tabla comparando ejemplos de seguridad pasiva y activa del campo de la informática y del campo de los vehículos.

2 >> Conceptos básicos en materia de seguridad

En el mundo de la seguridad de la información e informática, es habitual manejar una terminología específica (activos, vulnerabilidades, amenazas, ataques, riesgos, impacto, desastre, contingencias, etc.) que explicaremos a lo largo de este epígrafe.

2.1 > Activos

Un activo se define como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, consideraremos como activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc.

La seguridad informática tiene como objetivo proteger dichos activos, por lo que la primera labor será identificarlos para establecer los mecanismos necesarios para su protección y analizar la relevancia de los mismos en el proceso de negocio de la organización. No tiene sentido gastar miles de euros en proteger activos no importantes para el negocio o que no tengan un valor que justifique ese gasto.

Desde el punto de vista de la informática, los principales activos de una empresa son los siguientes:

- **Información:** todo aquel elemento que contenga datos almacenados en cualquier tipo de soporte. Como por ejemplo, documentos, libros, patentes, correspondencia, estudios de mercado, datos de los empleados, manuales de usuario, etc.
- **Software:** programas o aplicaciones que utiliza la organización para su buen funcionamiento o para automatizar los procesos de su negocio. Entre estos se pueden encontrar las aplicaciones comerciales, los sistemas operativos, etc.
- **Físicos:** toda la infraestructura tecnológica utilizada para almacenar, procesar, gestionar o transmitir toda la información necesaria para el buen funcionamiento de la organización. También estaría incluida en esta categoría la estructura física de la organización, tal como la sala de servidores, los armarios, etc.
- **Personal de la organización** que utilice la estructura tecnológica y de comunicación para el manejo de la información.

2.2 > Vulnerabilidades

En el campo de la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático. Estas debilidades, también conocidas como “agujeros de seguridad”, pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, a descuidos en la utilización de los sistemas, etc. Por ejemplo, no utilizar ningún tipo de protección frente a fallos eléctricos o carecer de mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos.

MAGERIT v. 3

MAGERIT es la metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica. Es un método formal adoptado por las Administraciones Públicas para investigar los riesgos que soportan los sistemas de información y recomendar las medidas adecuadas que deberán adoptarse para poder controlar dichos riesgos.

Es muy importante corregir cualquier vulnerabilidad detectada o descubierta, porque constituye un peligro potencial para la estabilidad y seguridad del sistema en general.

Las vulnerabilidades de algunas aplicaciones pueden permitir una escalada de privilegios, con lo que un atacante podría conseguir más privilegios de los previstos. Esto podría implicar que en algunos casos llegaran a tener los mismos que los administradores, pudiendo controlar el sistema. Un ejemplo sería cuando una vulnerabilidad produce un fallo en un servidor web que permite que un atacante acabe accediendo al sistema como si se tratara de un administrador, con lo que podría realizar acciones reservadas a estos.

Para minimizarlas, los administradores de los sistemas informáticos deben actualizar periódicamente el sistema operativo y las aplicaciones y mantenerse actualizados en temas relacionados con la seguridad informática. Para ello pueden visitar páginas web especializadas en materia de seguridad informática, como los equipos de respuesta a incidentes de seguridad de la información (CERT o CSIRT) o páginas web de seguridad, como www.hispasec.com, etc.

2.3 > Amenazas

Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como, por ejemplo, un desastre natural, en la mayoría de casos es necesaria una intención de producir daño.

Las amenazas se suelen dividir en pasivas y activas, en función de las acciones realizadas por parte del atacante:

- **Amenazas pasivas**, también conocidas como "escuchas". Su objetivo es obtener información relativa a una comunicación. Por ejemplo, los equipos informáticos portátiles que utilizan programas especializados para monitorizar el tráfico de una red WiFi.
- **Amenazas activas**, que tratan de realizar algún cambio no autorizado en el estado del sistema, por lo que son más peligrosas que las anteriores. Como ejemplos se encuentran la inserción de mensajes ilegítimos, la usurpación de identidad, etc.

Otra posible clasificación, en función de su ámbito de acción, sería diferenciar entre amenazas sobre la seguridad física, lógica, las comunicaciones o los usuarios de la organización.

MAGERIT presenta la siguiente clasificación de amenazas:

Grupos de amenazas	Ejemplos
Desastres naturales	Fuego, daños por agua, desastres naturales.
Desastres industriales	Fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
Errores y fallos no intencionados	Errores de usuarios, errores de configuración, etc.
Ataques deliberados	Manipulación de la configuración, suplantación de la identidad del usuario, Difusión de software dañino, etc.

2.4 > Ataques

Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. De hecho, en alguna metodología como MAGERIT se distingue entre ataques (acciones intencionadas) y errores (acciones fortuitas).

Como ejemplos de ataques, que desarrollaremos a lo largo de este libro, podemos citar la utilización de programas para conseguir acceso al servidor de forma ilegítima o la realización de ataques de denegación de servicio para colapsar el servidor.

Normalmente un ataque informático pasa por las siguientes fases:

- **Reconocimiento.** Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.
- **Exploración.** Se trata de conseguir información sobre el sistema a atacar, como por ejemplo, direcciones IP, nombres de *host,* datos de autenticación, etc.
- **Obtención de acceso.** A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.
- **Mantener el acceso.** Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.
- **Borrar las huellas.** Finalmente, se intentarán borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado.

En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a estas herramientas, como las orientadas a explotar las debilidades del factor humano.

Es el caso de la **ingeniería social**, que consiste en la obtención de información confidencial y/o sensible de un usuario mediante métodos que son propios de la condición humana. El ataque más simple sería el de engañar al usuario haciéndose pasar por el administrador del sistema de su organización para obtener alguna información de relevancia.

Ejemplos

Ataque de ingeniería social

Un usuario malicioso haciéndose pasar por el administrador de la organización envía un correo electrónico a los usuarios para obtener información, en este caso la contraseña, de manera fraudulenta.

```
From: Administrador <admin@organizacion.com>

To: Usuario <user@organizacion.com>

Se está llevando a cabo un mantenimiento del sistema con el objetivo de
conseguir un óptimo funcionamiento. Para poder conseguirlo, es necesario
que se cambie la contraseña, para ello pinche en el siguiente enlace.

http://mantenimiento.organizacion.com

Gracias por su colaboración,
```

Casos prácticos 1

Análisis de vulnerabilidades, ataques y amenazas a un sistema

•• Lee el siguiente artículo y responde a las preguntas que se hacen a continuación del mismo.

La compañía de seguridad para Internet BitDefender ha localizado un nuevo fraude en la red social Facebook que utiliza para propagarse el etiquetado en las fotos que permite dicha red social.

El método utilizado es el siguiente: un usuario es etiquetado en una foto de una chica joven y vestida de manera provocativa. Junto a esa foto, se incluye un mensaje que dice: "Descubre quiénes son tus principales seguidores", junto con un *link* para utilizar una aplicación que permitiría conocer esa información.

Si el usuario pincha en el *link*, será redirigido a una aplicación que, por un lado, le pedirá su nombre de usuario y contraseña y, por otro, le pedirá permisos para publicar mensajes en su muro y para acceder a su lista de contactos en Facebook. Una vez haya introducido los datos y dado permiso a la aplicación, esta mostrará un mensaje de error, señalando que no está disponible en ese momento.

Sin embargo, inmediatamente, comenzarán a publicarse nuevas fotos en la galería del usuario en la que serán etiquetados todos sus amigos. Además, en el muro de estos aparecerá que alguien les ha etiquetado en esa foto, junto con el comentario inicial ("Descubre quiénes son tus principales seguidores") más el *link* que conduce a la aplicación falsa.

En el momento en que uno de esos amigos pinche en el *link* e instale la aplicación creyendo que su amigo ya la ha aprobado y que se la está recomendando, el proceso volverá a comenzar. De esta manera, la aplicación consigue un efecto viral, propagándose por la red social.

Fuente: Europa Press. Madrid. 13/04/11

a) ¿De qué tipo de ataque se trata?
b) Analiza las vulnerabilidades y amenazas a ese sistema.
c) ¿Qué recomendaciones darías para evitar esta situación?

Solución ••

a) Se trata de un ataque basado en ingeniería social, realizado con la finalidad de conseguir los datos del usuario para propagarse.
b) La **vulnerabilidad** es el elemento personal, encarnado por la confianza del usuario en los contenidos recibidos, que le lleva a conceder privilegios totales al atacante. La **amenaza** existente es un tipo de amenaza pasiva, consistente en suplantar la identidad del usuario para permitir al atacante conseguir sus fines.
c) Se recomienda desconfiar tanto de las fotos como de los mensajes de este tipo, que pretenden llamar la atención ante situaciones curiosas. Al mismo tiempo, se debe desconfiar de las aplicaciones que supuestamente realizan acciones que en realidad no pueden llevarse a cabo, como por ejemplo saber cuántas veces han visitado tu perfil.

Actividades propuestas

3•• ¿Cuál es el activo más valioso para una empresa?

a) ¿Qué vulnerabilidades podrían afectarle?
b) ¿Qué amenazas son las que podrían afectarle? Clasifícalas.

PILAR

Es una aplicación implementada por la metodología MAGERIT, para el análisis y gestión de riesgos de un sistema de información. Ha sido desarrollada por el Centro Criptológico Nacional (CCN) y es de amplia utilización en la Administración Pública española.

2.5 > Riesgos

Existen diversas definiciones para definir el término riesgo; entre todas ellas destacamos las siguientes:

- Según la UNE-71504:2008, un riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.
- El Centro Criptológico Nacional define el riesgo como la probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y causando daño (impacto) en un proceso o sistema.

El riesgo es, por tanto, una medida de la probabilidad de que se materialice una amenaza. Por ejemplo, si la instalación eléctrica del edificio es antigua, existirá un riesgo elevado de sufrir una interrupción del servicio en caso de producirse una subida de tensión.

El coste asociado a la reducción de esa cifra aumenta de manera exponencial frente a la necesidad de minimizar el riesgo, por lo que se debe tratar de obtener un factor coste/riesgo que sea asumible por la organización. Ningún sistema de seguridad debería tener un coste superior al del sistema en conjunto o al de la información que protege.

Para poder establecer unos procedimientos de seguridad adecuados, será necesario realizar una clasificación de los datos y un análisis de riegos, con el fin de establecer prioridades y realizar una administración más eficiente de los recursos de la organización.

En el **análisis de riesgos** hay que tener en cuenta qué activos hay que proteger, sus vulnerabilidades y amenazas, así como la probabilidad de que estas se produzcan junto con el impacto de las mismas. Además, habrá que tener también en cuenta durante cuánto tiempo y qué esfuerzo y dinero se está dispuesto a invertir.

Los resultados del análisis de riesgos permiten recomendar qué medidas se deberán tomar para conocer, prevenir, impedir, reducir o controlar los riesgos previamente identificados y así poder reducir al mínimo su potencialidad o sus posibles daños.

Existen diferentes niveles de riesgo a los que puede estar expuesto un activo. El nivel dependerá de la probabilidad de que se materialice una amenaza y al grado de impacto producido. Por ejemplo:

Nivel	Tipo de riesgo
Alto	Robo de información Robo de hardware
Medio	Accesos no autorizados
Muy bajo	Inundaciones

Hay que tener en cuenta que el riesgo cero no existe, ya que no es posible prever y evitar todas las posibles situaciones que podrían afectar a nuestros sistemas.

2.6 > Impacto

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionamiento normal; estas consecuencias para la empresa reciben el nombre de impacto. Dicho de otra forma, el impacto sería el alcance producido o daño causado en caso de que una amenaza se materialice.

Dos organizaciones pueden verse afectadas en diferente medida ante la materialización de la misma amenaza si han adoptado estrategias diferentes para solucionarla. Así, el impacto del borrado del disco duro ocasionado por un virus informático será muy escaso en una empresa que realiza periódicamente copias de seguridad de la información importante, pero será bastante grave en una empresa que no lleva a cabo copias de seguridad regularmente.

Un impacto leve no afecta prácticamente al funcionamiento de la empresa y se produce en organizaciones que han identificado las amenazas y han establecido las pautas a seguir en el caso de que se materialicen. Por otro lado, un impacto grave afecta seriamente a la empresa pudiendo ocasionar su quiebra y se produce en organizaciones que no han considerado las consecuencias que supone para ellas la materialización de esa amenaza.

Las empresas deben, por tanto, identificar los impactos para la organización en el caso de que las posibles amenazas se produzcan. Esta tarea es uno de los objetivos del análisis de riesgos que debe realizar toda organización.

2.7 > Desastres

Según ISO 27001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque.

Un evento de este tipo puede destruir los activos de la empresa. Tradicionalmente se planteaba únicamente la destrucción de recursos físicos, como sillas, edificios, etc. pero hoy día las organizaciones se enfrentan a una nueva forma de desastre que afecta a los recursos lógicos, que constituye uno de sus principales activos: la información. Un desastre de este tipo podría ocasionar grandes pérdidas e incluso el cese de la actividad económica.

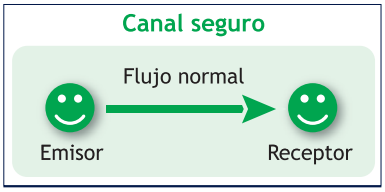
Las organizaciones deben estar preparadas ante cualquier tipo de desastre de manera que se reduzca el impacto que pueda ocasionar. Para ello, desarrollan e implantan planes de contingencia que permiten la prevención y recuperación de desastres informáticos.

Actividades propuestas

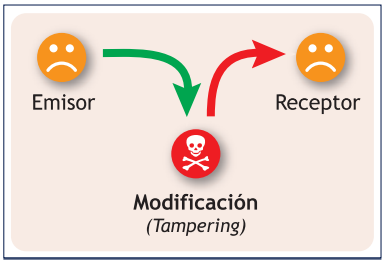
4·· ¿Crees que la evaluación de riesgos será igual para todas las empresas? ¿Por qué?

5·· Enumera posibles preguntas que podrían hacerse en la realización de una evaluación de riesgos.

6·· Busca en Internet aplicaciones comerciales que permitan realizar una evaluación de riesgos.



1.1. Flujo normal de la información.

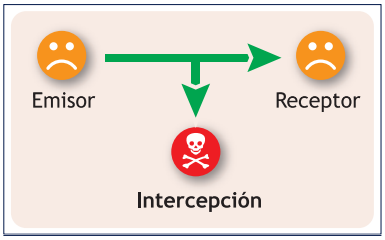


1.2. Violación de la integridad.

Sniffers

Sniffer es una palabra inglesa que significa "husmeo".

Un *sniffer* es un tipo de herramienta utilizada por atacantes para capturar información que circula por la red y no ha sido enviada para ellos. También se denomina así a los usuarios que husmean la información transmitida en una red.



1.3. Violación de la confidencialidad.

3 >> Principios de seguridad informática

Aunque la mayoría de expertos coinciden en que no existe ningún sistema totalmente seguro e infalible al 100%, se debe tratar de proteger la información y el sistema que la utiliza para ofrecer un nivel de seguridad razonable a los usuarios.

Para que un sistema se pueda considerar razonablemente seguro se debe garantizar que se cumplen los principios básicos de la seguridad informática: integridad, confidencialidad y disponibilidad.

3.1 > Integridad

La integridad es un principio básico de la seguridad informática que consiste en garantizar que la información solo pueda ser alterada por las personas autorizadas o usuarios legítimos, independientemente de si esa modificación se produce de forma intencionada o no. Así, por ejemplo, no se viola la integridad cuando usuarios autorizados modifican un registro de una base de datos o cuando un usuario que trabaja con la base de datos borra un registro que no debería por error.

La vulneración de la integridad tiene distinto significado según se produzca en un equipo o en una red de comunicaciones:

- **Equipo de trabajo.** Se produce violación de la integridad cuando un usuario no legítimo modifica información del sistema sin tener autorización para ello.
- **Red de comunicaciones.** Existe violación de la integridad cuando un atacante actúa como intermediario en una comunicación, recibe los datos enviados por un usuario, los modifica y se los envía al receptor (ataques *man-in-the-middle*). Un mecanismo que nos protege frente a este tipo de ataques es la firma electrónica, que se estudiará con más detalle en unidades posteriores.

3.2 > Confidencialidad

La confidencialidad es otro de los principios básicos de la seguridad informática que garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados.

La vulneración de la confidencialidad también afecta de forma diferente a equipos y redes:

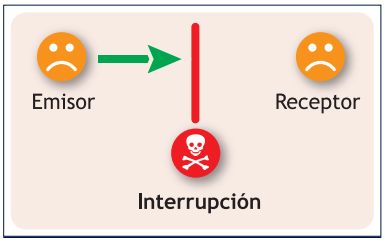
- **Equipo de trabajo.** Se produce una violación de la confidencialidad cuando un atacante consigue acceso a un equipo sin autorización, controlando sus recursos. Un ejemplo sería la obtención de las claves de acceso. Otro ejemplo, mucho más simple, se produce cuando un usuario abandona momentáneamente su puesto de trabajo, dejando su equipo sin bloquear y con información mostrándose en la pantalla.
- **Red de comunicaciones.** Se vulnera la confidencialidad de una red cuando un atacante accede a los mensajes que circulan por ella sin tener autorización para ello. Existen mecanismos que permiten protegerse frente este tipo de ataques, como el cifrado de la información o el uso de protocolos de comunicación.

3.3 > Disponibilidad

El tercer pilar básico de un sistema seguro es la disponibilidad, esto es, asegurar que la información es accesible en el momento adecuado para los usuarios legítimos.

La violación de la disponibilidad también se da de forma distinta en equipos y redes:

– **Equipos informáticos.** Se vulnera la disponibilidad de un equipo cuando los usuarios que tienen acceso a él no pueden utilizarlo. Por ejemplo, podría ser un virus que ha paralizado el sistema.
– **Redes de comunicaciones.** Se produce un ataque contra la disponibilidad cuando se consigue que un recurso deje de estar disponible para otros usuarios que acceden a él a través de la red. Existen una gran variedad de ataques que atentan contra la disponibilidad de un recurso en una red, como los ataques de denegación de servicio. Estos ataques, así como las técnicas que podemos utilizar para proteger las redes, se estudiarán en la unidad dedicada a la seguridad en redes.

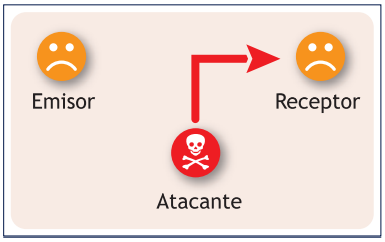


1.4. Violación de la disponibilidad.

3.4 > Otras características deseables en un sistema seguro

Además de los principios básicos que acabamos de ver, existen otros principios de seguridad que se consideran como deseables en todo sistema informático. Estos principios son los siguientes:

– **No repudio.** Este principio consiste en probar la participación de ambas partes en una comunicación. Por ejemplo, cuando se entrega la declaración de la renta telemáticamente, se firma con un certificado digital que solo puede poseer la persona que la presenta. La firma digital es una prueba irrefutable, de forma que impide que el ciudadano pueda negar o repudiar el trámite realizado. Este principio está estandarizado en la ISO-7498-2. Existen dos clases:
  • **No repudio de origen:** protege al destinatario del envío, ya que este recibe una prueba de que el emisor es quien dice ser.
  • **No repudio de destino:** protege al emisor del envío, ya que el destinatario no puede negar haber recibido el mensaje del emisor.
– **Autenticación.** Permite comprobar la identidad de los participantes en una comunicación y garantizar que son quienes dicen ser. Esta característica asegura el origen de la información. Existen ataques que atentan contra este principio, como la suplantación de la identidad o los de robos de contraseñas.



1.5. Violación de la autenticación.

Actividades propuestas

7·· A partir de los principios expresados en este epígrafe:

a) Plantea un posible ataque contra cada uno de estos principios.
b) Indica una posible solución para cada uno de los ataques planteados.

8·· Busca más información sobre los *sniffers* en Internet. ¿Qué son? ¿Qué utilidad tienen?

4 >> Políticas de seguridad

La RFC 1244 define la política de seguridad como:

> **Una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.**

En otras palabras, las políticas de seguridad informática detallan una serie de normas y protocolos a seguir donde se definen las medidas a tomar para la protección de la seguridad del sistema, así como la definición de los mecanismos para controlar su correcto funcionamiento.

Tienen como objetivo concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Se puede decir que son una descripción de todo aquello que se quiere proteger.

Las políticas de seguridad deben cubrir aspectos relacionados con la protección física, lógica, humana y de comunicación, tener en cuenta todos los componentes de la organización y no dejar de lado el entorno del sistema.

¿Qué aspectos se deben tener en cuenta a la hora de elaborar las políticas de seguridad?

- Elaborar las reglas y procedimientos para los servicios críticos.
- Definir las acciones que habrá que ejecutar y el personal que deberá estar involucrado.
- Sensibilizar al personal del departamento encargado de la administración del sistema informático de los posibles problemas relacionados con la seguridad que pueden producirse.
- Establecer una clasificación de los activos a proteger en función de su nivel de criticidad, de forma que los sistemas vitales sean los más protegidos y no se gasten recursos en proteger aquellos activos con menor importancia.

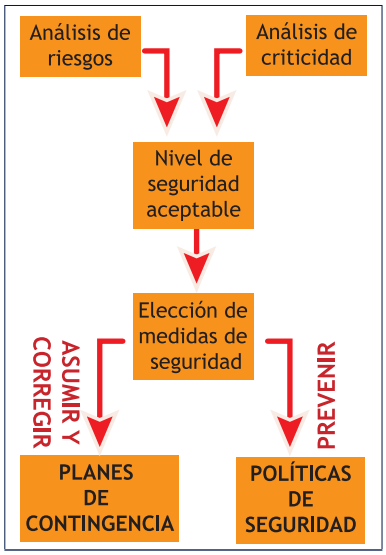
Las medidas de control deben ser efectivas, fáciles de usar, actualizadas periódicamente y, por supuesto, apropiadas a la situación. No hay que olvidar que deben funcionar en el momento adecuado.

Numerosas organizaciones internacionales han desarrollado documentos, directrices y recomendaciones con información relacionada con el uso adecuado de las nuevas tecnologías para sacarle el máximo provecho y evitar el uso inadecuado de las mismas.

RFC

Son las siglas de *Request For Comments* (petición de comentarios). Son unas notas emitidas por una organización de normalización (la IETF, *Internet Engineering Task Force*), con la intención de establecer estándares en Internet.

Cada RFC tiene un título y un número asignado.



1.6. Control de riesgos.

Actividades propuestas

9·· ¿Crees que establecer normas a los usuarios de una organización para que tengan una contraseña de acceso segura es una buena política de seguridad?

10·· Indica qué políticas de seguridad establecerías para evitar la caída de los servidores de la organización.

5 >> Planes de contingencia

Las políticas de seguridad contemplan la parte de prevención de un sistema, pero no hay que desechar la posibilidad de que, aun a pesar de las medidas tomadas, pueda ocasionarse un desastre. Hay que recordar que ningún sistema es completamente seguro. Es en este caso cuando entran en juego los planes de contingencia.

El plan de contingencia contiene medidas detalladas para conseguir la recuperación del sistema, es decir, creadas para ser utilizadas cuando el sistema falle, no con la intención de que no falle.

La creación de un plan de contingencia debe abarcar las siguientes fases:

- **Evaluación:** en esta etapa hay que crear el grupo que desarrollará el plan. Se deberán identificar los elementos considerados como críticos para la organización, analizar el impacto que pueda producirse ante un desastre y definir cuáles deberán ser las soluciones alternativas a cada uno de los problemas que se puedan producir.
- **Planificación:** en esta fase se deberá documentar y validar el plan de contingencia por parte de los responsables de las áreas involucradas de la organización.
- **Realización de pruebas** para comprobar la viabilidad del plan.
- **Ejecución** del plan para comprobar que efectivamente asegurará la continuidad de las tareas críticas de la organización en caso de posible catástrofe.
- **Recuperación:** tras el incidente o ataque, deberá restablecerse el orden en la organización.

El plan de contingencia deberá ser revisado periódicamente para que siempre pueda estar de acuerdo con las necesidades de la organización. Entre las numerosas medidas que debe recoger, podemos indicar las siguientes:

- Tener **redundancia**: es decir, tener duplicado el hardware para el almacenamiento de la información, de forma que quede asegurada la continuidad de la actividad diaria en caso de problemas con dicho hardware.
- Tener la **información almacenada de manera distribuida**, es decir, no tener almacenada en el mismo lugar toda la información considerada como crítica para la organización.
- Tener un **plan de recuperación** que contemple las medidas necesarias para restaurar el estado de los recursos tal y como estaban antes de la materialización de la amenaza. Por ejemplo, tener un buen plan para la realización de copias de seguridad.
- Tener a todo el **personal de la organización formado y preparado** ante cualquier situación de emergencia.

Soluciones de alta disponibilidad

Una solución de alta disponibilidad permite que los sistemas de información de la organización estén disponibles las 24 horas de los 7 días de la semana. Con esta solución las empresas pueden tener la posibilidad de no perder información debido a fallos en los sistemas.

Punto único de fallo

El punto único de fallo o SPOF *(Single Point of Failure)* puede ser un componente hardware, software o electrónico. Un fallo en él puede ocasionar un fallo general en el sistema. Para evitarlo, se utiliza la redundancia de elementos para evitar la caída del sistema si uno de ellos falla.

Actividades propuestas

11·· ¿Quiénes crees que deben elaborar el plan de contingencia para una empresa?

12·· ¿Crees que un plan de contingencia, una vez creado, es ya para toda la vida?

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿En qué se diferencian la seguridad activa y la seguridad pasiva?

2·· Indica algunas razones por las que a alguien le puede interesar realizar un ataque a la seguridad informática de una empresa.

3·· Enumera posibles activos asociados a una organización.

4·· ¿Cuáles son los posibles puntos débiles en los sistemas informáticos de una organización?

5·· ¿Qué recomendaciones harías para evitar el acceso no autorizado a la información en una organización?

6·· Enumera posibles vulnerabilidades asociadas a las estaciones de trabajo en una organización.

7·· Indica, para los siguientes supuestos, qué principios de la seguridad se están violando:

a) Destrucción de un elemento hardware.
b) Robo de un portátil con información de interés de la empresa.
c) Robos de direcciones IP.
d) Escuchas electrónicas.
e) Modificación de los mensajes entre programas para variar su comportamiento.
f) Deshabilitar los sistemas de administración de archivos.
g) Alterar la información que se transmite desde una base de datos.
h) Robos de sesiones.

8·· Pon un ejemplo de ataque por ingeniería social. ¿Cómo crees que se puede proteger una organización ante los ataques de ingeniería social?

9·· Analiza el grado del impacto que pueda ocasionar la acción de una amenaza meteorológica como pueda ser un huracán para una organización.

10·· ¿En qué consisten y qué aspectos deben cubrir las políticas de seguridad?

11·· ¿Por qué crees que es importante que una organización tenga un plan de contingencia? ¿Qué consecuencias podría haber si no tuviese un plan de contingencia establecido?

12·· ¿En qué consiste el análisis de riesgos? ¿Para qué sirve realizar un análisis de riesgos?

13·· ¿Qué utilidad tienen para las organizaciones los planes de contingencia?

.: APLICACIÓN :.

1·· Suponemos que el hospital X está ubicado cerca de un cauce de río que prácticamente no lleva agua. El hospital tiene su centro de cálculo situado en el sótano. Se han anunciado lluvias fuertes y por tanto existe una alta posibilidad de desbordamiento del río que pasa cerca de la zona debido a la falta de limpieza de su cauce.

Identifica los activos, las amenazas y las vulnerabilidades del sistema.

2·· ¿Qué tipo de aplicaciones se pueden utilizar para comprometer la confidencialidad del sistema?

3·· Una empresa se ha visto atacada de forma que su página web ha sido modificada sin previa autorización. ¿Qué tipo de ataque se ha producido? ¿Qué principios de la seguridad se han visto violados?

4·· ¿Qué soluciones se podrían aplicar para que el sistema informático de una entidad bancaria no se viera afectado por un desastre que afectara a sus clientes?

Caso final 2

Instalación y uso de una herramienta de análisis y gestión de riesgos

•• Instala en tu equipo la herramienta PILAR, desarrollada por el Centro Criptológico Nacional (CCN), que implementa la metodología MAGERIT de análisis y gestión de riesgos y que es de amplia utilización en la Administración Pública española. Abre el proyecto de ejemplo que incluye, analízalo y contesta a las siguientes cuestiones:

a) ¿Qué tipo de empresa se estudia en el ejemplo?
b) ¿Qué clasificación de activos tiene? ¿Cuáles se encuentran dentro de los de la sección *Equipamiento?* ¿Qué aplicación utilizan?
c) ¿Qué vulnerabilidades de los dominios se muestran?
d) Identifica las categorías de amenazas registradas. ¿En qué categoría entran las siguientes amenazas?

- Manipulación de la configuración.
- Fuego.
- Errores de configuración.
- Divulgación de la información.
- Corte de suministro eléctrico.
- Errores de los usuarios.
- Extorsión.

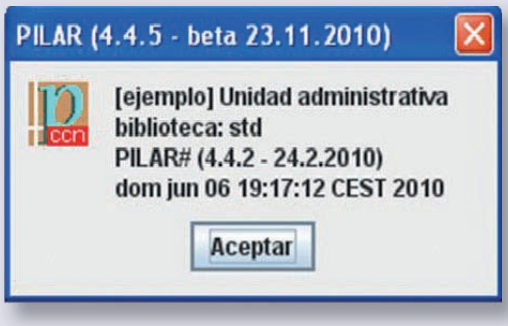
e) Proporciona alguna amenaza más por cada categoría.
f) ¿Qué valoración de las amenazas se da para los activos clasificados como *Equipos?* ¿Y para la *Sala de Equipos?*

Solución •• Las herramientas de software específicas para la gestión de riesgos pueden facilitar en gran medida el trabajo de análisis y gestión de riesgos en una organización para posteriormente elaborar unas políticas de seguridad y un plan de contingencia, ya que trabajan desde el punto de vista de los principios básicos: confidencialidad, integridad, disponibilidad y autenticidad.

Antes de comenzar a contestar las preguntas, debes proceder a descargar e instalar la aplicación. Para ello, comprueba que tu equipo cuenta con los requisitos mínimos necesarios para llevar a cabo la instalación de la herramienta PILAR:

- Microprocesador: Intel Pentium, AMD586 o similar.
- Disco duro libre: 20 MB.
- Memoria libre: 256 MB.
- Máquina virtual de Java: esta herramienta está desarrollada en Java, por lo que puede utilizarse en cualquier sistema operativo (Windows, Linux, Unix, etc.) que disponga de máquina virtual de Java versión 1.5.0 o superior.

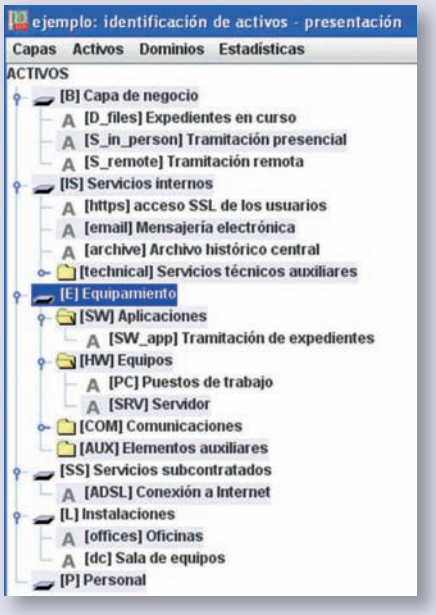
Si tu equipo cumple con los requisitos, descarga la aplicación desde la página https://www.ccn-cert.cni.es/ haciendo clic en *Herramientas / EAR / Pilar.*



Instala la herramienta y carga el proyecto de ejemplo que viene incluido. Ahora ya puedes responder a las preguntas planteadas.

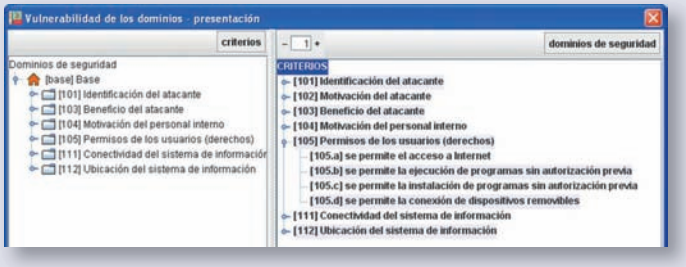
a) Como puedes ver en la imagen, la empresa que se estudia en el ejemplo es una unidad administrativa consistente en una biblioteca.

b) Esta unidad administrativa tiene la siguiente clasificación de activos, incluyendo el detalle de la sección *Equipamiento*:

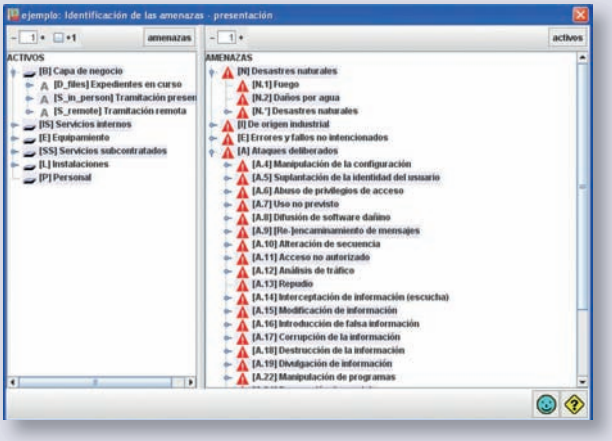


Estos activos utilizan la siguiente aplicación: *[SW_app] Tratamiento de Expedientes*

c) Se muestran las siguientes vulnerabilidades de los dominios:



d) PILAR registra las amenazas que muestra la siguiente imagen:



2

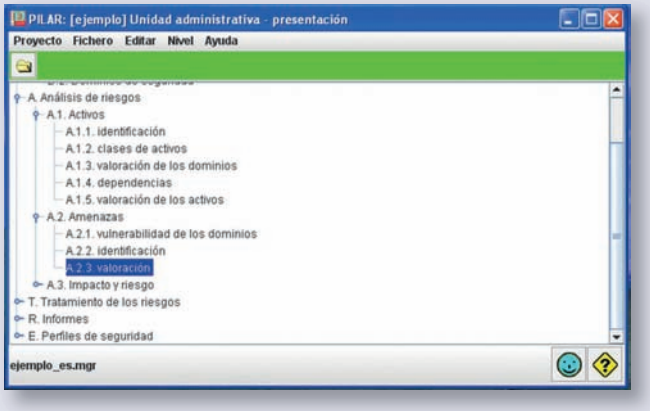
Como también se puede ver en la imagen, la categorización de las amenazas indicadas es la siguiente:

- Manipulación de la configuración: *[A] Ataques deliberados*
- Fuego: *[N] Desastres naturales*
- Errores de configuración: *[E] Errores y fallos no intencionados*
- Divulgación de la información: *[A] Ataques deliberados*
- Corte de suminstro eléctrico: *[I] De origen industrial*
- Errores de los usuarios: *[E] Errores y fallos no intencionados*
- Extorsion: *[A] Ataques deliberados*

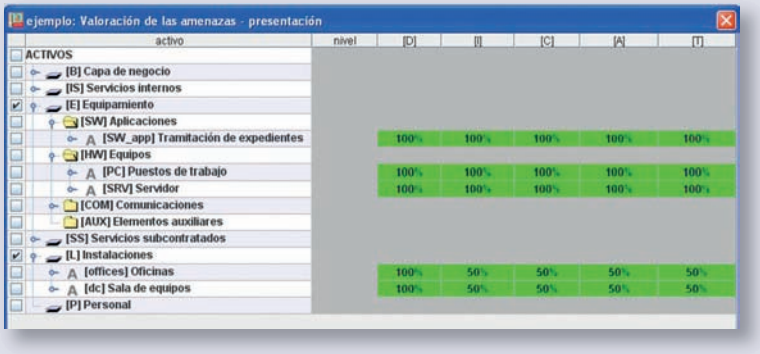
e) Además de las expuestas, se podrían incluir algunas amenazas más en las distintas categorías:

- Desastres naturales: daños por agua, desastres naturales.
- De origen industrial: contaminación mecánica, contaminación electromagnética.
- Errores y fallos no intencionados: errores del administrador, pérdidas de equipos.
- Ataques deliberados: robo de material informático, incendios provocados.

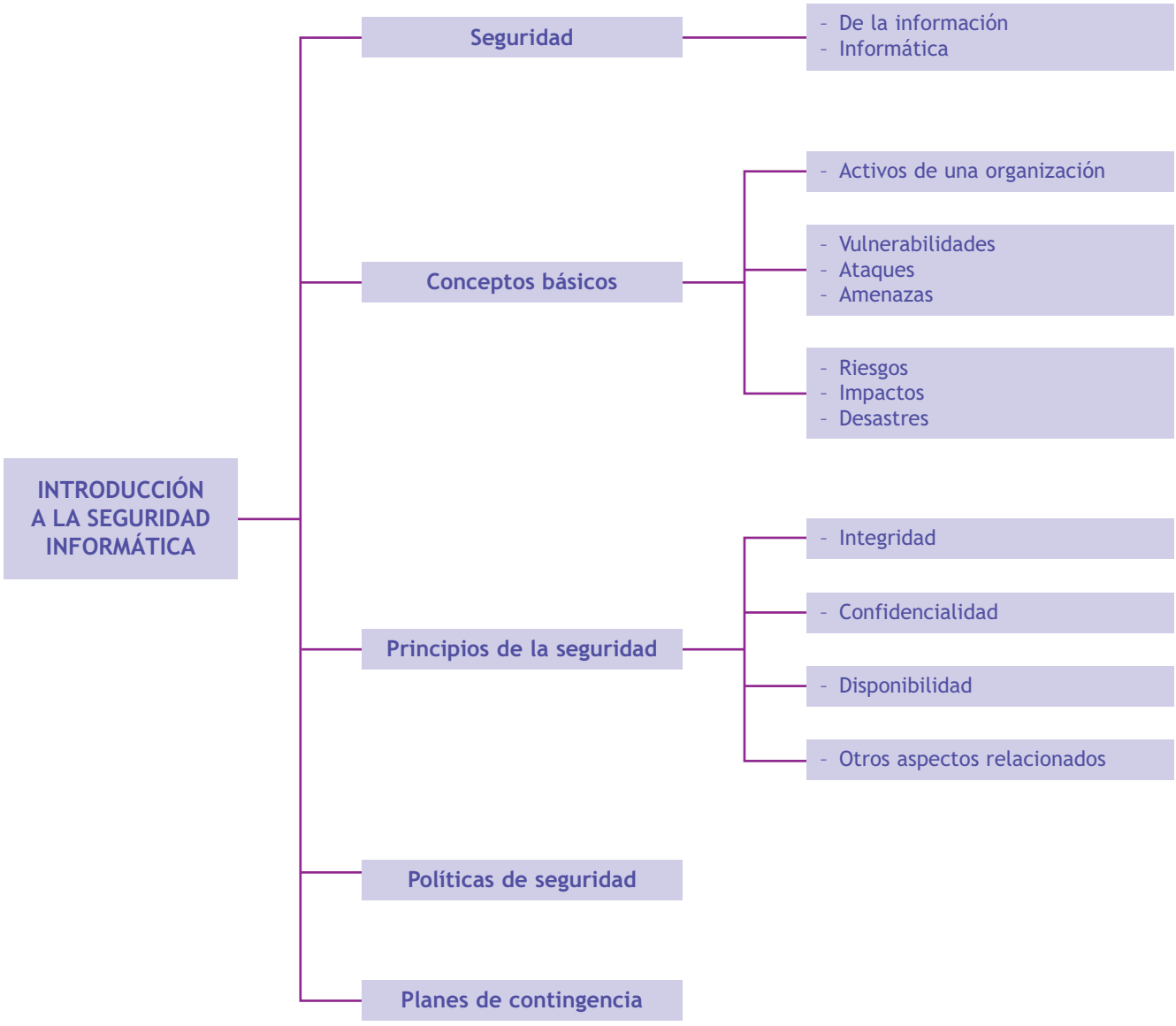
f) Para acceder a la valoración de las amenazas, en el árbol de categorías, debes desplegar la opción *Análisis de riesgos / Amenazas / valoración*.



- Para el equipamiento, la valoración de las amenazas que se da es que existe un 100%, tanto en disponibilidad (D), como en integridad (I), confidencialidad (C), autenticación (A) y trazabilidad (T). Por lo tanto, los niveles de seguridad son óptimos.
- En cambio, la sala de equipos tiene un 100% en disponibilidad (D), pero en el resto, en integridad (I), confidencialidad (C), autenticación (A) y trazabilidad (T), tiene únicamente una valoración del 50%, con lo que su seguridad es bastante mejorable.



Ideas clave

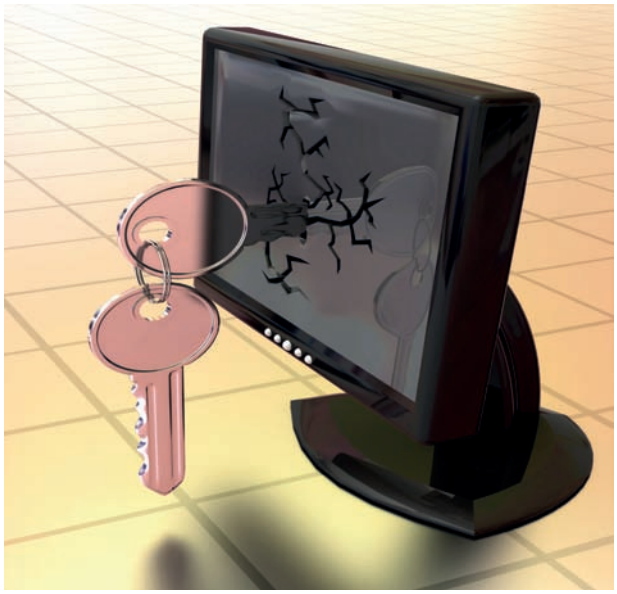

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA
Seguridad
- De la información
- Informática
Conceptos básicos
- Activos de una organización
- Vulnerabilidades
- Ataques
- Amenazas
- Riesgos
- Impactos
- Desastres
Principios de la seguridad
- Integridad
- Confidencialidad
- Disponibilidad
- Otros aspectos relacionados
Políticas de seguridad
Planes de contingencia

Exceso de confianza de las pymes frente a los ciberataques

Symantec Corp. presenta las conclusiones de su encuesta de 2011 sobre concienciación de las amenazas en las pymes (2011 *SMB Threat Awareness Poll*), que indicó que, aunque el nivel de concienciación es alto, las pymes no se consideran objetivo de los ciberataques. Debido a ello, no están implementando las medidas de protección apropiadas para salvaguardar su información.

La encuesta sobre concienciación de las amenazas en las pymes examina los niveles de concienciación de las pymes en lo que se refiere a los peligros de las amenazas a la seguridad, así como su preparación para defenderse contra este tipo de ataques.

"Nuestro estudio muestra que las pymes son bastante vulnerables a los ciberataques", afirma Steve Cullen, vicepresidente senior de marketing mundial para SMB y *cloud* en Symantec Corp. "Incluso con los presupuestos ajustados y con los recursos limitados actuales, unos cambios sencillos como, por ejemplo, iniciativas de formación y buenas prácticas, pueden fortalecer en gran medida el enfoque de una pyme hacia la seguridad para hacer frente a los posibles ciberataques".



Aspectos destacados de la encuesta:

- **Las pymes están familiarizadas con las amenazas a la seguridad.** La encuesta indica que más de la mitad de las pymes están familiarizadas con las diversas amenazas a la seguridad.

- **Las pymes piensan que no son objetivo de dichas amenazas.** Aunque las pymes conocen los daños de los ciberataques, piensan que no corren riesgo en este terreno. La mitad de las pymes piensa que no corren peligro, ya que solo las grandes organizaciones tienen que preocuparse. Sin embargo, según los datos de Symantec.cloud, el 40% de todos los ataques dirigidos a objetivos específicos se han perpetrado contra compañías de menos de 500 empleados, en comparación con tan solo el 28% dirigido a grandes organizaciones.

- **Las pymes no están realizando ninguna acción**. Como las pymes no se ven como objetivos, muchas de ellas no están tomando las precauciones básicas para proteger su información. Dos tercios de ellas restringe quién tiene la información necesaria para acceder a ciertos servicios, pero un 63% no protege las máquinas que utilizan para la banca *online,* más de la mitad (61%) no usa antivirus en todos los equipos y el 47% no usa seguridad en los servidores de correo.

Recomendaciones

- **Formar a los empleados:** desarrollar unas pautas sobre seguridad en Internet y formar a los empleados.

- **Valorar su estado de seguridad:** las pymes hacen frente a una mayor cantidad de riesgos que amenazan su información, por lo que resulta esencial proteger sus datos. Por ello, es importante que conozcan sus riesgos y los vacíos en seguridad que puedan tener para dar los pasos necesarios para proteger su información.

- **Tomar medidas:** ser proactivo y elaborar un plan de seguridad. Considerar acciones como las políticas de contraseñas, la protección de *endpoints*, la seguridad del correo electrónico y de los activos web, así como el cifrado de los datos.

Fuente: Madrid, 28 de noviembre de 2011. www.symantec.com

Actividades

1·· ¿Por qué crees que las empresas no están implementando las medidas de protección apropiadas para salvaguardar su información?

2·· Según el texto, ¿qué amenazas a la seguridad pueden sufrir las pymes? ¿Qué otras amenazas añadirías?

unidad 2

Seguridad física

SUMARIO

- Importancia de la seguridad física
- Protección física de los equipos
- Sistemas de alimentación ininterrumpida
- Centros de proceso de datos
- Sistemas de seguridad en los CPD
- Centros de respaldo

OBJETIVOS

- Tomar conciencia sobre la importancia de la seguridad física de los sistemas informáticos.
- Identificar los riesgos físicos a que están sometidos los equipos informáticos.
- Aplicar las medidas preventivas adecuadas para proteger los equipos informáticos.
- Describir las características y medidas de seguridad de un centro de proceso de datos.
- Valorar la importancia de los centros de respaldo de datos.

1 >> Importancia de la seguridad física

Desgraciadamente todos los días nos llegan noticias sobre sustracción de bienes materiales: dinero, joyas, etc. Una vez producido el delito, se puede intentar detener al culpable y recuperar los bienes robados; pero es mucho más útil e importante tomar medidas para que estos hechos no se produzcan instalando sistemas de seguridad preventivos: alarmas, rejas en ventanas, puertas de seguridad, etc. Del mismo modo, habitualmente se producen situaciones catastróficas ocasionadas por causas naturales como inundaciones, incendios, etc. Estas situaciones no pueden evitarse, pero sí disminuir sus consecuencias para las personas o bienes, mediante la adopción de medidas preventivas.

Si todas estas situaciones son desagradables en un entorno personal, en el ámbito de la empresa revisten especial gravedad, puesto que afectan a su patrimonio, necesario para llevar a cabo su actividad. En primer término se puede pensar que este patrimonio está integrado por los bienes tangibles de la empresa (mobiliario, ordenadores, etc.), pero aún más importantes que estos son los bienes intangibles (los datos). En efecto, una pérdida de un equipo físico puede ser reemplazada fácilmente; en cambio, es muy posible que la pérdida de los datos de la empresa sea irremplazable. Además, hay que tener en cuenta que esos datos pueden ser utilizados por otras personas con fines ilícitos (para estafar a la empresa, para averiguar sus secretos industriales, etc.).

Es por ello que la seguridad física adquiere una importancia vital a la hora de preservar tanto los datos que poseen las empresas, como los equipos y dispositivos encargados de su tratamiento y almacenamiento. Podemos, por tanto, definir la seguridad física como:

> **El conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos.**

Los riesgos externos a los que están sujetos los sistemas informáticos y las medidas preventivas que se pueden adoptar son los siguientes:

- **Fenómenos naturales,** como inundaciones, tormentas, terremotos, etc. Se pueden adoptar medidas preventivas como la instalación de los equipos en ubicaciones adecuadas dotadas de las oportunas medidas de protección (ubicaciones seguras, pararrayos, etc.).
- **Riesgos humanos,** como actos involuntarios, actos vandálicos y sabotajes. Entre las medidas preventivas estarían: control de acceso a recintos, elaboración de perfiles psicológicos de empleados con acceso a datos confidenciales, formación a usuarios en materia de seguridad, etc.

Actividades propuestas

1·· Indica varios ejemplos de fenómenos naturales y de riesgos humanos que pueden poner en peligro la seguridad física de los equipos informáticos de tu aula. Indica, respecto a cada uno, si puede evitarse o no y, en su caso, cómo podría evitarse.

2 >> Protección física de los equipos

En este epígrafe nos ocuparemos de las medidas de protección para los sistemas informáticos, centrándonos en los equipos de usuario. Dejaremos el estudio de la protección de los servidores para el siguiente apartado, ya que suelen estar situados en salas especiales y cuentan con medidas de protección especiales.

2.1 > Entorno físico del equipo

Uno de los elementos más importantes a la hora de fijar las medidas preventivas para la seguridad física de los equipos informáticos es el lugar donde estos están situados. Las condiciones físicas de esta ubicación determinan los riesgos a que están sujetos los equipos. Así:

Factor de riesgo	Medidas preventivas
Espacio	Los ordenadores deben tener una buena ventilación; por ello, se debe procurar que exista espacio suficiente alrededor de la carcasa para permitir la correcta circulación del aire caliente proveniente de su interior. Igualmente, se debe evitar colocar objetos sobre la carcasa para no obstruir las salidas de ventilación.
Humedad	La humedad relativa aconsejable es del 50% aproximadamente: una humedad excesiva provoca corrosión en los componentes. Una humedad muy escasa (por debajo del 30%) favorece la existencia de electricidad estática. Por ello, hay que tener cuidado con la calefacción y con el aire acondicionado, pues secan mucho el ambiente.
Luz solar	La luz solar directa debe ser evitada pues puede producir un sobrecalentamiento del equipo. Para evitar la incidencia de los rayos solares sobre el equipo, pueden instalarse persianas y cortinas o cambiar la ubicación del mismo.
Temperatura ambiente	Los ordenadores están formados por componentes electrónicos y magnéticos sensibles a la temperatura. La temperatura ideal para los equipos informáticos se sitúa entre 15 y 25 °C. Si la temperatura ambiente no está dentro del rango óptimo, es aconsejable la instalación de un aparato de refrigeración o climatización.
Partículas de polvo	El polvo y la suciedad afectan al buen funcionamiento del equipo informático. Por ejemplo, pueden disminuir la refrigeración de los componentes debido a la obstrucción de los ventiladores, etc. Por ello, los equipos deben situarse en zonas de mínimo impacto de partículas adversas y, periódicamente, se debe llevar a cabo una limpieza general del equipo.
Campos magnéticos	Los imanes y electroimanes alteran los campos magnéticos y pueden provocar la pérdida de datos en dispositivos de almacenamiento como el disco duro. Algunos de los dispositivos susceptibles de causar averías de este tipo son: destornilladores imantados, altavoces, motores eléctricos, etc.
Vibraciones y golpes	Pueden provocar averías en el equipo informático, sobre todo en los discos duros. Por ello, se debe colocar el equipo lejos de aparatos que produzcan vibraciones y en lugares resguardados que no sean de paso, fijar bien los componentes y utilizar carcasas de alta calidad.
Suelos	Determinados tipos de suelo (como los laminados), debido a su mala conductividad eléctrica, acumulan electricidad estática. Por ello, se debe poner especial cuidado respecto a la superficie donde se ubica el ordenador. Si se usan alfombras, debe cuidarse de que sean antiestáticas.

2.2 > Instalaciones

Además de las condiciones ambientales, hay otras circunstancias derivadas de la ubicación de los equipos y de su propio funcionamiento que pueden ocasionar riesgos para los mismos:

- **Instalación eléctrica adecuada:** los equipos informáticos funcionan gracias a la energía eléctrica que les llega a través de sus conexiones. Una instalación eléctrica defectuosa es susceptible de causar graves daños. Se pueden adoptar las siguientes medidas preventivas:
  - **Protecciones eléctricas adecuadas.** Los enchufes deben contar con tomas de tierra y la corriente suministrada debe ser lo más estable posible para evitar picos de tensión.
  - **Mantenimiento del suministro eléctrico.** La corriente eléctrica está sometida a anomalías, como apagones, caídas de tensión, etc. Hay que tomar las medidas necesarias para minimizar el riesgo de estas anomalías, así como para disminuir sus consecuencias negativas. Para prevenir las averías que estas anomalías pudieran producir a los equipos informáticos se desarrollaron **los sistemas de alimentación ininterrumpida (SAI)**. Un SAI es un dispositivo que tiene por finalidad proporcionar alimentación a los equipos conectados a él cuando se produce un corte en la corriente eléctrica, dando tiempo a que los equipos se apaguen de forma adecuada y no se produzca ninguna pérdida de información.
- **Instalación de red adecuada.** Los equipos estarán conectados a una red de datos y esta a su vez a una red general. En primer término, hay que proteger esta red de accesos físicos no deseados. Además, normalmente la red está configurada por cable, por lo que habrá que vigilar que el tipo de cable es el correcto, así como que su estado de conservación es el adecuado al entorno (los cables pueden estar expuestos a la humedad, afectados por radiaciones electromagnéticas, etc.).
- **Control de acceso.** Tanto si el ordenador está en una oficina, como si está en una sala especialmente destinada a su uso, habrá que controlar el acceso a ese lugar. Además, deberá asegurarse la entrada en el equipo en sí mediante el establecimiento de claves.
- **Protección frente a incendios.** Se deben utilizar tanto sistemas de prevención como sistemas de protección:
  - **Sistemas de prevención:** son los más eficaces, pues van encaminados a que no se produzca el incendio. Por ejemplo, instalación de detectores de humo y alarmas, mantenimiento del orden y la limpieza para evitar la acumulación de materiales combustibles, etc.
  - **Sistemas de protección:** son los que se ponen en marcha en caso de que se haya producido un incendio. Los más comunes son la colocación de barreras para aislar el incendio, la delimitación clara de las vías de evacuación y salidas de emergencia y la instalación de sistemas de extinción. En el caso de los incendios que se pueden producir en una oficina con equipos informáticos, los extintores apropiados son los de clase C (o ABC), de polvo seco polivalente o CO_2. Nunca se debe intentar apagar uno de estos incendios con agua a chorro debido al riesgo de sufrir una descarga eléctrica.

Vocabulario

Toma de tierra: es un sistema de protección para los equipos eléctricos y sus usuarios. En caso de un fallo en el aislamiento de los conductores, desvían la corriente a tierra.

Agua nebulizada como agente extintor

Si bien en los incendios de líquidos inflamables, equipos eléctricos y electrónicos el uso del agua a chorro está totalmente contraindicado, en los últimos tiempos se está extendiendo el empleo del agua nebulizada como agente extintor válido para este tipo de incendios.

Como veremos en el epígrafe dedicado a los CPD, en caso de incendio de componentes electrónicos, este sistema es muy recomendable, pues no solo extingue el fuego, sino que combate uno de los mayores enemigos de los sistemas electrónicos, como es el humo.

2.3 > Sistemas de alimentación ininterrumpida

Como hemos visto en el apartado anterior, una de las principales fuentes de riesgo para los sistemas informáticos es la corriente eléctrica. Esta corriente no es perfecta, sino que está sometida a anomalías (apagones, caídas y picos de tensión, sobrevoltajes, ruido eléctrico, etc.) que hacen que el funcionamiento de los equipos no sea el idóneo y que, en los casos más graves, pueden ocasionar importantes daños a los mismos.

Para prevenir estos riesgos se han desarrollado los **sistemas de alimentación ininterrumpida (SAI),** conocidos también por su nombre en inglés, ***Uninterrupted Power Supply*** **(UPS).**

> **Un SAI es un dispositivo cuya finalidad es proporcionar suministro eléctrico a los equipos conectados a él cuando se produce un corte en la corriente eléctrica.**

Los SAI no tienen capacidad para suministrar corriente durante mucho tiempo, por ello, no están pensados para que los equipos conectados a ellos sigan funcionando a pleno rendimiento, sino que su función es ganar tiempo para realizar un apagado ordenado de los equipos. Además de esta función principal, sirven como estabilizadores de la tensión eléctrica, filtrándola y reduciendo el efecto nocivo que producen los picos de tensión y el ruido eléctrico.

El uso de estos dispositivos es beneficioso para todo tipo de equipos, aunque, debido a su elevado coste, tradicionalmente solo se instalaban en sistemas críticos como servidores, grandes bases de datos, hospitales, etc., donde su uso no solo era beneficioso sino imprescindible. Actualmente su precio ha bajado bastante y existen modelos asequibles para ser instalados en cualquier ordenador.

Tipos de SAI

Dependiendo de su modo de funcionamiento, podemos distinguir varios tipos de SAI:

- ***Offline*** **pasivos.** Se ponen en funcionamiento cuando falla la alimentación eléctrica. Entre el fallo y su activación se produce un corte de energía muy pequeño que no es detectado por la mayoría de los equipos conectados a él. Son los más habituales para proteger ordenadores domésticos, televisores, etc.
- ***Offline*** **interactivos.** Están conectados con la corriente eléctrica y siempre se encuentran activos. Además de su función principal, disponen de filtros activos que estabilizan la señal. Son de mejor calidad que los anteriores y se suelen utilizar para proteger equipos de pequeñas empresas (ordenadores, pequeños servidores, etc.).
- ***Online*****.** Se colocan entre el suministro normal de corriente y los equipos a proteger, cumpliendo también con la función de estabilización y filtrado de la señal. Las baterías se van cargando mientras se suministra energía a los equipos, por lo que, en caso de apagón, en ningún momento deja de suministrarse energía. Esto tiene como consecuencia el progresivo deterioro de las baterías y la necesidad de su sustitución. Son los más caros y de mayor calidad.

Vocabulario

Apagón: pérdida total de la corriente eléctrica.

Caídas y picos de tensión: bajadas y subidas repentinas del voltaje de corta duración.

Sobrevoltaje: subidas repentinas del voltaje que se mantienen durante un cierto tiempo.

Ruido eléctrico: interferencias que alteran la señal eléctrica.

Ordenadores portátiles

Los ordenadores portátiles disponen de una batería que en caso de corte del suministro eléctrico hace las veces de un SAI, pues, si en ese momento tiene carga suficiente, puede seguir alimentando al equipo de forma autónoma.

Un SAI está compuesto por las siguientes partes o bloques funcionales:

- **Batería y cargador:** son los elementos que almacenan la carga eléctrica que se usará en caso de necesidad.
- **Filtro:** elemento destinado a limpiar la señal.
- **Conversor:** es un transformador que convierte la tensión de 12 v de su batería en corriente continua.
- **Inversor:** convierte la corriente continua en corriente alterna a 220 v.
- **Conmutador:** elemento que permite cambiar entre el suministro proporcionado por la red eléctrica y el generado por la batería del SAI.

Características de los SAI

Los SAI tienen dos características que permiten diferenciarlos:

- **Autonomía:** es el tiempo que el SAI puede seguir alimentando a un equipo en caso de fallo eléctrico. Se mide en minutos.
- **Potencia:** mide el consumo de energía de un SAI y se expresa en dos unidades distintas:
  - **Vatios (W):** es la potencia real consumida por el dispositivo.
  - **Voltiamperios (VA):** es la potencia aparente, que se halla multiplicando la tensión de la corriente en voltios por la intensidad en amperios. Normalmente, en las especificaciones técnicas de los SAI, la potencia va expresada en esta unidad.

La relación entre VA y W se denomina **factor de potencia** y su valor está siempre entre 0 y 1 (normalmente alrededor de 0,6), ya que la potencia real siempre es mayor que la aparente.

Casos prácticos 1

Cálculo de la potencia de un SAI

•• Un equipo informático doméstico está compuesto por un ordenador (200 W de consumo), un monitor (50 W), un *router* (10 W) y una impresora (10 W). Queremos instalar un SAI que proteja toda esa instalación y vamos a una tienda donde nos enseñan un modelo de 300 VA por 78 € y otro de 500 VA por 118 €. Ambos tienen un factor de potencia del 60%.

¿Cuál deberíamos elegir?

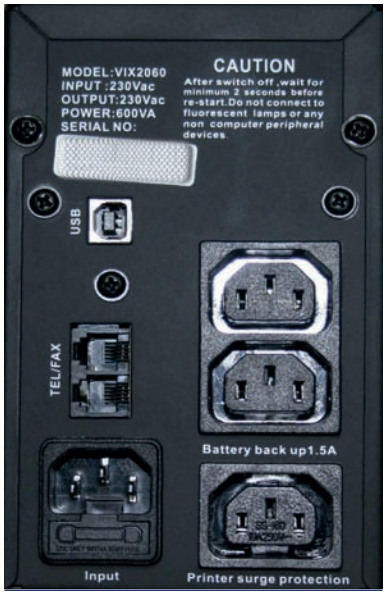
Solución •• El consumo total del equipo será de 270 W (200 + 50 + 10 + 10).

A simple vista podría parecer que con el de 300 VA nos serviría perfectamente para nuestro equipo, e incluso sobraría potencia, además, nos ahorraríamos 40 €. Pero debemos tener en cuenta que su potencia está expresada en distintas unidades de medida (VA en vez de vatios).

Por tanto, deberemos aplicar el factor de potencia para ver a qué potencia real en vatios equivalen los VA de los dos SAI:

$$300 \times 0{,}6 = 180 \text{ W} \rightarrow 500 \times 0{,}6 = 300 \text{ W}$$

Pese a la primera impresión, vemos que el SAI de 300 VA no es suficiente y, en este caso, habría que elegir el de 500 VA.



2.1. Vista trasera de un SAI que muestra los conectores IEC320 para alimentación y USB para datos.

Instalación y gestión de un SAI

Independientemente del tipo de SAI que estemos utilizando, la instalación y gestión de todos ellos se lleva a cabo siguiendo un procedimiento similar.

En primer lugar, hay que buscar aquella **ubicación** para el dispositivo que permita un funcionamiento óptimo. Una base estable y una ventilación adecuada, sin objetos encima o alrededor, harán que el SAI rinda mucho mejor.

El siguiente paso es la **conexión** del SAI. Estos equipos requieren dos tipos de conexión:

– **Conexión eléctrica:** para cumplir su función, estos dispositivos tienen que ir conectados por un lado a la red eléctrica y por otro al equipo informático al que van a proteger. El SAI habitualmente contará con conexiones tipo IEC320 suficientes y suele incluir los cables necesarios para conectarse con el ordenador. Si no las tuviera, el remedio es utilizar una regleta.
– **Conexión de datos:** una vez realizadas las conexiones eléctricas, llega el momento de conectar el cable de datos al sistema informático para poder gestionar el SAI, bien por el ordenador local o a través de una red (conexión de comunicaciones). Esta última conexión se suele realizar por alguno de los puertos serie o la interfaz de red. Los SAI permiten varios esquemas de conexión de datos:
  - **Conexión monopuesto local:** un único SAI va conectado a un único equipo local. En estos casos la conexión entre el ordenador y el SAI se realiza a través de los puertos serie: USB o RS-232C.
  - **Conexión de la batería del SAI a una LAN:** la batería del SAI se conecta, a través de un *switch*, a la red por TCP/IP y se gestiona mediante un servidor de la red o bien de equipos remotos de Internet.
  - **Otras:** dependiendo de la envergadura de la red, el tipo de SAI, etc., pueden usarse otras conexiones. En estos casos lo mejor es consultar las recomendaciones de los fabricantes.

Una vez realizadas todas las conexiones, ya se puede **encender** el equipo. Aunque es posible que el sistema operativo detecte el SAI, para mejorar su utilización lo mejor es utilizar los *drivers* del fabricante. Los SAI disponen de diversos avisos sonoros y/o luminosos para llamar la atención acerca de las incidencias que pueden suceder al encenderlos (aviso de batería baja, sobrecarga, etc.). La primera vez, hay que tener en cuenta que la batería no tendrá suficiente carga, por lo que hay que esperar unas cuantas horas hasta que se cargue totalmente.

Una vez conectado, habrá que **configurar** el SAI de acuerdo a las preferencias de cada usuario y ya se podrá gestionar su utilización desde el propio equipo a través de programas específicos. En concreto se podrán definir prioridades de apagado entre todos los equipos conectados en función de su importancia, programar las labores de encendido y apagado de los equipos conectados a la red para una mejor eficiencia y ahorro energéticos, monitorizar la actividad del SAI y el envío de mensajes de alerta e informes al administrador de la red a través de SMS, *email,* etc.

Ejemplos

Configuración y gestión de un SAI

Disponemos de un SAI BELKIN de 350 VA que queremos conectar a un ordenador tipo PC. Lo primero que haremos es seguir las instrucciones del fabricante para su conexión. Si no disponemos de esas instrucciones, podemos acudir a la página web del fabricante web.belkin.com/support para descargarlas.

Conexión del SAI al PC

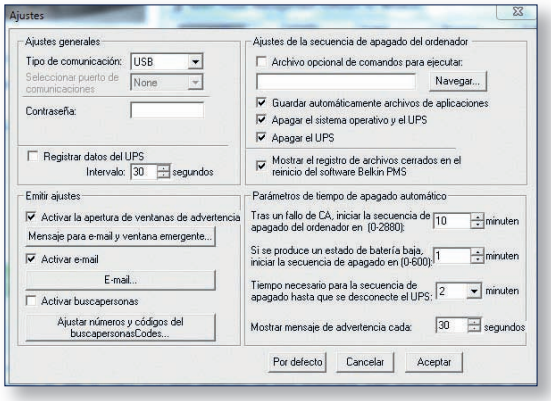
El primer paso será conectar el SAI al PC. Podemos hacer esto bien a través del puerto serie o a través del puerto USB. Nos aseguraremos de que, en función de la conexión elegida, el selector de la conexión RS-232 o USB esté en la posición correcta, pues no podemos usar ambas opciones a la vez. A continuación, conectamos el cable de alimentación del PC al SAI y el cable de alimentación del SAI a la red eléctrica.

Instalación del software

Una vez realizada la conexión física, seguramente el sistema operativo del ordenador detecte automáticamente al SAI. Tanto si lo ha detectado como si no, es recomendable instalar los *drivers* del fabricante, así como el programa de gestión.

Después de instalar el programa, aparecerá un icono característico en el área de notificación de Windows, correspondiente al servicio *Rupsmon* que comenzará su ejecución.

Configuración del SAI



Para configurar el SAI, hacemos clic con el botón secundario del ratón sobre el icono del área de notificación y accedemos al programa de gestión, que en este caso se llama *Belkin Power Management*.

En la columna izquierda haremos clic sobre *Seleccionar UPS* e indicaremos si el SAI a gestionar es local o remoto. Haciendo clic sobre *Ajustes* rellenaremos los campos con los valores adecuados, como por ejemplo cuál va a ser la operativa a seguir en caso de que el ordenador se apague: cuándo se apagará al fallar el suministro eléctrico, si enviará un correo o llamada de aviso, etc.

Gestión del SAI

El programa de gestión muestra el estado del SAI (tensiones de entrada y salida, frecuencia, carga, temperatura y capacidad de las baterías, etc.), digitalmente o en modo gráfico, lo que permite monitorizar la calidad de la energía suministrada. En caso de fallo de suministro eléctrico o nivel bajo de las baterías, el programa realizará su función de monitorización de manera automática, enviando los avisos en la forma que hayamos configurado y llevando a cabo las acciones pertinentes. Toda su actividad se puede almacenar en forma de registros.

2.4 > Controles de presencia y acceso

El primer punto débil de un sistema informático, hablando en términos de seguridad física, es la puerta de entrada al recinto o edificio. Debemos evitar que personal no autorizado tenga acceso físico a la sala donde se encuentran los ordenadores.

Un intruso podría robar los equipos o los soportes de almacenamiento internos (discos duros, tarjetas de memoria...) o externos (cintas, DVD, unidades de disco externas, etc.). Asimismo podría sabotear los equipos físicos o, lo que puede ser más grave para una empresa, acceder a la información contenida en los equipos.

Métodos de control de acceso físico

Los sistemas de control de acceso basan su funcionamiento en tres posibles métodos:

- Lo que soy (una clave).
- Lo que tengo (una tarjeta o dispositivo de acceso).
- Lo que soy (características biométricas).

Los sistemas más seguros emplean combinaciones de estos tres tipos.

Control de acceso en los entornos físicos

Medidas de seguridad	Funcionamiento
Sistemas de vigilancia	Personal de vigilancia que se encarga de evitar accesos no autorizados y alarmas y sistemas de detección de intrusos (cámaras, sensores de temperatura o movimiento, etc.) que complementan su trabajo.
Código de seguridad	Los usuarios deben recordar un código numérico o contraseña de seguridad para acceder al recinto o al sistema. La contraseña puede ser individual o común a un grupo de usuarios. Sus inconvenientes son la necesidad de recordar el código y la posibilidad de que un intruso acceda a las contraseñas de acceso.
Acceso mediante dispositivos	El acceso al área restringida o a los sistemas se realiza utilizando un instrumento de seguridad (llave, tarjeta, etc.). El inconveniente de estos sistemas es que el dispositivo de acceso debe custodiarse adecuadamente.
Sistemas biométricos	Estos sistemas se basan en la identificación de ciertos rasgos físicos únicos del sujeto para identificarlo (huella dactilar, reconocimiento facial, escáner del iris, reconocimiento facial, etc.). Sus ventajas son que no es necesario conservar ni recordar nada. Tampoco es necesario cargar con ningún dispositivo. Su principal inconveniente viene de que hay un incremento del coste, tanto económico como computacional, conforme aumenta su sofisticación.

Actividades propuestas

2·· Dispones de un SAI de 300 VA con el que quieres proteger un ordenador que tiene instalada una fuente de alimentación de 250 W. ¿Sería suficiente?

3·· En una instalación local en la que tenemos dos ordenadores, dos monitores, dos teclados inalámbricos y un *router* ADSL, pretendemos añadir un SAI. ¿Qué dispositivos deberíamos conectar al SAI? Justifica tu respuesta.

4·· Averigua qué sistemas de control de presencia y de acceso se utilizan en los equipos informáticos de los siguientes centros de trabajo: un banco, un ayuntamiento, un hospital, un supermercado.

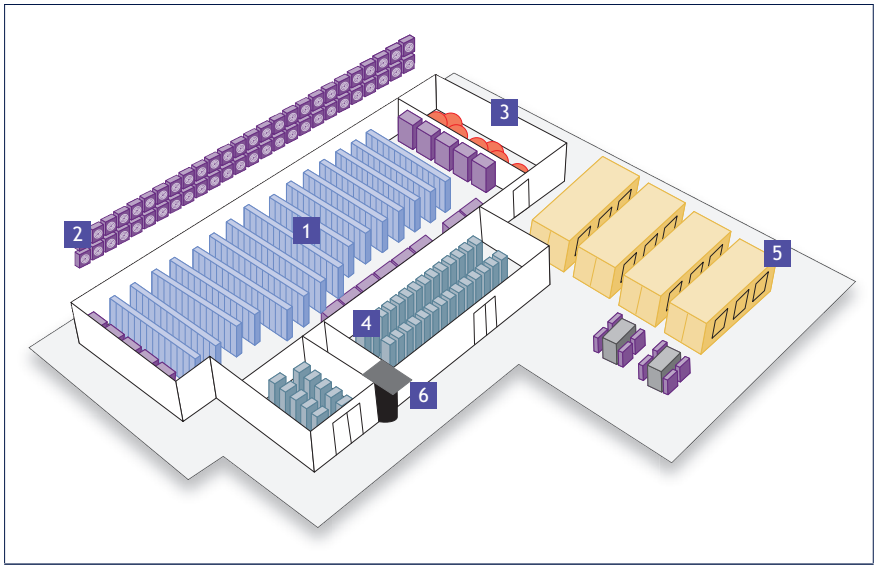
3 >> Centros de proceso de datos

Hasta ahora hemos visto el entorno físico de los equipos existentes en un ámbito doméstico o en una pequeña empresa, pero las empresas de tamaño mediano o grande cuentan con gran cantidad de equipos informáticos y necesitan servidores y otros dispositivos que realicen el control de todo el parque informático y de comunicaciones. Piensa, por ejemplo, en una sucursal bancaria o en una oficina ministerial y en todos los equipos informáticos con los que allí se trabaja.

Estos sistemas, que centralizan bases de datos, servicios de correo electrónico, gestión de usuarios, etc., precisan de unas instalaciones físicas y de unos requerimientos de hardware peculiares y reciben, en su conjunto, el nombre de **centro de proceso de datos** (CPD) o su denominación inglesa, ***data center***.

Los sistemas informáticos a esta escala requieren servidores con varios procesadores y unidades de disco, sistemas de comunicaciones avanzados (con varios *routers, switches,* etc.), equipos de alimentación redundantes, dispositivos para copias de seguridad, etc. Estos equipos deben trabajar a una temperatura ambiente baja (unos 17-19 ºC) y generan mucho ruido, por lo que deben ser confinados en un espacio físico diferenciado del trabajo con unas condiciones ambientales y de aislamiento acústico y térmico especiales. Además, esta situación de confinamiento permite adoptar respecto de estos equipos unas medidas de seguridad especiales.

Dado su cometido, los CPD deben estar operativos, ininterrumpidamente, las 24 h de todos los días del año, si bien no requieren la presencia de operadores en su interior. Dentro únicamente hay máquinas —servidores, equipos de comunicaciones, dispositivos de almacenamiento, equipos de climatización, sensores, etc.— que son controladas desde fuera de la sala, desde dentro del mismo edificio a través de la red local o bien remotamente a través de Internet mediante concentradores KVM.



2.3. Esquema de distribución de un CPD.

2.2. Distribución de *racks* en un CPD.

Web

www.google.com/about/datacenters: web sobre los *data centers* de Google. Página muy interesante para ver la estructura y funcionamiento de un CPD.

Concentradores KVM

Un concentrador KVM *(Keyboard-Video-Mouse)* es un concentrador de consolas que permite, mediante un teclado, pantalla y ratón, acceder de forma remota a las consolas de los servidores del CPD como si estuviéramos trabajando con un teclado y una pantalla directamente conectados a estos.

1. *Racks* de servidores.
2. Climatización.
3. Sistema de extinción de incendios.
4. SAI.
5. Generadores de copias de seguridad.
6. Sistemas de seguridad.

3.1 > Características constructivas y de disposición

De todo lo expuesto se deduce que los centros de proceso de datos necesitan cumplir ciertos requisitos constructivos y de disposición de sus distintos elementos (cableado, instalación, aislamientos, etc.) que les permitan llevar a cabo su función con eficacia y seguridad.

A la hora de configurar un CPD habrá que tener en cuenta el tipo de datos que van a manejarse, el número de equipos que va a contener y su tipología. Por ello, cada empresa, en función de su volumen y su actividad, dimensionará el CPD de acuerdo a sus necesidades. Por ejemplo, el CPD de una empresa mediana con pocos requerimientos de datos puede ocupar una pequeña habitación, mientras que cada uno de los *data center* de Google está enclavado en un enorme edificio en el que hay alojados decenas de contenedores, cada uno de los cuales incluye más de 1000 servidores.

Por tanto, hay que diferenciar los supuestos de que el CPD ocupe un edificio específico del supuesto en que ocupe una parte del edificio en el que se ubican las oficinas de la empresa.

- **Edificio dedicado:** debe encontrarse en una zona lo más segura posible frente a catástrofes naturales (incendios, inundaciones, terremotos, etc.). La zona debe presentar escasa o nula actividad sísmica o, de lo contrario, debe contar con características técnicas preparadas para este tipo de sucesos. Todo el centro de proceso de datos suele rodearse de un encofrado que lo aísla de fenómenos ambientales externos y asegura sus propiedades ignífugas.
- **Ubicación del CPD en una sala dentro de un edificio**: los requerimientos de esta ubicación son los siguientes:
  - Como los CPD se suelen rodear de un encofrado de hormigón, metal o ambos, requieren un reforzamiento importante de la estructura arquitectónica del edificio. La zona donde se ubique el centro debe soportar el peso de este y por eso no se suelen ubicar en los pisos superiores. Sin embargo, la ubicación en sótanos debe realizarse teniendo en cuenta el mayor riesgo de humedades e inundaciones para proveer las medidas necesarias para evitarlos.
  - El cofre, por dentro, presenta generalmente falso suelo para el cableado y el sistema de refrigeración, así como falso techo para albergar los sistemas de detección y extinción de incendios y conducciones extra del sistema de refrigeración.
  - Deben tenerse en cuenta los accesos exteriores, salidas de emergencia, cercanía de material inflamable o peligroso, etc.
  - Habrá que asegurarse de que las dimensiones de la sala son las adecuadas, así como de la distribución de la sala en sí, con la presencia de columnas u otros factores que limiten el espacio.
  - Debe estar en una zona libre de inundaciones. En caso de que hubiera cierta probabilidad de humedad dentro de la sala, es necesaria la instalación de equipos especiales para la extracción de la misma.
  - La sala debe contar con sistemas de control de acceso y presencia que garanticen la seguridad de la información y equipos.

CPD externo

Las pequeñas empresas, que no dispongan de medios económicos ni espacio para tener un CPD propio, pueden utilizar uno ya existente de otra empresa o bien crear uno nuevo entre varias pequeñas empresas y compartirlo. Con ello se consigue tener un CPD a menor precio con prácticamente la misma funcionalidad.

Aislamiento térmico y sonoro

A la hora de ubicar y encofrar los CPD hay que tener en cuenta sus peculiares condiciones térmicas y de ruido, incompatibles con el trabajo de oficina. Esto hace que se deba elegir un aislamiento térmico y sonoro que confine el calor, frío y ruido dentro de la sala del CPD.

3.2 > Sistemas de seguridad del CPD

Además de contar con unas características constructivas y de ubicación especiales, la sala o edificio dedicado a CPD debe contar con medidas de seguridad adecuadas frente a cualquier tipo de riesgos.

Sistemas contra incendios

El CPD debe disponer de medidas para su protección frente a incendios (detectores, extintores, mangueras, etc.). En salas informáticas y CPD el material debe ser ignífugo en la medida de lo posible.

El material de extinción de incendios debe ser adecuado a los equipos existentes; se estima que los sistemas más adecuados son los que utilizan el agua como agente extintor y el nitrógeno como agente impulsor (sistemas de agua nebulizada), frente a los agentes extintores gaseosos. Además de ser más respetuosos con el medio ambiente, la extinción de incendios mediante agua nebulizada es inocua para los equipos protegidos y únicamente elimina el oxígeno en la zona de contacto directo con la llama, por lo que no supone un riesgo para el personal que se encuentre en la sala.

2.4. Dispositivo de agua nebulizada para extinción de incendios.

Sistemas eléctricos

En primer lugar, las instalaciones eléctricas deben ser adecuadas a la carga estimada que van a soportar, teniendo en cuenta cierta previsión de futuro para posibles nuevas exigencias.

Pero una instalación muy completa genera mucho cableado; por ello, el **diseño de las canalizaciones** es vital para, por un lado, aislar adecuadamente los cables y, por otro, que estos no ocasionen un problema en sí mismos al estar visibles y poder ocasionar caídas u otro accidente. Por ello, la canalización, tanto vertical como horizontal, debe realizarse a través de falsos techos y falsos suelos, que no hagan visibles los cables. En caso de que tengan que establecerse canalizaciones a la vista, hay que tratar de que estén en zonas donde no molesten (por ejemplo, encima de los armarios).

Las canalizaciones, por su parte, deben asegurar el perfecto **aislamiento de las líneas eléctricas** frente a interferencias, humedades, etc. Las líneas eléctricas y de datos deben quedar separadas entre sí, para evitar daños o interferencias.

Además, los servidores van provistos de **fuentes de alimentación redundadas** para evitar que un fallo en una fuente de alimentación deje al servicio sin energía. Por ello, es básico que los CPD cuenten con dos acometidas de potencia diferentes en cada *rack,* de forma que cada una de las fuentes de alimentación de los servidores se conecte a una regleta distinta. Si se llegara a quemar o estropear una regleta ello no interrumpiría el servicio debido a que el servidor seguiría recibiendo potencia a través de la otra.

Como hemos visto, el **SAI** es imprescindible en los sistemas informáticos, pero, en estos casos, además, al sistema de SAI se le suele añadir un generador que permita funcionar al CPD de forma autónoma en caso de grandes paradas en el suministro eléctrico.

3.3 > Climatización

Dadas las especiales características de los equipos existentes en un CPD y su sensibilidad a las condiciones climáticas (temperatura y humedad), estos centros deben contar con unos sistemas de climatización que garanticen que dichas condiciones sean las óptimas.

La climatización de un CPD no consiste en la mera instalación de equipos de aire acondicionado. Dado que se trata de una sala cerrada y llena de ordenadores y equipos que producen calor, hay que pensar en algún sistema que elimine todo este calor, inyecte aire libre de partículas y mantenga también unas condiciones óptimas de temperatura (17-19 ºC) y humedad, recomendándose una humedad relativa del 45% (±5%). Para ello, hay que cuantificar y estimar la carga térmica de la sala con el fin de dimensionar bien el sistema de refrigeración.

Existen varias formas de inyectar aire dentro de la sala, por el techo o por el suelo, formando lo que se llaman **"pasillos fríos"**. De la misma forma, las salidas de aire caliente de los equipos se deben disponer de forma que se puedan direccionar hacia un mismo sitio con el fin de ser recogido por extractores de aire para su enfriamiento y filtrado. La zona donde se mueve todo este aire cálido se denomina **"pasillos calientes"**.

Los servidores no incorporan ventiladores debido a que estos serían incapaces de enfriar suficientemente las temperaturas que se producen por las altas capacidades de proceso actuales. En su lugar, lo que llevan son disipadores y turbinas. Su estructura se diseña de forma que se favorezcan lo más posible las corrientes de aire desde la parte frontal hacia la trasera atravesando los disipadores. Las turbinas contribuyen a generar ese ciclo de aire. Y en esto es básico que el CPD esté configurado en torno a pasillos fríos y pasillos calientes, aislados unos de otros.

Web

www.rediris.es: Página web de RedIRIS. En su apartado *Publicaciones*, se puede acceder al *Boletín* n.º 76 de esta Red, que recoge un interesante artículo sobre "Climatización en Centros de Proceso de Datos".

Gasto energético de la climatización

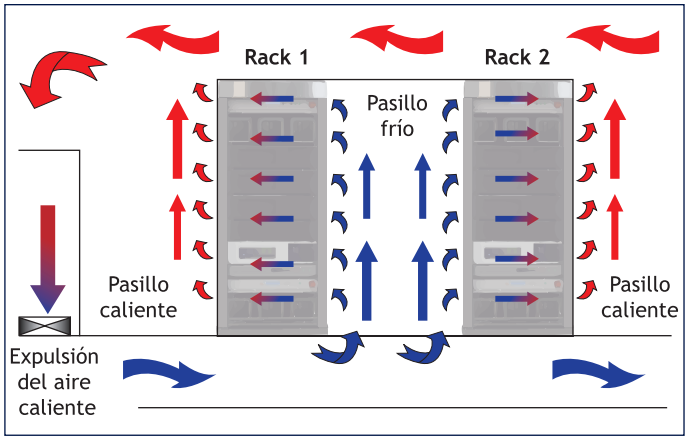
Más de la mitad del consumo de energía de un CPD procede de los sistemas de refrigeración, la iluminación y otros equipos auxiliares, por lo que la elección del sistema de climatización es algo muy importante, así como la óptima configuración del mismo (una excesiva refrigeración supondría un gasto innecesario y además perjudicaría a los equipos).

Ejemplos

Utilización de pasillos fríos y calientes para climatizar un CPD

Imaginemos que tenemos un CPD que contiene varios *racks* dispuestos en filas.

Las filas de *racks* están dispuestas de forma que las partes frontales de los servidores den a un pasillo (pasillo frío) de donde toman el aire refrigerado a través de las rejillas de su cara frontal y lo hacen pasar a través de sus disipadores hacia la parte trasera. En su paso por el interior de los equipos, el aire se calienta y acaba siendo expulsado al pasillo cálido por la parte trasera de los equipos. Si hubiera un tercer *rack*, su parte trasera daría al pasillo caliente y estaría enfrentada con la de uno de los dos anteriores. Además, deben existir equipos que recojan todo ese aire caliente y lo expulsen fuera del CPD.



3.4 > Datos

Un centro de proceso de datos debe contar con redes y equipos robustos, los cuales deben poder soportar sistemas de comunicación de alta velocidad y altas prestaciones capaces de atender al tráfico de redes SAN (*Storage Area Networks*), NAS (*Network Attached Storage*), granjas de distintos tipos de servidores, servidores *blade* y otros dispositivos diversos.

Pero además de contar con unos equipos adecuados a la función requerida, en el apartado de datos es fundamental contar con un cableado adecuado, respecto del que se adopten análogas medidas de aislamiento y conducción de las que hemos expuesto para el cableado eléctrico.

Los cables de datos serán tanto de tipo Ethernet como de fibra óptica y la primera medida de aislamiento es mantenerlos convenientemente separados de los cables eléctricos para evitar interferencias electromagnéticas que afecten a su eficacia.

En segundo término, estos cables de datos deben quedar ocultos por falsos techos y suelos, pero a la vez deben ser fácilmente accesibles para los técnicos y dejar espacio suficiente para su manipulación y sustitución. Las canalizaciones deben estar diseñadas de forma que los técnicos no tengan opciones a la hora de llevar el cableado de un punto a otro, sino que el camino esté claramente definido. Finalmente, las redes de cableado de datos deberán contar con la suficiente protección para evitar cualquier daño accidental.

2.5. Cableado, agrupado por abrazaderas, en un CPD.

3.5 > Centros de respaldo

A lo largo de este epígrafe, hemos visto la importancia de las salas de servidores, centros de proceso de datos y las medidas que se pueden adoptar para protegerlos de posibles riesgos de todo tipo. Pero por muchas medidas que se adopten, siempre puede ocurrir algún suceso imprevisto y desastroso que lo destruya absolutamente todo (terremoto, ataque terrorista, etc.).

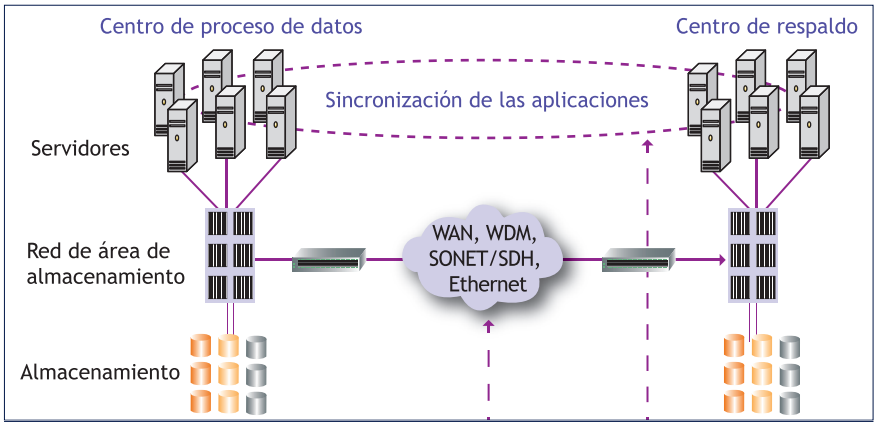
Esto hace, que, de forma adicional a todas las medidas expuestas, muchas empresas mantengan o contraten **centros** o **salas de respaldo** (en inglés DRS, *Disaster Recovery Sites*), que son réplicas, más o menos exactas, del CPD principal, diseñadas para que, en caso de fallo de este, puedan tomar el control del sistema, evitando la pérdida de datos.

La primera medida a la hora de diseñar uno de estos centros es la separación física de la sala de servidores para intentar que cualquier eventualidad que pudiera afectar a uno no impacte en el otro. Se estima que la distancia óptima se encuentra en torno a 20-40 km, ya que tiene en cuenta los condicionantes de seguridad y las limitaciones impuestas por las líneas de comunicación existentes entre ambas.

En cuanto al diseño del centro de respaldo y a los equipos con que debe contar, hay que tener en cuenta que los costes son un factor fundamental en la seguridad. Así, a la hora de plantear un centro de respaldo hay que tener siempre en mente durante cuánto tiempo es asumible que los sistemas de la organización estén parados en caso de desastre y cuántos recursos estamos dispuestos a invertir para minimizar ese tiempo de parada.

Basándonos en estos dos criterios, coste y tiempo, y dado que no es estrictamente necesario que ambas salas estén dotadas del mismo equipamiento, existen varias tipologías para el centro de respaldo:

- ***Cold site* o sala fría:** es un CPD externo a la organización con toda la infraestructura necesaria en cuanto a climatización, potencia eléctrica, etc., para poner en marcha un CPD semejante al nuestro. En caso de contingencia, habría que trasladar allí los servidores y reinstalar todo el sistema a partir de copias de seguridad, por lo que la puesta en funcionamiento es de más de una semana, si bien es la solución más barata.
- ***Hot site* o sala caliente:** es un CPD con comunicaciones, sistemas y software análogo al principal (aunque puede estar dimensionado a la mitad de capacidad de cálculo y memoria para ahorrar). En caso de contingencia, solo hay que restaurar los datos al último momento disponible en los *backups*, por lo que la puesta en funcionamiento es inferior a un día, pero su coste de mantenimiento es mayor, puesto que cualquier modificación que se haga en el principal debe realizarse también en el centro de respaldo.
- ***Mutual backup*:** en este caso, se llega a un acuerdo con otra organización para ejercer de centro de *backup* mutuo entre sí. En este sentido, cada organización reserva un espacio de su CPD para los servidores de respaldo de la otra organización. Estos pueden estar apagados (con lo que la solución se aproxima a la de la sala fría) o bien estar encendidos funcionando al modo de una sala caliente.
- ***Mirror site* o centro espejo:** es una evolución de la sala caliente en la que los datos son replicados en tiempo real de un CPD a otro, por lo que el paso de un CPD a otro es bastante rápido al no tener que realizarse restauración de datos.
- **Configuraciones activo-activo:** todas las configuraciones anteriores son de tipo activo-pasivo. Para organizaciones que no pueden permitirse un solo momento de parada se utilizan configuraciones de tipo activo-activo entre CPD en las que los sistemas están configurados en clústeres geográficos repartidos en ambos CPD. Los usuarios trabajan indistintamente y de forma transparente con los sistemas de uno u otro en todo momento y, en caso de caída total de un CPD, el servicio no se ve afectado debido a que el otro puede funcionar de forma autónoma.



2.6. Esquema de un centro de respaldo tipo activo-activo.

Ejemplos

Diseño de un centro de respaldo

La empresa SYSTEL LABS es una empresa valenciana dedicada al diseño de prototipos mecánicos.

Si bien el tamaño de la empresa no es excesivo, pues están alojados en la planta baja y primera planta de un céntrico edificio de Valencia, la información que manejan es muy valiosa y abundante y no pueden detener su actividad de cálculo en ningún momento. Tienen además otra sede de oficinas en Londres de similares características.

Actualmente disponen de un CPD donde están ubicados los diez servidores desde los que se prestan servicios de aplicaciones, almacenamiento, comunicaciones y proceso de datos, con todos los procedimientos de seguridad necesarios para asegurar su funcionamiento. Los sistemas y la electrónica cuentan con diversos grados de duplicidad para garantizar el servicio. Se están planteando la posibilidad de contar con un centro alternativo desde el cual prestar los mismos servicios en caso de caída o fallo del primero en un polígono cercano a la ciudad o en otra planta de las oficinas de Londres.

Analizando las distintas posibilidades, hay que considerar varios aspectos:

- Por un lado, está la **elección de la tipología de la sala.** Dado que se trata de una empresa que no puede dejar de dar servicio, las posibilidades más adecuadas son la creación de un centro espejo y configuración activo-activo. En efecto, si se elige un centro espejo, como los datos son replicados en tiempo real de un CPD a otro, en caso de necesidad, el paso del CPD al centro de respaldo es bastante rápido al no tener que realizarse restauración de datos. Si se elige la configuración activo-activo, como los usuarios trabajan indistintamente con los sistemas de uno u otro centro, en caso de fallo en un centro el servicio no se ve afectado debido a que el otro puede funcionar de forma autónoma.
- Por otro lado, está el asunto de la **ubicación física de la sala.** Dadas las circunstancias de la empresa, que cuenta con un robusto sistema de comunicaciones con la sede en Londres, lo más adecuado, siempre que fuera económicamente viable, sería ubicar el centro de respaldo en las oficinas londinenses. De este modo, se aprovecharía la dispersión geográfica para salvaguardar el centro de posibles catástrofes naturales (un terremoto o unas inundaciones en Valencia no afectarían al centro en Londres). Además, el sistema de comunicaciones con Londres está activo y funciona perfectamente, mientras que en caso de elegir la instalación en el polígono industrial habría que comprobar que las condiciones de las líneas de comunicaciones entre el centro de respaldo y la sala CPD de Valencia permiten la creación de dicho centro.

Actividades propuestas

5·· Accede a la página web del Área de Sistemas de Información y Comunicaciones de la Universidad Politécnica de Valencia. (www.asic.upv.es). Indica las tareas que realiza y los servicios que ofrece. ¿Se le puede considerar un centro de proceso de datos? ¿Por qué?

6·· ¿Cuál es el sistema de extinción de incendios más adecuado para ser utilizado en un CPD? ¿Por qué?

7·· Realiza un esquema de la distribución adecuada de un CPD compuesto por seis filas de *racks*, para optimizar su climatización. Indica dónde estarán los pasillos fríos y calientes, por dónde se inyectará el aire frío y por dónde se extraerá el aire caliente.

8·· Debate con tus compañeros sobre qué tipo de instalaciones deberían contar con un CPD de respaldo.

9·· Investiga en Internet cómo se lleva a cabo el proceso de replicación de la información entre el CPD principal y el de centro de respaldo.

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿Qué es la seguridad física?

2·· Cuáles son los factores de riesgo a que están expuestos los equipos informáticos?

3·· Enumera las características que deben cumplir las instalaciones para proteger adecuadamente a los equipos informáticos.

4·· ¿Qué es y para qué sirve un SAI?

5·· ¿En qué magnitud se mide la carga de un SAI? ¿Cómo se relaciona esa magnitud con las unidades de medida de potencia de los dispositivos electrónicos conectados al mismo?

6·· Explica brevemente los distintos tipos de SAI. Busca por Internet tres ejemplos de cada uno de ellos. Realiza un cuadro comparando sus precios y prestaciones.

7·· ¿Por qué los CPD se suelen ubicar en las plantas bajas o en los sótanos de los edificios?

8·· ¿Qué diferencias hay entre un centro de datos configurado como *cold site*, *hot site* o *mirror site*, desde el punto de vista del coste de cada uno y el tiempo que se tardaría en recuperar la información? ¿Cuál sería el más adecuado para una empresa de venta de productos por Internet? ¿Por qué?

9·· Indica a qué factores de riesgo están expuestos los siguientes equipos:

a) Ordenador ubicado en el sótano sin ventilación del almacén de una tienda de pirotecnia.
b) Ordenador situado en un hospital, en el archivo de las historias clínicas en papel.

.: APLICACIÓN :.

1·· Investiga las medidas de seguridad física de que disponen los equipos informáticos de tu centro escolar. Para ello deberás tener en cuenta cuántas puertas de acceso tiene el centro escolar y las aulas donde hay material informático, qué horario de apertura y cierre tiene el centro, si existe algún tipo de control de acceso, si existe alguna medida electrónica de vigilancia (alarmas, cámaras, etc.). ¿Tienen los equipos contraseñas de acceso o algún sistema de seguridad que impida que un intruso acceda libremente a los datos almacenados en ellos? ¿Existen las mismas medidas de seguridad para los ordenadores de las salas de informática que para los que contienen datos sensibles como matrículas, notas, etc.?

2·· Imagina que el propietario de una pequeña tienda de golosinas acude a ti para que le asesores en cuanto a las medidas de seguridad a adoptar para evitar que los intrusos accedan al ordenador donde lleva la contabilidad, que está ubicado en la propia tienda. Indica qué sistemas de protección le recomendarías y por qué.

3·· Una empresa de nueva apertura quiere diseñar la sala donde van a instalarse sus equipos informáticos. La sala tiene 20 m^2, está instalada en una cuarta planta y tiene grandes ventanales por los que entra la luz del sol. Dicha sala constará de seis puestos de trabajo, cada uno de los cuales estará dotado de un ordenador de sobremesa y un monitor de 23 pulgadas. Todos los equipos están conectados en red y comparten dos impresoras láser. El servidor se encuentra también en la sala.

Indica todos los factores de riesgo para los equipos, así como las medidas preventivas a tener en cuenta: condiciones ambientales, colocación del mobiliario, espacios, instalación eléctrica, etc.

4·· Analiza la estructura de tu aula informática, fíjate en los cables de los ordenadores, las conexiones eléctricas y de comunicaciones. ¿Te parece adecuada la canalización? ¿Cómo está realizada? ¿Cómo se podría mejorar? Justifica la respuesta.

Caso final 2

Diseño de un sistema de seguridad informática

•• PACKAGING SPAIN, SA es una empresa dedicada a la elaboración de envoltorios de plástico para productos alimenticios. En esta empresa se genera gran cantidad de información acerca de distintas pruebas realizadas de control de calidad que se almacena en una pequeña infraestructura de servidores. Imagina que te acaban de contratar para mejorar el sistema de almacenamiento de la empresa y dotarlo de medidas de seguridad con el mínimo coste posible y has detectado lo siguiente:

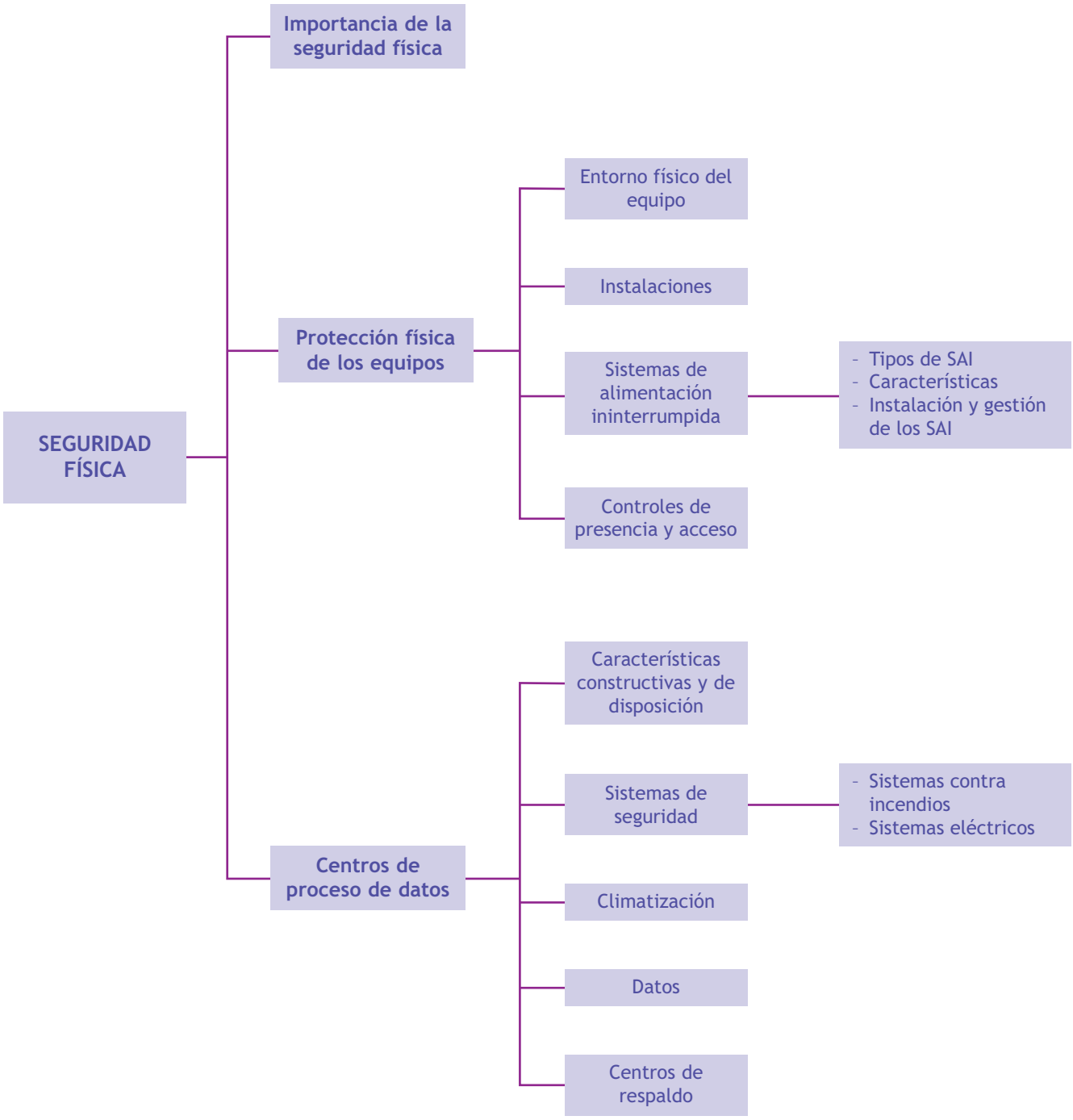
- La información de la empresa está distribuida entre varios servidores que realizan las mismas funciones.
- Las copias se seguridad se realizan de cuando en cuando y no se lleva a cabo copia de toda la información, sino solo de aquella que es considerada importante en el momento de realizar la copia.
- No se realiza ningún tipo de control sobre quién accede a qué información, sino que esta simplemente está almacenada en los servidores.
- Hay datos y servicios, como los registros de control de las máquinas de producción y su monitorización, que no pueden detenerse.

Indica las acciones que deberías llevar a cabo para que el sistema tuviera las adecuadas medidas de seguridad.

Solución ••

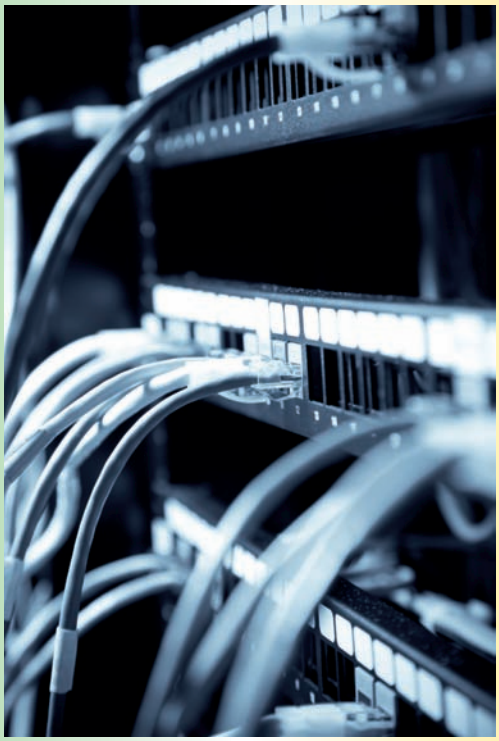
- En primer lugar hay que solucionar el tema de las copias de seguridad, estableciendo una política adecuada en función de la variabilidad de los datos. Dado que hay servidores que no se pueden detener, hay que dotar al sistema de programas de copia de seguridad "en caliente", esto es, que no precisen de una parada de los servicios del servidor.
- Otro de los aspectos a mejorar es la duplicidad de funcionalidades de los servidores. En vez de tener varios servidores haciendo la misma función, se puede plantear un *mirroring* de los servidores principales o bien establcer *clusters* entre los mismos, que garantizarían, además, la continuidad del servicio en caso de fallo de alguno de ellos.
- Sería recomendable analizar el volumen de los datos a almacenar y el grado de acceso a los mismos con el fin de valorar sistemas de almacenamiento diversos, como por ejemplo:
  - Crear un único servidor de almacenamiento con una estructura de directorios accesible por los distintos usuarios y departamentos de la empresa regulados mediante una política de cuotas de disco y permisos.
  - Crear una SAN, una red de almacenamiento.
- Aunque no se menciona la existencia de ningún CPD, sería recomendable revisar las instalaciones eléctricas, de comunicaciones, etc. de los servidores con el fin de disminuir riesgos de caídas del sistema, así como de los equipos de red.

Ideas clave


SEGURIDAD FÍSICA
Importancia de la seguridad física
Protección física de los equipos
Entorno físico del equipo
Instalaciones
Sistemas de alimentación ininterrumpida
- Tipos de SAI
- Características
- Instalación y gestión de los SAI
Controles de presencia y acceso
Centros de proceso de datos
Características constructivas y de disposición
Sistemas de seguridad
- Sistemas contra incendios
- Sistemas eléctricos
Climatización
Datos
Centros de respaldo

¿Cómo funcionan los servidores de Google™?

Uno no es consciente de la importancia que tiene un *data center* o un puñado de servidores hasta que no tienes la oportunidad de observarlos más de cerca. Por suerte o por desgracia, he conocido de cerca algunos *data centers* de cierta envergadura y siempre he tenido fascinación por su funcionamiento y sus secretos. En el caso particular del gigante Google, ¿qué infraestructura sostiene el buscador más popular del mundo? ¿Qué hace que funcionen sus servicios al 99,9% de fiabilidad? Hoy vamos a fijarnos un poco más a fondo en cómo funciona Google y sus *data centers.*



¿Cómo funciona Google?
Poniendo como ejemplo una gran empresa como es Google, imaginad la infraestructura tan enorme que ha de disponer para poder ofrecer sus servicios ininterrumpidamente y con un margen de fallo tan ínfimamente pequeño (un 99,9% de servicio garantizado). Pues hasta hace no demasiado todavía era una especie de secreto, tanto el funcionamiento como la localización de los *data centers* del gigante Google. Como tantas otras grandes empresas, Google ha mantenido cierto recelo a revelar su funcionamiento y organización interna en lo que a sistemas se refiere. Y es lógico: los sistemas son lo que mantienen vivo todo lo demás, y tanto Google como otros (Amazon, Facebook o Apple) dependen en cierta forma de ellos.
Hemos hablado del gasto que supone su mantenimiento, un poco del interior de los *data centers* de Google y de cómo afectan en mayor o menor medida al ecosistema, y de cómo Google y otras empresas tratan de disminuir el impacto.

¿Qué servidores usa Google? ¿Cómo lo tiene organizado?
Google hace sus propios servidores a medida desde hace unos cuantos años y monta sus *data centers.* Decidió montárselo por su cuenta y ahora tiene ocho *data centers* propios: seis en Estados Unidos y dos en Europa. Hay planeado construir dos más en Asia y otro en Europa. Podemos consultar su localización en una página habilitada para ello. Es admirable cómo Google ha pasado del más absoluto secretismo a compartir bastante información sobre sus centros de datos.

¿Cómo es un *data center* de Google por dentro?
No hay *tours* de visita ni se permite la entrada al público en general. De hecho, hasta el personal de Google que no esté autorizado no puede entrar. Las medidas de seguridad son una de las cosas que Google se toma muy en serio y no hay rincón que no esté debidamente vigilado mediante todos los métodos posibles: cámaras, detectores de calor, escáneres de iris, etc. Los servidores que albergan los centros de datos de Google están concentrados en *containers.* Sí, como los que transportan barcos y camiones de un lado a otro del mundo. Cada *container* puede contener 1160 servidores. Los *containers* se apilan de dos en dos y son totalmente independientes.

Fuente: Extracto del artículo "Como funcionan los servidores de Google: Dónde y cómo almacenan toda la información". www.omicrono.com. Ismael Callejas, 14 julio 2012

Actividades

1·· Enumera las características de las instalaciones de un CPD que se nombran en el artículo.

2·· Analiza el significado de la frase: "Toda la información necesaria para el funcionamiento de las empresas está en los servidores que utiliza". ¿Qué implica esta afirmación?

unidad 3

Seguridad lógica

SUMARIO

- Concepto de seguridad lógica
- Acceso a sistemas operativos y aplicaciones: contraseñas y listas de control de acceso
- Acceso a aplicaciones por Internet
- Autenticación y autorización de usuarios

OBJETIVOS

- Conocer qué es la seguridad lógica y apreciar su importancia.
- Describir los sistemas de protección de acceso a sistemas operativos y aplicaciones mediante contraseñas y listas de control de acceso.
- Analizar los sistemas de protección de acceso a las aplicaciones a través de Internet.
- Identificar diversas alternativas de gestión de identidades, explicando las diferencias entre autenticación y autorización de usuarios.

1 >> Concepto de seguridad lógica

En el tema anterior estudiamos la seguridad física. Aunque la protección física de los equipos informáticos es muy importante para cualquier empresa, no es menos importante la información que está almacenada en los mismos.

Antiguamente, cuando las organizaciones tenían sus datos y aplicaciones en grandes servidores de proceso por lotes de trabajo, garantizar la seguridad lógica suponía asegurar que solo tenían acceso físico al sistema las personas autorizadas (esto es, garantizar la seguridad física) y mantener una política robusta de copias de seguridad de los datos para poder recuperarlos en caso de incidente grave.

Actualmente, sin embargo, con la enorme interconexión existente entre los sistemas con la implantación masiva de Internet y las redes de datos, el tema de la seguridad lógica se ha convertido en el foco de atención de los departamentos de tecnología de las organizaciones. Esto es así porque los sistemas pueden ser comprometidos de forma remota por un atacante a través de una red mal protegida o aprovechando un sistema sin los adecuados sistemas de seguridad.

Además, cada vez más, se puede acceder a Internet desde multitud de dispositivos móviles (*smartphones*, *tablets*, etc.) y realizar desde allí actividades como adquirir bienes o servicios, reservar viajes, etc. Varios son los mecanismos de protección a los que estamos acostumbrados en la vida diaria: el PIN del teléfono móvil, la clave de acceso en los cajeros automáticos, el usuario y la contraseña para realizar compras *online,* etc. Estas son algunas de las medidas de protección lógica.

> **La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas.**

Políticas de seguridad corporativa

La primera medida de seguridad lógica que debe adoptar una empresa es establecer unas normas claras en las que se indique qué se puede y qué no se puede hacer al operar con un sistema informático. Estas normas marcan las pautas generales de utilización del sistema y configuran el marco de actuación de todos los usuarios.

En sentido genérico, el conjunto de normas que definen las medidas de seguridad y los protocolos de actuación a seguir en la operativa del sistema reciben el nombre de **políticas de seguridad corporativa** en materia informática.

Estas normas son aplicables a toda la empresa, por lo que todos los departamentos de la misma deben estar implicados en su elaboración, ya que todos van a tener que cumplirlas. Además, la política genérica engloba, a su vez, las distintas normas específicas aplicables a cada sector de la empresa, que estarán adaptadas, en cada caso, a los niveles específicos de seguridad de cada sector.

Entre las políticas de seguridad relacionadas con la seguridad informática tenemos las siguientes:

- Instalación, mantenimiento y actualización de los equipos.
- Control de acceso a áreas críticas de la empresa y a recursos críticos del sistema.
- Utilización de recursos de las redes informáticas.
- Mantenimiento de las redes.
- Adquisición, instalación y actualización de software.
- Privacidad de la información.
- Autenticación de usuarios.
- Información de errores o de accesos al sistema.
- Contraseñas.

Algunas de las medidas o mecanismos establecidos en las políticas de seguridad son las siguientes:

- **Autenticación de usuarios:** sistema que trata de evitar accesos indebidos a la información a través de un proceso de identificación de usuarios, que en muchos casos se realiza mediante un nombre de usuario y una contraseña.
- **Listas de control de acceso:** mecanismos que controlan qué usuarios, roles o grupos de usuarios pueden realizar qué cosas sobre los recursos del sistema operativo.
- **Criptografía:** técnica que consiste en transformar un mensaje comprensible en otro cifrado según algún algoritmo complejo para evitar que personas no autorizadas accedan o modifiquen la información.
- **Certificados digitales:** documentos digitales, identificados por un número de serie único y con un periodo de validez incluido en el propio certificado, mediante los cuales una autoridad de certificación acredita la identidad de su propietario vinculándolo con una clave pública.
- **Firmas digitales:** es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos que pueden ser utilizados como medio de identificación del firmante. Ejemplo: DNI electrónico.
- **Cifrado de unidades de disco o sistemas de archivos:** medidas que protegen la confidencialidad de la información.

Además, en las políticas, como en todos los reglamentos, no solo se establecen obligaciones y protocolos de actuación sino que también se pueden establecer sanciones para el caso de incumplimiento de sus disposiciones.

Actividades propuestas

1·· ¿Qué diferencia existe entre la seguridad lógica y la seguridad física?

2·· ¿Qué son las políticas de seguridad corporativa? ¿Afectan a toda la empresa?

3·· Enumera algunos ejemplos de políticas de seguridad dentro del ámbito de la seguridad informática.

4·· ¿Cuál es el objetivo de la autenticación de los usuarios?

5·· ¿Cuál es la diferencia entre el certificado digital y la firma digital?

2 >> Acceso a sistemas operativos y aplicaciones

Como hemos visto, para acceder a la información almacenada en un sistema informático en primer lugar hay que superar las barreras físicas de acceso. Una vez superadas estas barreras, el siguiente paso en materia de seguridad será establecer unas barreras lógicas que impidan el acceso a nuestros datos.

La primera barrera lógica que se puede establecer es la creación de mecanismos de control de acceso a la información. Para ello, en vez de que al encender los equipos se pueda acceder directamente a todos los datos almacenados en los mismos, una primera medida sería la creación de usuarios para organizar la información, de forma que cada usuario únicamente pudiera acceder a la información de la cuenta para la que dispone de autorización.

Las cuentas de usuario permiten asignar a cada uno de ellos unos derechos y privilegios que restringirán las operaciones que este va a poder realizar dentro de un sistema informático, así como la posibilidad de rastrear dichas operaciones. Como sistema de verificación de la identidad de cada uno de los usuarios se suele establecer la combinación entre un nombre identificativo (usuario, *user*, etc.), con la de una contraseña o *password*.

Además, los equipos tienen instaladas distintas aplicaciones, respecto de las que se puede establecer un control de usuarios integrado con el del sistema operativo o independiente del mismo.

Si se trabaja en un entorno de red, es posible que, para acceder a algún recurso de la misma, se exijan unas credenciales determinadas, establecidas a través de las listas de control de acceso (ACL, *Access Control List*) que veremos en un epígrafe posterior. Además, en las redes, los dispositivos de red, como los *routers*, pueden servir de barrera lógica impidiendo el acceso a determinadas zonas de la red para algunos usuarios (asignándoles un rango restrictivo de direcciones IP).

2.1 > Contraseñas

Al igual que una llave permite abrir una cerradura que impide el paso a un lugar, las contraseñas son la llave que permite el acceso a aplicaciones y sistemas informáticos.

En el ámbito informático podemos, por tanto, decir que una contraseña es un sistema de autenticación de usuarios compuesto por una combinación de símbolos (números, letras y otros signos).

En determinados supuestos, basta con conocer la contraseña para controlar un dispositivo informático, como por ejemplo un teléfono móvil. Sin embargo, lo habitual es que un mismo sistema pueda ser usado por diferentes usuarios, por lo que cada contraseña va asociada a un usuario del sistema. De esta forma, para acceder al mismo, el usuario debe proporcionar su código identificador y la contraseña asociada a este y el sistema comprueba si ambos datos son correctos y si se corresponden entre sí, en cuyo caso habilita el acceso.

De lo expuesto se deduce que cuanto más robusta sea una contraseña más difícil resultará acceder a la información protegida por la misma. Una contraseña muy difícil de averiguar por alguien que no la conozca aporta seguridad a un sistema, pero no basta. En efecto, de nada sirve tener una contraseña muy difícil de averiguar si la guardamos de forma que sea fácilmente accesible, si la revelamos indiscriminadamente a terceras personas o si la comunicamos sin tomar medidas de seguridad que impidan que otras personas puedan interceptar nuestra comunicación y obtenerla.

Por tanto, como administradores de un sistema informático, hay que ser estrictos a la hora de controlar las contraseñas de acceso al sistema desde todos los puntos de vista: fortaleza, almacenamiento y comunicación de las mismas.

Amenazas para las contraseñas

Si alguien intenta acceder a un sistema informático protegido con contraseña, previamente deberá averiguar esta. Cuanto más robusta sea una contraseña, más difícil será averiguarla. Una combinación de cifras, números y otros caracteres hace que sea más fuerte, pero hay que tener en cuenta que los usuarios son seres humanos y tienden a establecer contraseñas fáciles de recordar, por lo que es habitual que los sistemas establezcan restricciones que obliguen a los usuarios a cumplir unas determinadas normas a la hora de seleccionar sus contraseñas.

Ahora bien, por muy sencilla que sea la contraseña, los intrusos deben poner en práctica algún sistema para averiguarla. Existen diversos sistemas para tratar de averiguar las contraseñas, los más habituales son los siguientes:

- **Utilización de *sniffers*:** programas que registran la actividad de un equipo informático y pueden interceptar las comunicaciones "escuchando" para obtener datos como las contraseñas.
- **Uso de *keyloggers*:** son programas o dispositivos cuyo fin es capturar las pulsaciones en un teclado, con lo que se pueden obtener las contraseñas que han sido escritas con ese teclado.
- **Ataques por fuerza bruta:** consisten en probar todas las combinaciones posibles de caracteres hasta encontrar la clave que permite acceder al sistema. Por esto, cuanto más larga sea la cadena de caracteres que tenga la clave más se dificulta el acceso, pues más tiempo requiere averiguar la contraseña: por ejemplo, *e345Tj6k3L9934pR* es más difícil de averiguar que *x4jT*.
- **Ataques por diccionario:** consisten en generar diccionarios con términos relacionados con el usuario y probar todas esas palabras como contraseñas para acceder a ese sistema. Suelen ser más eficaces que los ataques por fuerza bruta, ya que los usuarios tienden a establecer como contraseñas palabras de su idioma, pues son más fáciles de recordar. Por eso, a igualdad de longitud de la cadena de caracteres de la contraseña, cuanto menos significado y más caracteres tenga esta, más difícil será de hallar: por ejemplo, *hola* es mucho más fácil de averiguar que *x4jT*.
- **Ataques por ingeniería social:** consisten en engañar a los usuarios para que proporcionen sus contraseñas a los intrusos, haciéndose estos pasar por amigos, empleados de un banco, técnicos, etc.

John The Ripper

John The Ripper es una herramienta originalmente diseñada para averiguar contraseñas a través de ataques de fuerza bruta. Debido a esto, se suele utilizar por los administradores de sistemas para comprobar la robustez de las contraseñas de los mismos y su vulnerabilidad a ataques de *hackers* utilizando las mismas herramientas que estos.

Políticas de seguridad en materia de contraseñas

Con el fin de evitar que las amenazas expuestas en el apartado anterior sean efectivas y que un usuario malintencionado pueda acceder a los datos de un sistema informático, es esencial que los usuarios y empresas establezcan unas políticas de seguridad relativas a las contraseñas.

Establecimiento de las contraseñas

Las contraseñas deben elegirse en función de su idoneidad para proteger la información, no en función de su facilidad para ser recordadas por el usuario. Como se adelantó en la página anterior, una adecuada política de seguridad prestará atención en fijar unas normas para la elección de contraseñas que dificulten los ataques por diccionario o por fuerza bruta. Para ello, las normas básicas son las siguientes:

- **No deben ser o contener palabras usuales ni relacionadas con el entorno del usuario,** como por ejemplo: nombres de mascotas, fechas de cumpleaños, número del DNI, etc.
- **No deben ser palabras con significado,** por ejemplo, *alimento*. La contraseña debería ser una combinación de mayúsculas, minúsculas, números y otros caracteres, por ejemplo: *aX4t$5#*. A mayor variedad de símbolos utilizada, mayor dificultad para averiguar la contraseña.
- **La longitud de la contraseña debería ser de ocho caracteres como mínimo.**
- Hay que **evitar que el usuario utilice la misma contraseña en varios sitios,** por ejemplo, que se utilice la misma contraseña para entrar a las aplicaciones de la empresa, al correo y a redes sociales.
- Se deben **cambiar las contraseñas proporcionadas por defecto** al registrarse por Internet en cualquier servicio.

Ejemplos

Establecimiento de contraseña segura

El establecimiento de una contraseña que cumpla con los requisitos de seguridad puede generar cierta ansiedad por parte los usuarios que van a trabajar en el sistema. Una posible solución para crear contraseñas que cumplan con todos los requisitos y sean fáciles de recordar para el usuario es elaborarlas a partir de la primera letra o sílaba de cada palabra que integre una frase.

Por ejemplo, partiendo de la frase: *La selección española ganó el mundial de Sudáfrica en 2011!,* se pueden tomar las primeras letras de cada palabra, los números y el signo de admiración para crear una contraseña segura como la siguiente: *LsegemdSe2011!*

Comunicación de las contraseñas

Para evitar los ataques de ingeniería social, se debe vigilar la comunicación de las contraseñas por parte del usuario, instruyéndole en la desconfianza del restablecimiento de contraseñas o de números de tarjeta bancaria, etc. mediante correos electrónicos o encuestas telefónicas. Además se deben tomar medidas para que los medios a través de los que se transmita la información (cable, WiFi, etc.) sean seguros, encriptando la información para dificultar el acceso a la misma en caso de que sea interceptada.

Gestores de contraseñas

Existen programas de gestión de contraseñas que permiten almacenar todas nuestras contraseñas de forma cifrada y segura. En estos programas se establece una contraseña maestra para acceder a ellos de forma que, en lugar de tener que recordar innumerables contraseñas, basta con recordar la que da acceso al programa. Por ejemplo KeePass Password Safe (http://keepass.info/) es una aplicación de código abierto y disponible en varias plataformas.

Combinaciones de contraseñas

Teóricamente, un ataque de fuerza bruta tendrá éxito siempre y cuando se le deje actuar el tiempo suficiente. Por ello, cuantas más combinaciones de contraseñas tenga que probar y menos tiempo se le dé para ello, más difícil será que averigüe la contraseña correcta.

Por ejemplo, una contraseña de seis caracteres compuesta por las letras en minúscula del alfabeto castellano tendría $27^6 = 387\,420\,489$ combinaciones. Si subimos el número de caracteres a ocho y utilizamos mayúsculas y minúsculas y los signos de puntuación más usuales, el número de combinaciones es de más de mil quinientos billones.

Si además, cambiamos la contraseña cada tres meses, el atacante solo dispondrá de ese tiempo para probar todas las posibles combinaciones.

Almacenamiento de las contraseñas

De nada sirve la fortaleza de una contraseña si esta no se almacena correctamente. Por ello, no se deben anotar las contraseñas ni en papel ni en archivos de texto plano en el ordenador. Si se quieren almacenar contraseñas en el ordenador, se debe recurrir al uso de programas **gestores de contraseñas**.

No obstante, cuando se lleva una política de contraseñas robusta, con cierta frecuencia ocurre que se pierde la contraseña del usuario administrador del sistema, ya sea porque se olvida o porque se almacenó mal en el gestor de contraseñas. En el caso de sistemas Linux, es posible regenerarla si se tiene acceso al sistema desde una consola. Para ello, basta con reiniciar el sistema y seleccionar el modo de arranque en modo monousuario. Este modo, que solo levanta unos servicios mínimos del sistema y, por ejemplo, no habilita la red, sí proporciona acceso por consola como usuario root sin necesidad de introducir contraseña. Una vez arrancado, se modifica la contraseña de root desde el modo monousuario y se reinicia normalmente.

Es por motivos como este que **seguridad física y lógica deben ir de la mano**. Como vemos, establecer una política segura de contraseñas puede no servir de nada si un atacante logra tener acceso físico a la consola del servidor y reiniciarlo.

Papel del administrador del sistema

En todo caso, como administradores de sistemas, si bien hay que prestar especial atención en la formación al usuario para que cumpla todas las normas propuestas, habrá que tomar medidas adicionales para el caso de que estos no cumplan dichas normas, "forzándoles" a tomar ciertas medidas de seguridad:

- Estableciendo un número máximo de intentos para acceder al sistema. Por ejemplo, si el usuario introduce tres veces seguidas una contraseña incorrecta, se bloquea el acceso y solo puede ser desbloqueado por el administrador.
- Obligando al usuario a que establezca contraseñas con un mínimo de ocho caracteres alfanuméricos que combinen, al menos, una mayúscula, una minúscula, un número y un signo de puntuación.
- Obligando al usuario a cambiar la contraseña cada cierto tiempo (por ejemplo, cada tres meses).
- Impidiendo al usuario repetir las tres últimas contraseñas utilizadas.

Una herramienta que permite al administrador gestionar las contraseñas de un sistema son las **cuentas de usuario**. Estas cuentas permiten conceder unos determinados permisos y privilegios a cada usuario, el cual solo podrá utilizar los recursos del sistema en función del rol que el administrador le haya asignado.

Las políticas relacionadas con las contraseñas se gestionan, en los sistemas Windows, desde **la consola de *Directivas de seguridad local,*** que es una herramienta muy valiosa desde el punto de vista de la seguridad, ya que afina al máximo los privilegios de los usuarios y diversas directivas relacionadas con la seguridad.

Eso sí, el administrador del sistema deberá tener en cuenta que el establecimiento de estas medidas puede provocar que, ante la dificultad de recordar las nuevas contraseñas que el sistema le obliga a crear y cambiar constantemente, el usuario caiga en la tentación de apuntarlas en papel o en un archivo en texto plano. Aquí sería especialmente recomendable el uso de un programa gestor de contraseñas.

En cualquier caso, habrá que evaluar la criticidad de los sistemas a proteger y llegar a un compromiso entre la facilidad de gestión y el nivel de seguridad requerido. Una política muy robusta de contraseñas lleva aparejados frecuentes incidentes de tipo olvido de contraseñas, bloqueo de usuarios por sucesivos intentos fallidos, etc. que pueden hacer que no merezca la pena utilizarla en sistemas no críticos.

Casos prácticos 1

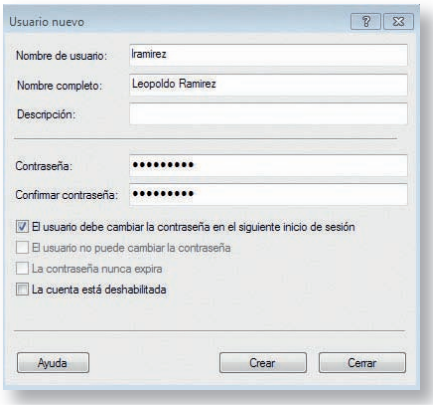
Administración de políticas de contraseñas

•• El administrador de sistemas de una empresa ha decidido aplicar una política de contraseñas que controle la elección, utilización y administración de las mismas, para evitar posibles intrusiones en el sistema. La política determina que:

- Cada usuario tendrá una contraseña establecida por defecto, que deberá cambiar por una de su elección en el próximo inicio de sesión.
- Las contraseñas que se elijan por los usuarios deberán ser de diez caracteres como mínimo y tendrán una vigencia máxima de un mes.

Indica cómo realizar dichas tareas si todos los usuarios utilizan Windows 7, versión Professional.

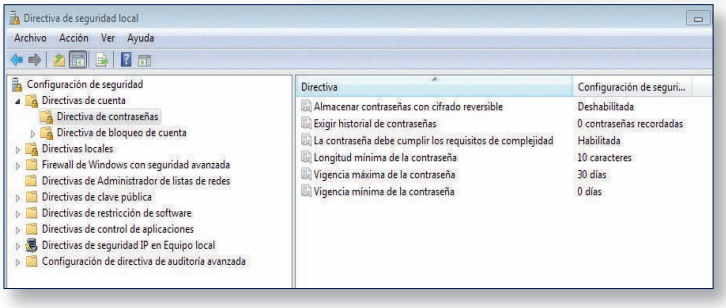
Solución •• Para establecer las contraseñas y poder gestionarlas adecuadamente, en primer lugar se debe crear una cuenta para cada usuario, a la que se podrán atribuir ciertos derechos y privilegios.



Para crear un usuario en Windows 7 hay que acceder al menú de Inicio / *Panel de control* / *Herramientas administrativas* / *Administración de equipos* / *Usuarios y grupos locales* / *Usuarios* / menú *Acción* / *Usuario nuevo*.

Se crea un usuario nuevo y se le asigna una contraseña determinada. En la misma ventana se marca la casilla de verificación *El usuario debe cambiar la contraseña en el siguiente inicio de sesión*.

Para configurar el resto de opciones de las contraseñas utilizadas por los usuarios, se debe abrir la consola de *Directivas de seguridad local*. Para ello, se accede desde menú de Inicio / *Panel de control* / *Herramientas administrativas* / *Directiva de seguridad local* / *Directivas de cuenta* / *Directivas de contraseña*. Una vez allí, en la parte derecha de la ventana, se configuran las opciones elegidas.



2.2 > Listas de control de acceso

En ocasiones, para restringir el acceso a los recursos del sistema no es suficiente con la utilización de perfiles de usuario y la creación de grupos, sino que es necesario realizar un ajuste más riguroso. Por ejemplo, puede existir un directorio donde únicamente deban acceder dos usuarios que pertenecen a grupos distintos para realizar cosas diferentes. Para estos supuestos se utilizan las listas de control de acceso o ACL (*Access Control List),* cuya utilización variará en función del sistema operativo instalado, aunque los fundamentos son los mismos.

Las listas de control de acceso son una herramienta que permite controlar qué usuarios pueden acceder a las distintas aplicaciones, sistemas, recursos, dispositivos, etc.

Las ACL son un mecanismo básico para proporcionar seguridad a las redes de datos pudiéndose utilizar tanto para restringir y controlar el acceso desde el punto de vista de la red (proporcionando seguridad a las redes de datos), como desde el punto de vista del sistema operativo para realizar esas mismas tareas sobre distintos recursos del sistema. Por un lado, los elementos constitutivos de la red suelen utilizar ACL basadas en direcciones de red, direcciones IP o direcciones MAC para configurar las políticas de acceso o bloqueo a los recursos. Así, mediante el establecimiento de políticas de seguridad en los *firewall* que protegen la red, puede permitirse el acceso desde o hacia solo determinados sistemas, pueden bloquearse todos los puertos que no vayan a ser explícitamente necesarios, etc.

Por otro lado, las ACL también se aplican masivamente en servicios básicos de red tales como *proxy* (para controlar quién puede salir a Internet o quién puede visitar qué páginas), servidores DNS (para evitar ataques desde direcciones IP no identificadas), servidores de correo electrónico (para evitar ataques por *spam* desde direcciones IP no autorizadas), etc.

Algunas de las ventajas de crear y utilizar ACL en redes son:

- Posibilidad de mejorar el rendimiento de la red limitando determinado tráfico. Por ejemplo, se puede impedir que los empleados de una oficina descarguen o visualicen ficheros de vídeo. Los ficheros de vídeo ocupan mucho ancho de banda y pueden llegar a colapsar la red.
- Posibilidad de permitir o denegar el acceso de equipos a ciertas zonas de la red. Por ejemplo, los alumnos que utilizan el servidor que proporciona servicios a su aula no deberían tener acceso al servidor de la secretaría del centro o los empleados que trabajan en una zona de red (caracterizada por un rango de direcciones IP) no deberían acceder a la zona de red donde trabaja el personal de administración.
- Permiten que no se ejecuten determinados comandos por la red destinados a fines malintencionados (instalación de troyanos, comandos de apagado, etc.).

A cambio, presentan el inconveniente de que la exhaustividad en el nivel de control complica bastante la administración de la seguridad del sistema. Por tanto, habrá que valorar hasta qué punto las ventajas superan a los inconvenientes en cada supuesto.

ACL en los *router*

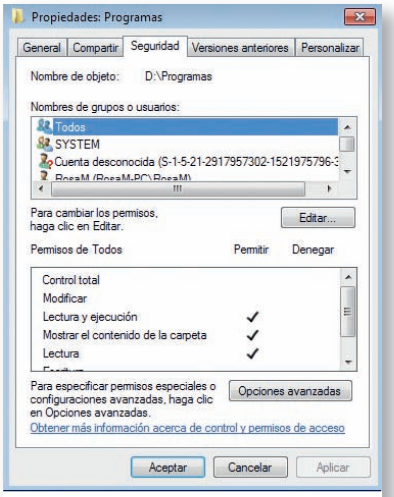
En los *routers* se pueden establecer listas de control de acceso de las siguientes formas:

- **Por protocolo:** se define una ACL para cada protocolo.
- **Por interfaz:** se define una ACL para cada interfaz del *router.*
- **Por dirección IP:** se define una ACL para restringir el tráfico por IP.

Veamos a continuación la configuración de las listas de control de acceso en los distintos sistemas operativos.

ACL en Windows

En sistemas Windows, las opciones de compartición de recursos van a depender del sistema de archivos con el que se trabaje. Si FAT32 únicamente permitía la compartición de recursos a todos los usuarios o prácticamente a ninguno, NTFS abre un mundo de posibilidades que permite aprovechar al máximo las ventajas de la compartición de recursos y la asignación de permisos avanzada. En los discos o volúmenes formateados con NTFS, cada fichero y cada directorio tiene una lista de control de acceso o permisos NTFS. Para cada usuario que tiene acceso a un directorio o a un fichero existe una entrada de acceso que indica el tipo de operaciones que puede realizar.



3.1. Lista de permisos en Windows.

Windows distingue dos tipos de privilegios de acceso:

- Los **permisos**: establecen la forma de acceder a un objeto concreto, por ejemplo, escribir un archivo NTFS.
- Los **derechos**: establecen qué acciones se pueden realizar en el sistema, como por ejemplo iniciar sesión.

El propietario de un recurso (o un administrador) asigna permisos sobre dicho recurso a través del cuadro de diálogo de propiedades del mismo. Por ejemplo, si en la carpeta *D:\Programas* se hace clic sobre ella con el botón secundario del ratón, se abre el cuadro de diálogo *Propiedades*. Si se selecciona la pestaña *Seguridad* se ven los usuarios que tienen permisos sobre ella.

Los administradores configuran los derechos y privilegios del usuario dentro del sistema a través de la consola *Directiva de seguridad local,* a la que se accede desde *Panel de control* / *Herramientas administrativas*. Desde allí también se puede configurar la asignación de los usuarios a grupos del sistema.

Los permisos sobre ficheros son distintos de los que se pueden aplicar a los directorios. Unos y otros tienen un usuario propietario, que es quien ha creado esa carpeta o fichero y quien tiene control total sobre el objeto.

Para cada objeto (fichero, directorio, recurso) se establece una lista de usuarios y/o grupos y a cada uno de ellos se les aplican los permisos pertinentes. Esta lista se denomina **ACL (*Access Control List*).** Cada una de las entradas que forman estas listas recibe el nombre de **ACE (*Access Control Entry*).**

En un sistema en red debidamente configurado, el administrador del sistema se encarga de establecer los permisos, los derechos y los privilegios del usuario. Los usuarios normales, no administradores, deberían tener privilegios mínimos o nulos dentro del sistema y no se les debería permitir la realización de acciones como la instalación de programas o modificaciones en el sistema. Tan solo deben ser propietarios de sus directorios de trabajo en zonas de trabajo seguras (directorios en la red, directorios locales, etc.).

Máscara

En Linux existe una máscara, o patrón de permisos por defecto, que se aplica en la creación de los ficheros y directorios. Los permisos por defecto en la creación de ficheros son 644 (`rw-r--r--`), mientras que para los directorios es de 755 (`rwxr-xr-x`).

ACL en Linux

Antes de ver cómo se establecen las listas de control de acceso en Linux, veremos cómo se establecen los permisos en Linux.

En Linux, todos los usuarios pertenecen a un grupo principal (que lleva el nombre de ese usuario o se le puede asignar otro existente) y, además, pueden pertenecer a otros secundarios. El usuario administrador del sistema se denomina root y tiene todos los privilegios del sistema, como la creación de nuevos usuarios, el cambio de las contraseñas de los otros usuarios o la ejecución de comandos privilegiados del sistema. Desde el punto de vista de la seguridad, no es recomendable trabajar con este usuario, sino con otro con menos privilegios.

Cada fichero o directorio pertenece a un usuario y, por tanto, a uno de los grupos a los que pertenece el usuario. Los permisos de cada fichero o directorio se ajustan para el usuario propietario (*u*), para su grupo (*g*) y para el resto (*o*).

Estos permisos aplicados implican que el recurso puede leerse (*r*), ser editado (*w*) o ser ejecutado (*x*), además existe un cuarto campo que indica la máscara.

Los permisos sobre ficheros y directorios se establecen mediante el comando `chmod`, usando la notación UGO o la notación octal. Por ejemplo: `chmod g-wx,o-rwx fichero` es lo mismo que `chmod 740 fichero`, lo que significa que el propietario tiene todos los permisos, los usuarios del grupo solo permiso de lectura y el resto de usuarios ningún permiso.

Ejemplos

Establecimiento de permisos en Linux

En un sistema Linux, tenemos creado un usuario tecnico1 que pertenece al grupo tecnicos. Al ejecutar el comando `ls -l` en un directorio, vemos una serie de columnas, de las cuales únicamente explicaremos las relevantes para este ejemplo.

```
[tecnico1@localhost ~]$ ls -l
total 32
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago  6 19:43 Descargas
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago  6 19:43 Documentos
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago  6 19:43 Escritorio
drwxr-xr-x. 2 tecnico1 tecnicos 4096 ago  6 19:43 Imágenes
```

- La primera columna contiene un grupo de letras que indican lo siguiente: la primera letra indica el tipo de fichero (`d` indica directorio), las tres siguientes letras indican los permisos (`r` lectura, `w` escritura, `x` ejecución) del usuario (tecnico1) sobre el directorio (por ejemplo *Descargas*); los tres siguientes caracteres indican los permisos (`r-x`, tiene permisos de lectura y ejecución pero no de escritura) del grupo al que pertenece el usuario (tecnicos); los tres siguientes indican los permisos del resto de usuarios (`r-x`, tiene permisos de lectura y ejecución pero no de escritura).
- La tercera columna hace referencia al usuario propietario del fichero o directorio, en este caso tecnico1.
- La cuarta columna hace referencia al grupo al que pertenece el usuario propietario (tecnicos).
- La última columna contiene el nombre del directorio o fichero (*Descargas, Documentos,* etc.).

En ocasiones, estos permisos no serán suficientes para establecer restricciones a los usuarios de un sistema, por ello se utilizan las ACL. Por ejemplo, puede existir un directorio al que interese dar acceso a todos los usuarios de dos grupos concretos, manteniéndolo restringido para el resto de los usuarios. En este caso, el permiso de grupo solo nos permitiría darle acceso al grupo propietario, dejando al otro fuera, mientras que el permiso *others* sería demasiado amplio, pues daría acceso a todos los grupos

En Linux, si las ACL están habilitadas, para activarlas en una partición o directorio hay que añadir la palabra `acl` al final de la línea correspondiente a dicha partición en el fichero `/etc/fstab.` A continuación tendríamos que desmontar y montar la partición:

```
#mount -o remount -o acl /dev/sda3 /home
```

En caso de no tener las ACL habilitadas, habría que descargar el paquete correspondiente.

Una ACL está compuesta por varias entradas, cada una de las cuales especifica los permisos de acceso a un recurso para un usuario o un grupo, utilizando una combinación de los permisos tradicionales de lectura (*r*), escritura (*w*) y ejecución (*x*). Estas entradas son:

- **La categoría:** usuario (*u*), grupo (*g*), otros (*o*) o máscara (*m*).
- **UID** (identificador de usuario) o **GID** (identificador de grupo) del usuario o grupo afectado. Este campo puede estar vacío, en cuyo caso la ACL se vincula al usuario propietario o al grupo propietario.
- **Cadena con los permisos asignados**.

El conjunto de la categoría y el identificador del usuario o grupo definen el tipo de entrada. En la tabla siguiente se muestran los tipos de entradas:

Tipo de entrada	Visualización	Descripción
owner	`u[ser]::rwx`	Privilegios de acceso del propietario.
group	`g[roup]::rwx`	Privilegios de acceso del grupo propietario.
other	`o[ther]::rwx`	Privilegios que no corresponden a ninguna entrada (otros).
named user	`u[ser]:name:rwx`	Privilegios de acceso para los usuarios identificados por una ACL.
named group	`g[roup]:name:rwx`	Privilegios de acceso del grupo identificado por una ACL.
mask	`m[ask]::rwx`	Privilegios máximos otorgados a *named user, group* y *named group*.

Las **tres primeras** entradas de la tabla se conocen como **ACL estándar** y coinciden con la gestión simple de los permisos: *owner, group* y *other.* **Las otras tres** se conocen como **ACL extendida**, que proporciona mayor flexibilidad, dado que permite otorgar permisos a un usuario concreto indicando su nombre (*named user*), a un grupo concreto indicando su nombre (*named group*) o utilizando una máscara (*mask*).

El orden de aplicación de reglas es el siguiente: *owner, named user, owning group, named group* y *other.* La máscara se aplica sobre cualquier entrada, a excepción de *owner* y *other*, esto es, actúa sobre las entradas de tipo *named user, owning group* y *named group.*

Comandos para trabajar con las ACL en Linux

Los comandos para trabajar con las ACL en Linux son:

- `setfacl`: sirve para establecer y asignar las ACL.
- `getfacl`: muestra las ACL de un archivo o directorio.

Ejemplos

Utilización de ACL en Linux

Vamos a ver cómo se utilizan las ACL en Linux; para ello, en primer lugar instalamos el soporte de ACL, ejecutando como root alguno de los siguientes comandos en función de la distribución Linux que tengamos instalada:

- `apt-get install acl` para distribuciones tales como Debian, Ubuntu, etc.
- `yum install acl` para distribuciones tales como en Red Hat, Fedora, etc.

A continuación creamos dos usuarios: tarzan, que pertenece al grupo jungle, y jane, que pertenece al grupo city. Para ello podemos usar la interfaz gráfica o bien los comandos siguientes:

- `groupadd jungle`
- `groupadd city`
- `useradd –m –G jungle tarzan`
- `useradd –m –G city jane`

Creamos dentro de nuestro directorio */home* un directorio llamado *mydir* con permisos `rwxrwx– – –`. Si lo hacemos con comandos, será: `chmod 0770 mydir` y, seguidamente, creamos los ficheros *docum1* y *docum2*, con permisos `rwxrwx– – –`. Si lo hacemos con comandos: `chmod 0770 docum*`.

El siguiente paso es asignar permisos de lectura, escritura y ejecución al grupo jungle para el directorio *mydir* con el comando: `setfacl –R –m g:jungle:rwx /home/alumno/mydir`. Al grupo city le asignamos permisos de lectura y ejecución para el directorio *mydir* con el comando: `setfacl –R –m g:city:rw /home/alumno/mydir`.

Ahora, asignamos permisos de lectura, escritura y ejecución al usuario jane para el fichero *docum1*. El usuario jane no puede leer ni escribir ni ejecutar el fichero *docum2*. Si lo hacemos con comandos será: `setfacl –m u:jane:rwx /home/alumno/mydir/docum1`.

Vamos a dar un paso más y añadimos un nuevo usuario llamado john al grupo jungle. Seguimos el mismo procedimiento que utilizamos con tarzan y jane. Una vez creado, comprobamos que puede entrar al directorio *mydir* y que puede leer o modificar los ficheros.

Si queremos limitar a este último usuario las acciones que puede realizar en este directorio, por ejemplo, le quitamos los permisos de lectura y ejecución al directorio *mydir* a través del comando `setfacl –m u:john:w /home/alumno/mydir` y comprobamos que no puede acceder a dicho directorio.

También podemos crear una máscara ACL en el directorio *mydir* que indique que los permisos máximos que tendrá en el mismo cualquier usuario que no sea el propietario o el resto serán de lectura o ejecución. La creamos a través del comando: `setfacl –m m::rx /home/alumno/mydir`.

Finalmente, comprobamos que los usuarios creados (tarzan, john o jane) no pueden crear archivos en el directorio *mydir* debido a la máscara, que elimina el permiso de escritura a cualquier usuario distinto del propietario u otros.

Actividades propuestas

6·· ¿Cómo se accede a la consola de *Directiva de seguridad local* en Windows?

7·· Indica algunas directivas relacionadas con la seguridad de contraseñas.

3 >> Acceso a aplicaciones por Internet

Internet es una fuente inagotable de recursos y de aplicaciones que nos facilitan mucho la vida. Tanto es así que nos parece casi imposible vivir sin estar conectados a Internet.

Varios son los tipos de aplicaciones a las que el usuario puede acceder, algunas de ellas no requieren ninguna credencial para su consulta o para trabajar con ellas, pero otras sí. Es importante garantizar y proteger la identidad de los usuarios cuando se identifican en una página web. Por otro lado, se deben configurar las páginas web de modo que la transferencia de datos con los usuarios sea segura, especialmente, si estos datos son sensibles.

Por eso, independientemente del tipo de aplicaciones web de que hablemos, hay unas normas generales aplicables a todas ellas que ponen especial énfasis en el eslabón más débil de la cadena a efectos de seguridad, el usuario:

- **Mantener actualizados tanto el sistema operativo como el navegador** y, dependiendo del sistema operativo instalado, disponer de un **antivirus actualizado.** Los *bugs* detectados y no corregidos mediante las actualizaciones son auténticos agujeros de seguridad.
- La importancia de una **correcta administración de los nombres de usuario y las contraseñas.** Todo lo dicho hasta ahora en esta unidad respecto a los sistemas operativos, aplicaciones y redes de comunicaciones es aplicable aquí.
- **Desconfiar de las webs en las que para regenerar una contraseña olvidada permiten introducir una cuenta de correo** a la que enviar la nueva contraseña debido a que, si alguien averiguara el identificador del usuario, podría conseguir fácilmente su contraseña.
- **Acceder a las distintas aplicaciones desde un ordenador seguro si los datos son muy sensibles** (fundamentalmente transacciones económicas): se debe evitar acceder desde ordenadores públicos (locutorios, bibliotecas, etc.), así como desde conexiones WiFi abiertas.
- **No facilitar por correo electrónico ni telefónicamente las contraseñas, ni modificarlas por estas vías:** la Administración Pública y las empresas como los bancos nunca solicitarán realizar operaciones de este tipo. Los correos que dicen ser de un banco y contienen un enlace a una página donde se solicitan claves suelen ser una trampa para conseguir estas claves.
- **No acceder nunca a través de enlaces** a la página web de una empresa u organismo público para realizar un trámite. Si se quiere acceder a estas páginas hay que teclear siempre en el navegador la dirección, para evitar ser víctima del *phishing*.
- **Cerrar la sesión correctamente**, usando el vínculo *Salir*, *Cerrar sesión* o similar de la página web en la que nos hallamos registrado, sea un banco o una cuenta de correo pues, en caso contrario, puede que la conexión quede abierta. Además, para mayor seguridad, después de cerrar cada sesión se deberían borrar los archivos temporales y el historial de navegación.

Phishing

Fraude que consiste en suplantar la identidad de otras personas o entidades a través de Internet para conseguir las claves de otra o para realizar en su nombre operaciones en la web.

En cuanto a las páginas de acceso, es importante asegurarnos de que el canal por el que se accede a la web en cuestión es fiable. Para ello, basta con observar en la barra de navegación que la dirección web comienza por https en vez de por http. Eso indica que la conexión es segura. Además, en el navegador suele aparecer un candado cerrado indicando que la conexión es cifrada y al hacer doble clic sobre él aparece el certificado de identidad del banco.

El protocolo **https** (*hyper text transfer protocol secure*) está basado en el **http** y su finalidad es proporcionar un plus de seguridad a la transmisión de datos sensibles. Este protocolo crea un canal seguro a base de cifrar los datos que se están transmitiendo, de modo que si se interceptan las comunicaciones únicamente se puede acceder a un código que el intruso no puede interpretar.

Por otro lado, la esencia de las transacciones de datos comerciales y administrativas realizadas por vía electrónica es la realización de un acto con eficacia jurídica (una declaración tributaria, una reserva de hotel, una transferencia bancaria, etc.). Por ello, tan importante como la seguridad en la transmisión de los datos es la acreditación de la identidad de las partes intervinientes. Para ello, se han creado los **certificados digitales**, que desarrollaremos en unidades posteriores.

En la emisión y gestión de estos certificados son esenciales las **autoridades de certificación**, instituciones a las que uno o más usuarios confían la creación y asignación de certificados y/o las claves de usuario. Por ejemplo, en España, CERES.

Además, en las **transacciones electrónicas de dinero** que se llevan a cabo en el comercio electrónico y en el uso de la banca *online*, hay que extremar las precauciones, pues no solo es información lo que está en juego sino también nuestro dinero. Estas páginas suelen incorporar medidas de seguridad adicionales como son la implementación de teclados virtuales en pantalla para introducir los datos (para evitar a los *keyloggers*). En la banca electrónica, se suele exigir para acceder a sus servicios, además del usuario y contraseña, la inserción de unas coordenadas que figuran en una tarjeta de coordenadas que la entidad entrega al usuario.

En todo caso, en estas transacciones electrónicas, las precauciones generales son comunes: comprobar que el canal por el que se accede a la web de la empresa u organismo público es fiable y que los métodos de pago (tarjeta de crédito, plataformas de pago, etc.) son seguros.

VeriSign

Es una empresa proveedora de servicios de autenticación que actúa como autoridad de certificación a nivel mundial. Emite certificados SSL para la protección de sitios en Internet. Por ello, si una conexión está verificada por esta empresa, ello indica que es un servicio de confianza.

Plataformas de pago

Una plataforma o pasarela de pago es un servicio de comercio electrónico que autoriza los pagos realizados a través de Internet. Cifra los datos sensibles, como número de cuenta o de tarjeta. Una de las más utilizadas es **PayPal.**

Actividades propuestas

8·· Entra en la web de una empresa de venta de libros (Casa del libro, Fnac, Amazon, etc.) y simula la compra de un libro. ¿Qué formas de pago te ofrece?

9·· ¿Has comprado alguna vez algún producto por Internet? ¿Qué medidas de seguridad de las que exponemos en este epígrafe observaste? ¿Qué método de pago utilizaste?

10·· Investiga en Internet el significado de *captcha,* BIDI y QR. ¿Para qué se utilizan? Busca ejemplos de la utilización de los mecanismos anteriores.

4 >> Otras alternativas de gestión de identidades

A lo largo de esta unidad hemos visto distintas posibilidades para controlar la seguridad en la gestión de los sistemas y aplicaciones informáticos. Estas medidas de seguridad se pueden centrar tanto en el acceso al propio sistema o aplicación, como en el acceso a ciertos recursos o funcionalidades del mismo.

Existen por tanto dos conceptos básicos que deben manejarse en la gestión de identidades de usuarios, como son la autenticación y la autorización. La **autenticación** es lo que permite identificar al usuario (mediante usuario y clave, certificado, etc.) mientras que la **autorización** es el mecanismo que decide a qué recursos puede acceder un usuario una vez autenticado.

4.1 > Autenticación de usuarios

Existen métodos de autenticación diferentes a los ya vistos de usuario y contraseña, como por ejemplo las contraseñas de un solo uso, los métodos basados en *hardware token* y los sistemas biométricos.

Contraseñas de un solo uso (OTP, *One Time Password)*

Se utilizan normalmente en entornos con elevados requerimientos de seguridad. Cada vez que se quiere acceder al sistema se utiliza una contraseña nueva, que tiene un periodo de validez muy corto, con lo cual se minimiza el efecto de acceso por intrusos. Por ejemplo, para realizar operaciones en la banca electrónica los bancos suelen enviar a sus usuarios por SMS la contraseña para realizar cada operación.

Security token, hardware token

Es un pequeño dispositivo hardware que autentica al usuario que lo lleva y permite, por ejemplo, su acceso a una red. Puede tomar diferentes formas (tarjeta, llavero, etc.).

Se utiliza lo que se llama autenticación de dos factores:

- El usuario tiene un número de identificación personal (PIN), que le autentica como propietario del dispositivo.
- El dispositivo muestra un número que identifica al usuario y le permite el acceso a determinado servicio.

El número de identificación es cambiado frecuentemente para cada usuario. Funciona de forma similar a las contraseñas de un solo uso, con la diferencia de que el valor que debe introducirse aparece en una pequeña pantalla en un dispositivo y este cambia regularmente.

3.2. Dispositivo *hardware token* RSA SecurID SID800.

Identificación biométrica

Se trata del uso de sistemas que permiten la autenticación de usuarios mediante características personales inalterables, como las huellas digitales, los rasgos faciales, el iris del ojo, etc. Requiere la instalación tanto de hardware adicional que capte este tipo de información, como de software específico (algoritmos de reconocimiento) que permita su posterior procesado y almacenamiento.

4.2 > Autorización de usuarios

En la operativa habitual de un sistema informático, cada aplicación realiza la autorización de sus usuarios de una manera (por roles, grupos de usuarios, etc.). Cuando se intenta centralizar la autenticación y la autorización de todas las aplicaciones en único sistema, se recurre a lo que se denomina sistemas de *Single Sign-On* (SSO).

Single Sign-On (SSO)

Uno de los principales problemas en las organizaciones es la gestión de identidades. En una organización normalmente habrá un sinfín de aplicaciones diferentes que requerirán unos determinados niveles de acceso en cada caso. Así, por ejemplo, todos los empleados deberán tener acceso a la Intranet corporativa para poder ver sus nóminas, pero solo un conjunto determinado de usuarios podrán acceder a las aplicaciones de gestión de contenidos para publicar información nueva en la Intranet. O, por seguir con el ejemplo, solo los directivos tendrán acceso al servidor con los informes del *data warehouse.*

En cada una de estas aplicaciones, lo habitual es que haya un método diferente de gestión de los usuarios (tendrán, por ejemplo, una base de datos de usuarios y contraseñas donde se almacene el rol del usuario, que es el que define el nivel de acceso a la aplicación). El problema de este enfoque es que ello obliga a los usuarios a introducir sus credenciales cada vez que cambian de aplicación e, incluso, a tener diferentes pares usuario/contraseña en cada una de ellas.

Aparte de la incomodidad de este sistema para el usuario, esto genera una serie de problemas adicionales de administración de usuarios, etc. Por ejemplo, si un usuario abandona la organización hay que proceder a borrar su usuario en todos los sistemas, lo cual puede suponer un quebradero de cabeza cuando estos son muy heterogéneos. Por ello, en las organizaciones, lo habitual es tratar de establecer sistemas de SSO, de forma que haya una única base de datos centralizada con todos los usuarios/contraseñas. El problema es gestionar desde esta base centralizada los diferentes roles que requiere cada aplicación y aquí es donde entra el proceso de autorización.

Uno de los protocolos más extendidos de autenticación es **Kerberos**, que ideó el sistema de generar un *ticket* para el usuario una vez se ha autenticado. Está muy extendido, ya que es el protocolo que utiliza el Active Directory *de* **Windows** para la gestión de los usuarios y roles del dominio. Así, con la combinación de Active Directory + Kerberos es posible establecer la base de un SSO para los servicios básicos proporcionados por la red corporativa de Windows.

Si tenemos aplicaciones de otros fabricantes o bien que han sido desarrolladas a medida, normalmente ya no basta con Active Directory para implementar el SSO. Será necesario que dichas aplicaciones lleven soporte nativo para integrarse con Active Directory o bien utilizar algún tipo de software que haga de intermediario y proporcione la integración SSO entre Active Directory y las aplicaciones.

Web Single Sign-On (Web-SSO)

Actualmente, la mayor parte de las aplicaciones que se desarrollan están pensadas para que el usuario acceda a estas mediante su navegador. Debido a esto, se han generalizado los sistemas de tipo **web-SSO**, que siguen un sistema semejante al SSO, con la diferencia de que solo sirven para acceso a aplicaciones vía navegador, ya que el *ticket* se intercambia entre el servidor web-SSO y el navegador del cliente, que guarda los datos relativos al *ticket* en *cookies.*

Así, cuando el usuario quiere acceder a alguna aplicación, esta le remite al servidor SSO para que introduzca allí sus credenciales. El SSO mira si se trata de un usuario registrado en la base de datos de usuarios (fase de autenticación) y, a continuación, una vez autenticado, examina si el usuario pertenece al rol necesario para acceder a la aplicación a la que pretende entrar. Si se cumple esta segunda condición (fase de autorización), se genera un *ticket,* que es lo que el usuario le presenta al servidor al que quería acceder. Con esto, además de facilitar la administración (en lugar de *n* sistemas de autenticación únicamente hay que gestionar uno centralizado), se evita que el usuario tenga que introducir sus credenciales repetidamente.

Identidad federada

En organizaciones muy grandes, con muchas sedes y departamentos independientes, es posible que cada sede tenga sus propias aplicaciones y, a la vez, existan una serie de aplicaciones comunes. En estos casos, se intenta establecer relaciones de confianza entre los distintos sistemas de SSO de forma que los usuarios puedan acceder a las aplicaciones a las que estén autorizados con las mismas credenciales en todas las sedes. Es lo que se denomina identidad federada.

OpenID

Es la aplicación de la identidad federada a Internet. Si en el caso anterior hablamos de una única organización con diferentes sedes, en este caso lo que tenemos son distintas webs sin relación alguna entre ellas.

El proyecto OpenID surge para ofrecer la posibilidad de crear una identidad federada entre todos los sitios web que decidan utilizar este sistema. Es, por tanto, un sistema abierto y descentralizado, ya que es mantenido por la comunidad de software libre y está disponible para cualquier aplicación o servicio que quiera usarlo.

Web

www.jasig.org/cas: página web del proyecto CAS de la Universidad de Yale, un sistema de web-SSO bastante extendido. Está basado en Java y es de código abierto.

Actividades propuestas

11·· Busca en Internet ejemplos de sistemas y aplicaciones informáticas donde se utilicen algunas de las alternativas de autenticación y autorización vistas en este epígrafe.

12·· ¿Qué sistemas de identificación biométrica utiliza el DNI electrónico?

13·· ¿Qué son los sistemas SSO?

14·· ¿Qué diferencia hay entre autenticación y autorización?

Actividades finales

.: CONSOLIDACIÓN :.

1·· Indica algunos mecanismos de los establecidos en las políticas de seguridad.

2·· ¿Qué se considera una contraseña segura?

3·· ¿Cómo sabes cuándo entras en una página o sitio seguro en Internet? ¿Se indica de alguna forma al visitante que sus datos utilizan un canal seguro?

4·· Si tu sistema operativo de trabajo es Windows, relaciona los parches que se instalan a través de las actualizaciones automáticas con la seguridad. Si tu sistema operativo es Linux, ¿las actualizaciones que se instalan tienen que ver con la seguridad?

5·· ¿Qué es un gestor de contraseñas? Indica algún ejemplo.

6·· Indica diferentes sitios en Internet a los que te conectes y que te pidan usuario y contraseña para entrar. ¿Se les puede considerar sitios seguros? ¿Por qué?

7·· ¿Dónde se almacenan las contraseñas de tu sistema operativo?

8·· ¿Qué procedimiento se utiliza en las cuentas de correo web, como Hotmail, Gmail, etc. para restablecer la contraseña si no la recuerdas? ¿Crees que es un procedimiento seguro? Justifica tu respuesta.

9·· ¿Qué es una lista de control de acceso o ACL?

10·· ¿Qué contraseña te parece más segura para un usuario llamado Armando Morales, nacido en 1980?

a) arm.ando
b) amorales80
c) ArmdM-80

11·· Realiza un breve esquema sobre los sistemas de autenticación vistos en la unidad.

.: APLICACIÓN :.

1·· Como técnico de sistemas en una empresa, te han encomendado reforzar el sistema de contraseñas de la misma. Los empleados utilizan para autenticarse un usuario y una contraseña. Revisando la operatoria de algunos de los empleados, has visto que muchos de ellos utilizan como usuario y contraseña la misma palabra. ¿Qué política de contraseñas utilizarías para reforzar la seguridad y evitar agujeros de seguridad como el que has detectado? Explica cómo hacerlo en un sistema operativo como Windows 7.

2·· Investiga qué medidas de seguridad lógica hay implementadas en el aula informática de tu centro de estudios. ¿Se pueden mejorar? ¿Cómo?

3·· En una empresa se está valorando la posibilidad de implantar un sistema biométrico de control de acceso basado en los rasgos faciales de las personas.

a) ¿Te parece un método seguro?
b) ¿Crees que posible "engañar" a un sistema de este tipo? ¿Cómo?
c) ¿Cómo podrían evitarse los accesos no autorizados al sistema?

4·· En un centro de trabajo con varios departamentos, donde los usuarios de cada departamento trabajan sobre su partición departamental correspondiente de disco del servidor, han decidido incrementar la seguridad encriptando algunas de estas particiones. ¿Cómo se puede realizar esta operación si se trata de un servidor Windows? ¿Y si es Linux?

Caso final 2

Auditoría de contraseñas en Linux

•• La empresa LIXSECURITY INC está muy preocupada por el tema de la seguridad informática. Por ello, ha encargado a su administrador de sistemas que realice un ajuste más seguro en las políticas de contraseñas de los usuarios. Una vez establecido el perfil y los permisos de usuario a través de permisos y ACL, ha decidido dar un paso más y comprobar la seguridad de las contraseñas del sistema.

El administrador de sistemas ha decidido comprobar la calidad de las contraseñas de su sistema operativo Linux utilizando la herramienta John The Ripper para auditar las contrseñas. De momento quiere probar la herramienta con tres usuarios, que son: Administrador (contraseña: *admin*), plopez (contraseña: *pepe-el-de-cuentas*), mrobles (contraseña: *123responda3*)

¿Cómo llevará a cabo esta tarea?

Solución •• En primer lugar instalaremos la herramienta John The Ripper descargando el fichero comprimido que la contiene. Al descomprimir, veremos que se crean varios subdirectorios. En el directorio *doc* se encuentra el fichero de ayuda *INSTALL*. El fichero *EXAMPLES* contiene ejemplos de uso de esta herramienta.

Para instalar la aplicación, desde el directorio *src*, en línea de comandos ejecutaremos el comando `make`. Nos aparecerá un listado con las distintas opciones de instalación en función de la plataforma. Es importante que se elija la plataforma correcta. En nuestro caso, elegiremos `linux-x86-sse2`, que es el más habitual para arquitecturas de 32 bits. Para compilar ejecutaremos el siguiente comando desde el subdirectorio *src:*

```
$make clean linux-x86-sse2
```

Esto creará los archivos ejecutables de John The Ripper y sus utilidades relacionadas en el directorio *run* de la instalación. Desde el directorio *run* ejecutaremos:

```
$./john ––test
```

Esto ejecuta John y realiza un test de velocidad probando con distintos cifrados de contraseñas (DES tradicional, MD5, etc.). En función del ordenador, este test tardará más o menos tiempo en ejecutarse.

Antes de empezar a usar John, hay que realizar la fusión de la información del fichero */etc/passwd* con el fichero */etc/shadow*. En Linux, las contraseñas ya no se guardan en */etc/passwd* sino que se cifran en */etc/shadow,* solo accesible por root. Para realizar esto, desde el directorio *run,* con privilegios de root ejecutaremos:

```
#./unshadow /etc/passwd /etc/shadow > mypasswd
```

Esto crea un fichero llamado *mypasswd* con la información fusionada. A continuación ejecutaremos:

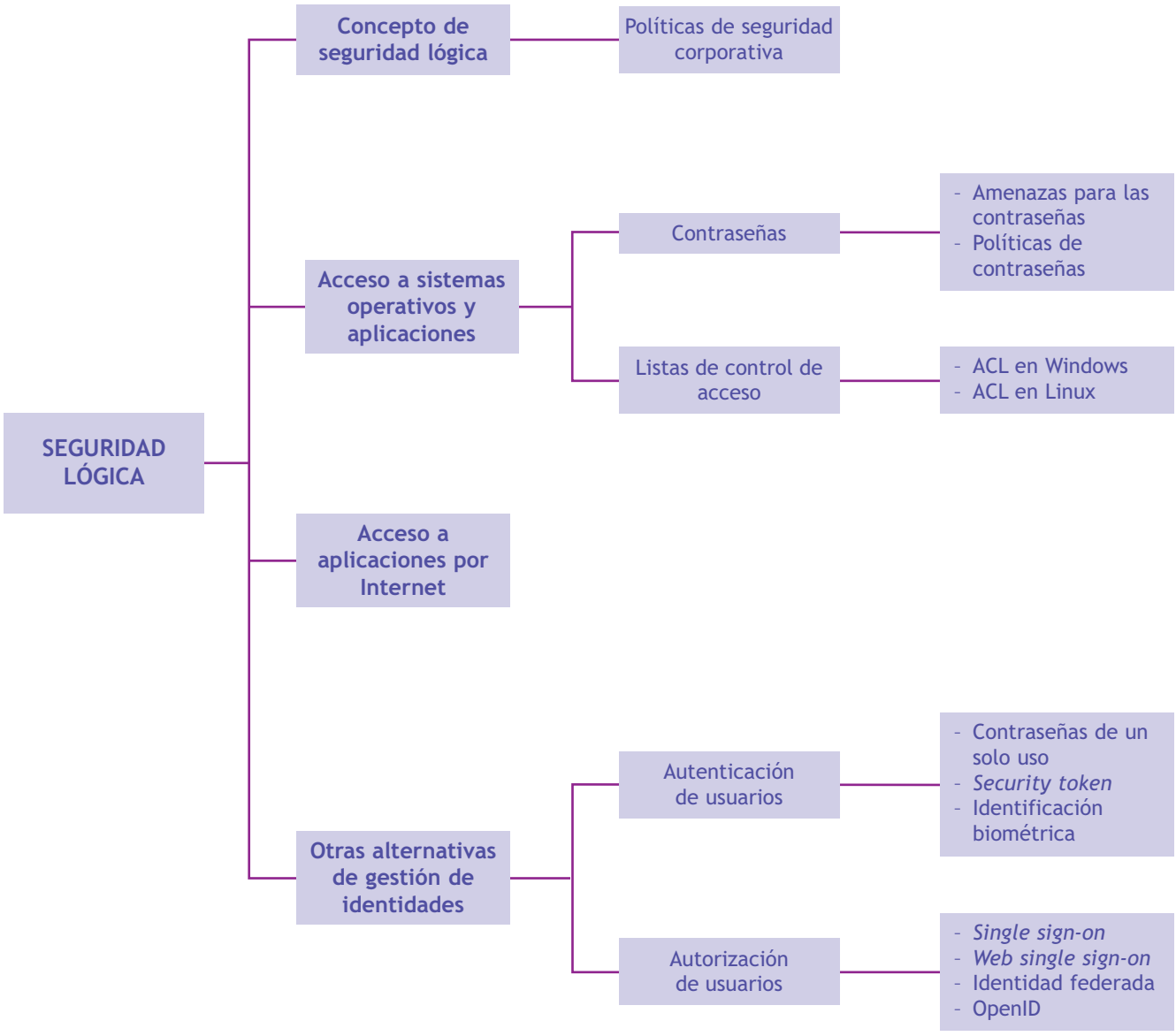
```
#chmod a+r mypasswd
```

Que dará permisos de lectura al fichero, para poder ejecutar John y leer el fichero con el usuario habitual. Desde el directorio *run* ejecutaremos:

```
$./john mypasswd
```

Pasamos como parámetro el fichero de contraseñas que debe intentar descifrar. John va a intentar descubrir las contraseñas de todos los usuarios del fichero con distintas técnicas, como la fuerza bruta y probando combinaciones definidas en las reglas del programa (que se pueden modificar). Podemos comprobar que enseguida adivina las contraseñas débiles, entre las cuales está la del usuario Administrador.

Ideas clave


SEGURIDAD LÓGICA
Concepto de seguridad lógica
Políticas de seguridad corporativa
Acceso a sistemas operativos y aplicaciones
Contraseñas
- Amenazas para las contraseñas
- Políticas de contraseñas
Listas de control de acceso
- ACL en Windows
- ACL en Linux
Acceso a aplicaciones por Internet
Otras alternativas de gestión de identidades
Autenticación de usuarios
- Contraseñas de un solo uso
- *Security token*
- Identificación biométrica
Autorización de usuarios
- *Single sign-on*
- *Web single sign-on*
- Identidad federada
- OpenID

Programas espía

¡Cuidado con los programas espía! Qué son y cómo evitarlos

Los programas espía o *spyware* se han convertido en apenas seis meses en uno de los mayores peligros que acechan al internauta mientras navega por Internet. Las cifras que ofrece un reciente informe de G Data Security Labs demuestran que esta clase de códigos malignos han crecido en un 50% en el último semestre. Lo más peligroso de estos programas es que se utilizan para robar todo tipo de datos personales, pero sobre todo los referentes a las cuentas bancarias y las tarjetas de crédito.

Estos datos son después ofrecidos en el mercado negro de Internet para que los delincuentes monten todo tipo de estafas con ellas. Como es habitual, el sistema operativo más castigado por esta plaga es Windows. La infección por programas espía suele tener siempre el mismo patrón. En primer lugar, se instala en el ordenador un troyano que o bien lleva en su interior el programa espía y lo instala, o se conecta en remoto a una página de donde lo descarga.

El negocio del robo de información personal se ha disparado en los últimos meses. Según Ralf Benzmüller, experto en seguridad y responsable de G Data Security Labs, "se están recolectando datos de tarjetas de crédito, direcciones y contraseñas de correos electrónicos, datos de acceso a juegos *online*, números de registro de programas informáticos y códigos de clientes del servicio de mensajería urgente. Toda esta información se puede transformar en poco tiempo en dinero negro".

Las listas de precios aparecidas en ciertos foros de *hackers* demuestran que esta es una economía de escala, en la que el delincuente está obligado a obtener miles de contraseñas y claves de acceso para que el negocio sea rentable. Las cuentas de PayPal cuestan unos cuatro euros, mientras que las tarjetas de telefonía móvil se ofrecen a partir de 10 euros. Por 250 euros se consigue una lista con un millón de direcciones de correo electrónico que llenar con correo basura. También se venden claves de acceso para juegos *online,* por entre 7 y 15 euros, y todo tipo de complementos de juegos.

Los programas espía suelen ser bastante discretos, pero conllevan una serie de consecuencias desagradables que los delatan. Si el navegador pierde la página de inicio habitual y muestra otra diferente, o recibimos avalanchas de ventanas publicitarias incluso sin estar conectados a Internet, o si el ordenador tarda más tiempo en arrancar, hay muchas posibilidades de que el ordenador tenga una infección de programas espía. Otros síntomas pueden ser la navegación lenta, los errores frecuentes al intentar entrar en determinadas páginas o al realizar ciertas búsquedas relacionadas con la seguridad. En ocasiones, también aparece una ventana que indica que el ordenador está infectado y ofrece un enlace gratuito de donde descargar un sistema antivirus. Cualquiera que pulse dicho enlace habrá infectado voluntariamente y sin saberlo su propio ordenador.

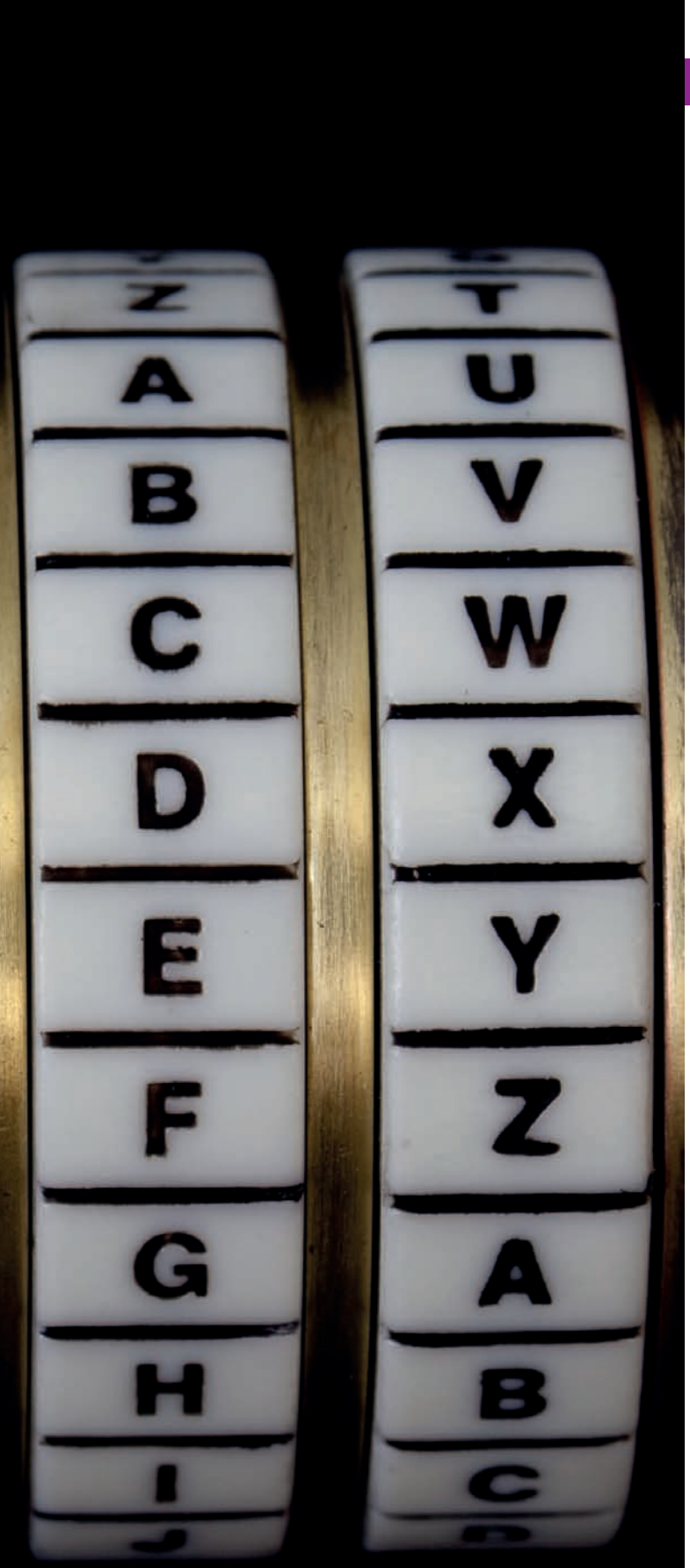
Para evitar este tipo de ataques maliciosos, es imprescindible tener un ordenador limpio, con un antivirus actualizado periódicamente. Si en lugar de antivirus es una *suite* completa de seguridad, los resultados serán mucho más satisfactorios. De todas formas, ningún antivirus es invulnerable y por eso es conveniente tener además herramientas extra como por ejemplo Spybot Search and Destroy, o el conocido AdAware.

Fuente: Juan F. Marcelo www.tuexperto.com

Actividades

1·· ¿De qué tipo de ataques habla el artículo? ¿Se pueden evitar? ¿Cómo?

2·· En el texto se habla de algunos productos de "limpieza" en concreto. ¿Podrías ampliar la información e indicar otras herramientas que realicen las funciones deseadas de prevención de riesgos informáticos?



unidad 4

Criptografía

SUMARIO

- Introducción a la criptografía
- Cifrado de clave simétrica
- Cifrado de clave asimétrica
- Algoritmos de cifrado *hash*
- Criptosistemas híbridos

OBJETIVOS

- Conocer qué es la criptografía y para qué se utiliza.
- Distinguir los tipos de sistemas de cifrados utilizados en la criptografía.
- Describir las ventajas e inconvenientes de los criptosistemas.
- Conocer el algoritmo de cifrado *hash*.
- Apreciar las ventajas de los criptosistemas híbridos.

1 >> Introducción a la criptografía

Desde que el ordenador pasó a formar parte de nuestras vidas almacenando nuestros datos personales y convirtiéndose en una de las principales herramientas de comunicación, mediante el uso de Internet, ha ido creciendo la conciencia de que nuestros datos están expuestos a posibles intromisiones por parte de otras personas que quisieran apoderarse de ellos.

Esto ha hecho que, cada vez más, vayamos tomando conciencia de los peligros que supone dejar desprotegidos y a merced de posibles intrusos estos datos. La peor consecuencia de que alguien entre en nuestros equipos o intercepte nuestras comunicaciones es que se lleve datos importantes, como claves bancarias, números de tarjetas de crédito, etc., que pongan en riesgo nuestra integridad o permitan la suplantación de nuestra identidad.

Cuando se habla de medidas de seguridad informática, lo primero que nos viene a la cabeza son las medidas destinadas a impedir infecciones o accesos no autorizados en los equipos informáticos. Pero hay otro tipo de medidas que se pueden tomar respecto de los propios datos y son las consistentes en hacer que estos datos sean indescifrables por personas que accedan a ellos indebidamente.

Por ello, vamos a ver en qué consisten todas estas medidas: qué es un certificado digital, qué significa encriptar o cifrar un mensaje, qué significa el símbolo del candado en las comunicaciones por Internet, qué diferencia hay entre utilizar HTTP o HTTPS a la hora de navegar por Internet, etc.

1.1 > Definiciones

Esta materia utiliza una terminología específica con la que debemos familiarizarnos:

- **Criptología:** proviene del griego *krypto*, "oculto", y *logos*, "estudio". Se trata del estudio de los criptosistemas. Sus áreas principales de estudio son, entre otros, la criptografía y el criptoanálisis:
  - **Criptografía**: proviene del griego *krypto*, "oculto", y *graphos*, "escribir"; es decir, significa "escritura oculta". El diccionario de la RAE lo define como "el arte de escribir con clave secreta o de un modo enigmático". La criptografía no pretende ocultar un mensaje, sino únicamente su significado, a través de la codificación.
  - **Criptoanálisis:** es la ciencia que se ocupa de descifrar criptogramas rompiendo la clave utilizada para descubrir el contenido del mensaje. Es el reverso de la criptografía.
- **Criptosistema:** según el Centro Criptológico Nacional (CCN), es el conjunto de claves y equipos de cifra que, utilizados coordinadamente, ofrecen un medio para cifrar y descifrar.

Relacionando todos estos conceptos, podemos decir que la criptografía está integrada por las técnicas utilizadas para, utilizando una clave, convertir un mensaje inteligible (llamado texto nativo) en otro (texto cifrado), cuyo contenido solo puede ser comprendido por quienes conozcan la clave. Los algoritmos de cifrado son el método utilizado para ocultar el contenido del mensaje y el criptosistema es el conjunto de equipos y claves usados para cifrarlo.

Vocabulario

Cifrar: transcribir, utilizando una clave, un mensaje cuyo contenido se quiere ocultar.

Clave: conjunto de signos utilizados para la transmisión de un mensaje privado cuyo contenido se quiere ocultar.

Orígenes de la criptografía

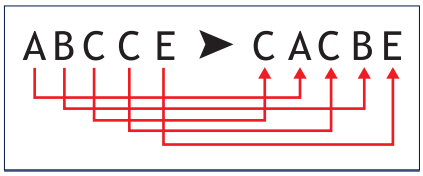
El primer método de criptografía conocido fue la escitala, utilizado en Esparta en el siglo V a. de C., que utilizaba técnicas de transposición.

Los sistemas evolucionaron hacia el uso de la sustitución de caracteres, como por ejemplo en el cifrado César, utilizado en Roma por Julio César.

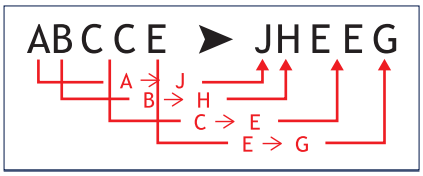
El uso de cifras y claves no es nuevo, ni ha venido de la mano de las nuevas tecnologías. Ya en la antigua Grecia, cuando se quería ocultar un mensaje, se utilizaba la **esteganografía**, que era una técnica consistente en ocultar el mensaje en sí mismo (por ejemplo, utilizando tinta invisible). Este sistema no ofrecía gran seguridad, ya que cualquiera que consiguiera acceder al mensaje podría ver su contenido. Por ello, comenzaron a utilizarse los primeros métodos de criptografía. La criptografía clásica se basaba métodos como el intercambio de letras, el ocultamiento del mensaje dentro de otro, etc. La criptografía moderna se basa en el uso de las matemáticas y en la utilización de mecanismos de cifrado (máquinas de cifrado o, actualmente, ordenadores).

Los sistemas criptográficos se basan en dos técnicas:

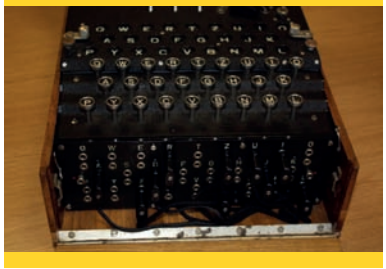
- **Transposición:** los signos o símbolos del mensaje original se cambian de posición.
- **Permutación o sustitución:** los signos o símbolos del mensaje original son sustituidos por otros.



4.1. Transposición.



4.2. Sustitución.



Máquina Enigma

La máquina Enigma se usó en la Segunda Guerra Mundial por las fuerzas militares de Alemania para cifrar los mensajes.

Usaba un mecanismo de cifrado rotatorio que le permitía tanto cifrar como descifrar. Su sistema de cifrado fue finalmente descubierto.

A lo largo de la historia, por tanto, las claves para mantener oculto un mensaje eran la técnica utilizada y el algoritmo empleado, que únicamente debían ser conocidos por el emisor y el receptor del mensaje. Si se daba esta premisa, el mensaje resultaría indescifrable; ahora bien, el problema de todos estos sistemas es que en toda lengua existen una serie de patrones (distribución de los espacios entre palabras, letras que se repiten con más frecuencia, etc.) a partir de los cuales es posible deducir el algoritmo, con lo cual se pierde la privacidad del mensaje.

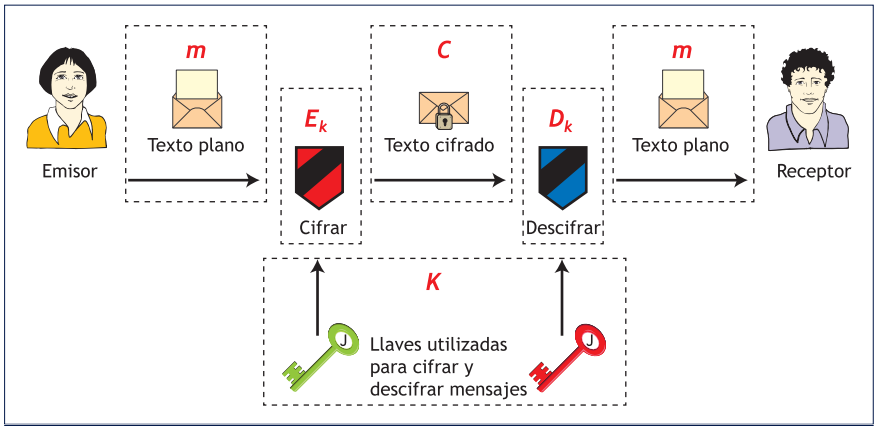
Por ello, la gran novedad de los criptosistemas modernos ha sido la introducción de métodos en los que el algoritmo es públicamente conocido y el secreto está en la clave que se utiliza como base para el cifrado. También es posible que el sistema simultanee ambas operaciones (algoritmo y clave desconocidos).

1.2 > Elementos de un criptosistema

Los criptosistemas están compuestos por los siguientes elementos:

- **Mensajes sin cifrar, texto plano o texto nativo *(m)*:** son los documentos originales sin haber sido cifrados.
- **Mensajes cifrados *(C)* o criptogramas.**
- **Conjunto de claves *(K)*:** son los datos o llaves que permiten cifrar los mensajes.
- **Transformaciones de cifrado *(E)*:** existe una transformación diferente para cada valor de la clave *k*.
- **Transformaciones de descifrado *(D)*.**

Veamos cada elemento en un esquema para comprenderlo mejor:



4.3. Esquema de un criptosistema.

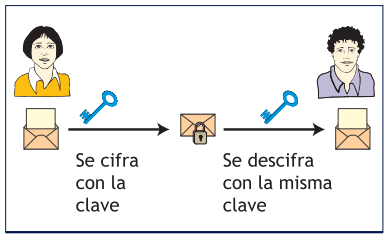
Todo criptosistema cumple la propiedad $D_k \cdot [E_k(m)] = m$.

Es decir, si se tiene un mensaje m y se cifra utilizando la clave k, se obtiene E_k. Si a ese mensaje cifrado se le aplica la transformación de descifrado para esa misma clave (D_k), se obtiene el mensaje original m.

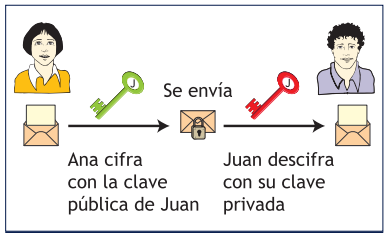
1.3 > Tipos de sistemas de cifrado

Hay dos tipos de sistemas de cifrado basados en claves, aunque existen también otros sistemas no basados en clave, de los que hablaremos más adelante:

- **Criptosistemas simétricos o de clave secreta.** En estos sistemas existe una única clave secreta que conocen y comparten emisor y receptor y que es utilizada para cifrar y descifrar el mensaje. La seguridad de este tipo de sistemas consiste en mantener dicha clave en secreto.
- **Criptosistemas asimétricos o de clave pública.** En este tipo de sistemas cada usuario crea un par de claves inversas: una privada y otra pública. Lo que el emisor cifra con una clave, el receptor lo descifra con la clave inversa. La seguridad de este tipo de sistemas radica en la dificultad de averiguar la clave privada a partir de la pública.



4.4. Sistema de clave simétrica.



4.5. Sistema de clave asimétrica.

Actividades propuestas

1·· Averigua qué es una escítala y explica en qué consistía. Consigue una imagen y referencias web.

2·· Investiga los orígenes del cifrado César. En qué consiste y qué vulnerabilidades presenta. Crea un mensaje cifrado utilizando este método y entrégaselo a un compañero para que lo descifre.

3·· Cifra el mensaje "Bienvenidos a la criptología" mediante la técnica de sustitución, usando la siguiente tabla de equivalencias:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

2 >> Cifrado de clave simétrica

Como ya hemos avanzado en el punto anterior, en estos sistemas se utiliza la misma clave para cifrar y descifrar un mensaje. Dicha clave solo deberá ser conocida por el emisor y el receptor del mensaje y deberá mantenerse en secreto y a buen recaudo, pues en cuanto un atacante la descifre el criptosistema se ha roto.

Estos sistemas son mucho más rápidos y sencillos de implementar que los de clave pública (asimétrica) y resultan apropiados para el cifrado de grandes volúmenes de datos.

Hay dos grandes grupos de algoritmos de cifrado:

- **Cifradores de flujo:** cifran bit a bit.
- **Cifradores de bloque:** cifran un bloque de bits (habitualmente, cada bloque es de 64 bits) como una unidad.

Uno de los inconvenientes de este tipo de cifrado es que la clave debe ser conocida por el emisor y el receptor, quienes deben encontrar un modo seguro de comunicarla entre ambos.

El manejo de claves de este tipo de sistemas es costoso, ya que se necesita una clave por cada par de usuarios, lo que hace crecer exponencialmente el número de claves según se van incrementando los usuarios. El número de claves sería una combinación de m elementos (el número de usuarios) tomados de n en n (en este caso, de dos en dos, pues las claves las comparten siempre dos personas). Para calcular el número de claves necesarias aplicaríamos la siguiente fórmula:

$$C_m^n = \frac{m!}{n!(m-n)!}$$

Por ejemplo, para cinco usuarios harían falta:

$$C_5^2 = \frac{5!}{2!(5-2)!} = 10$$

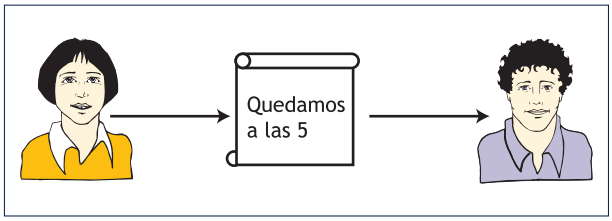
Hay dos sistemas para atacar un cifrado asimétrico:

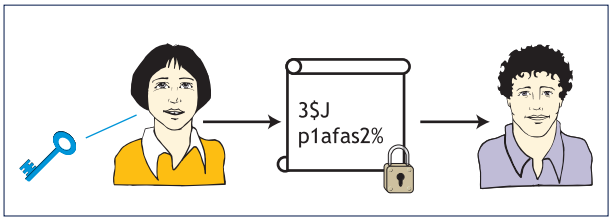
- **Criptoanálisis.** Se basa en la naturaleza del algoritmo y el conocimiento de algunas características del texto nativo y algunos pares texto nativo/texto cifrado. Este tipo de ataque aprovecha las características del algoritmo para intentar averiguar el texto originario o bien la clave secreta que se está utilizando. Este último sería el peor de los casos, ya que compromete todas las comunicaciones cifradas con esa clave. Es el caso del cifrado WEP en redes inalámbricas.
- **Método de fuerza bruta.** Consiste en probar todas y cada una de las posibles claves empleadas para cifrar el texto. Una vez que se haya encontrado la clave adecuada, ya se podrá descifrar el mensaje. La fortaleza del cifrado en casos de ataque por fuerza bruta depende de la complejidad de la clave que se haya empleado para cifrar. Si la clave es corta o fácilmente deducible, el sistema será vulnerable a este tipo de ataques aunque el algoritmo sea robusto.

Ejemplos

Utilización de clave simétrica

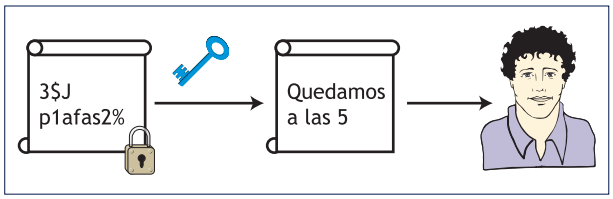
Vamos a ver en un ejemplo el funcionamiento de la clave simétrica. Ana quiere enviar un mensaje a Juan y, como pretende que su contenido sea secreto, lo cifra utilizando una clave simétrica. Esta clave debe ser conocida tanto por Ana como por Juan.



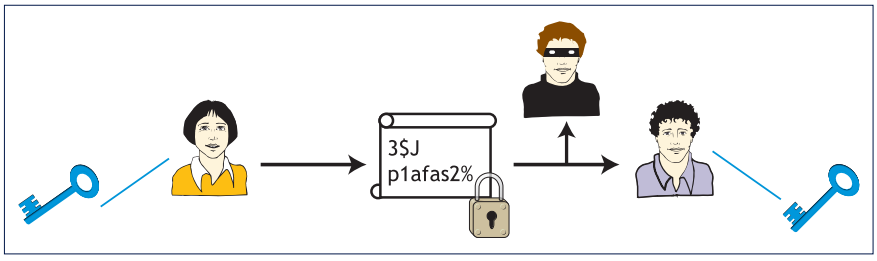


Una vez que Ana ha utilizado la clave, el mensaje será indescifrable para todo el mundo excepto para Juan, que conoce la clave. ¿Qué pasa si una tercera persona intercepta el mensaje?

El mensaje solo puede descifrarse si se conoce la clave. En este caso, solo lo puede descifrar Juan, que es quien conoce la clave.



Si un intruso interceptase el mensaje, solo podría descifrarlo si conociera la clave compartida por Ana y Juan. Eso podría suceder si Ana o Juan no la guardaran adecuadamente o si hubieran fijado una clave no muy compleja, fácil de ser averiguada por ataques de fuerza bruta.



Ventajas e inconvenientes de los sistemas de cifrado simétricos	
Ventajas	- Son rápidos y eficientes. - Resultan apropiados para el cifrado de grandes volúmenes de datos.
Inconvenientes	- Exigen una clave diferente por cada pareja de interlocutores (el espacio de claves se incrementa enormemente conforme aumentan los interlocutores). - Requiere un control estricto sobre el intercambio seguro de la clave entre el emisor y el receptor. - Son vulnerables a ataques por fuerza bruta, por lo que la fortaleza de la clave es fundamental.

Algoritmos de cifrado

Algunos de los algoritmos de cifrado más utilizados son los siguientes:

DES (*Data Encryption Standard*)

Nació en los años 70 y fue un algoritmo de cifrado muy utilizado hasta no hace mucho, no caracterizándose precisamente por su seguridad.

Utiliza cifrado por bloques con bloques de 64 bits, esto es, toma un texto plano de esa longitud y lo transforma, mediante una serie de operaciones, en texto cifrado de la misma longitud.

Se utilizan claves de 64 bits, de los cuales solo se utilizan 56, para realizar el cifrado de los bloques. El resto llevan información de paridad. Esta longitud tan corta se considera insuficiente para protegerse frente a ataques de fuerza bruta y es uno de los motivos por los que se considera inseguro, ya que estas claves se han llegado a romper en 24 horas. Aun así se sigue utilizando en las transacciones realizadas en cajeros automáticos.

AES (*Advanced Encryption Standard*)

El estándar de encriptación avanzada es uno de los algoritmos más populares de clave simétrica y, de hecho, remplazará al DES utilizado habitualmente.

Es rápido y eficiente y proporciona una encriptación segura utilizando un cifrado por bloques, con bloques de 128 bits y claves de 128, 192 o 256 bits. Se utiliza fundamentalmente en aplicaciones bancarias por Internet, comunicaciones inalámbricas, protección de datos en discos duros, etc.

RC5 (*Rivest Cipher*)

Diseñado por Ronald Rivest en 1994, se trata de un algoritmo que opera con un tamaño variable de bloques (32, 64 y 128 bits) y un número también variable de claves (entre 0 y 2040 bits).

Puede implementarse tanto por hardware como por software, consumiendo poca memoria y adaptándose a microprocesadores con distintos tamaños de palabra.

Aunque es muy seguro, se puede mejorar su efectividad modificando sus modos de operación: RC5-cifrador en bloque, RC5-CBC, RC5-CBC-relleno, RC5-CTS.

IDEA (*International Data Encryption Algorithm*)

Es un algoritmo descrito por primera vez en 1991 y propuesto para reemplazar al DES.

Este algoritmo trabaja con bloques de 64 bits y utiliza una clave de 128 bits, lo que hace que sea inmune al criptoanálisis diferencial. Además, el enorme número de posibles claves que hay que analizar hace que, con el estado actual de la computación, sea imposible de averiguar a través de ataques por fuerza bruta.

Al igual que ocurría con DES, en IDEA se usa el mismo algoritmo para el cifrado y el descifrado.

Triple DES

Triple DES aumenta la seguridad de DES ejecutando el algoritmo DES tres veces, cada una de ellas con una clave distinta. Aunque está siendo sustituido por AES, aún es el algoritmo utilizado por muchas tarjetas de crédito.

Algoritmo Rijndael

AES también es conocido como algoritmo Rijndael. El NIST (Instituto Nacional de Estándares y Tecnología de EEUU) convocó un concurso de algoritmos de encriptación para incorporarlos al estándar AES que estaban preparando. Los belgas Joan Daemen y Vincent Rijmen enviaron su algoritmo Rijndael, que resultó el ganador del concurso y fue adoptado por el estándar.

Sistemas de cifrado en redes inalámbricas

Los sistemas de cifrado más comunes en las redes inalámbricas como WEP, WPA-PSK, WPA2-PSK utilizan sistemas de clave simétrica como RC4 o AES.

Ejemplos

Criptografía de clave simétrica

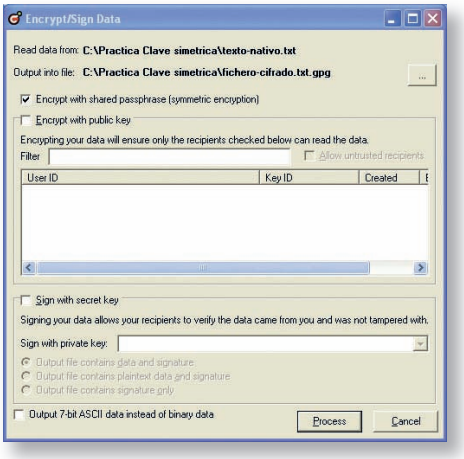
Vamos a mostrar con un ejemplo cómo funciona un criptosistema de clave simétrica.

Para ello utilizaremos un programa llamado Cryptophane, que funciona bajo Windows. Se trata de una aplicación de software libre que además permite utilizar el sistema de cifrado simétrico y el asimétrico. Para el cifrado de clave pública utiliza GnuPG, una versión libre de PGP.

Cryptophane permite encriptar archivos y firmarlos para verificar su autenticidad. También permite descifrar archivos cifrados y verificar firmas generadas con cualquier aplicación de OpenPGP.

En primer lugar instalamos el programa Cryptophane descargándolo de la siguiente dirección web: http://code.google.com/p/cryptophane/

A continuación creamos en el equipo un documento de texto. No es necesario que su extensión sea .doc u .odt, basta con un archivo en texto plano de tipo .txt. Lo llamamos *Fichero-nativo.txt* y escribimos un contenido dirigido a otra persona.



Abrimos el programa y seleccionamos *File / Encrypt* (o <Ctrl> + <E>) para seleccionar un documento a encriptar.

Seleccionamos el archivo e indicamos que se guarde con el nombre *Fichero-cifrado.txt* (botón *Output into file...*). En la ventana que aparece después, seleccionamos *Encrypt with shared passphrase (symmetric encryption)* (y desmarcamos *Encrypt with public key)*. Hacemos clic en el botón *Process* y luego escribimos dos veces la clave que vamos a usar para el cifrado simétrico.

Enviamos el documento a otra persona y le indicamos la clave a través de un canal seguro, porque si no la encriptación no serviría de nada (por ejemplo, si le enviamos el documento cifrado, lo que no podemos es enviarle la clave en el mismo mensaje).

Cuando el destinatario del mensaje quiera abrir el fichero cifrado con el Bloc de notas, le pedirá la clave utilizada para encriptarlo, que le habrá sido proporcionada por el emisor. Sin esa clave, no podrá abrir el archivo. Evidentemente este archivo es ininteligible para cualquier persona que lo abra sin tener la clave.

Actividades propuestas

4·· Si tenemos seis usuarios que quieren comunicarse por medio de cifrado simétrico, ¿cuántas claves serán necesarias? ¿Cuántas se necesitarían si se aumentara en un usuario más?

5·· Investiga qué otros algoritmos de clave simétrica existen además de los expuestos en este apartado y explica brevemente en qué consisten.

3 >> Cifrado de clave asimétrica

Los sistemas de clave simétrica vistos en el epígrafe anterior se basaban en que el proceso de descodificación de un mensaje era esencialmente igual al utilizado para la codificación, solo que a la inversa. La gran novedad de los sistemas de cifrado de clave asimétrica es, precisamente, que la clave y el sistema utilizado para cifrar el mensaje son diferentes a los usados para el descifrado.

Estos sistemas utilizan **un par de claves: una privada** (que solo conoce su propietario) y **otra pública**, que es de conocimiento general y, de hecho, se distribuye a todo el mundo. Pese a la existencia de estas dos claves, estos sistemas se suelen conocer popularmente como sistemas de clave pública.

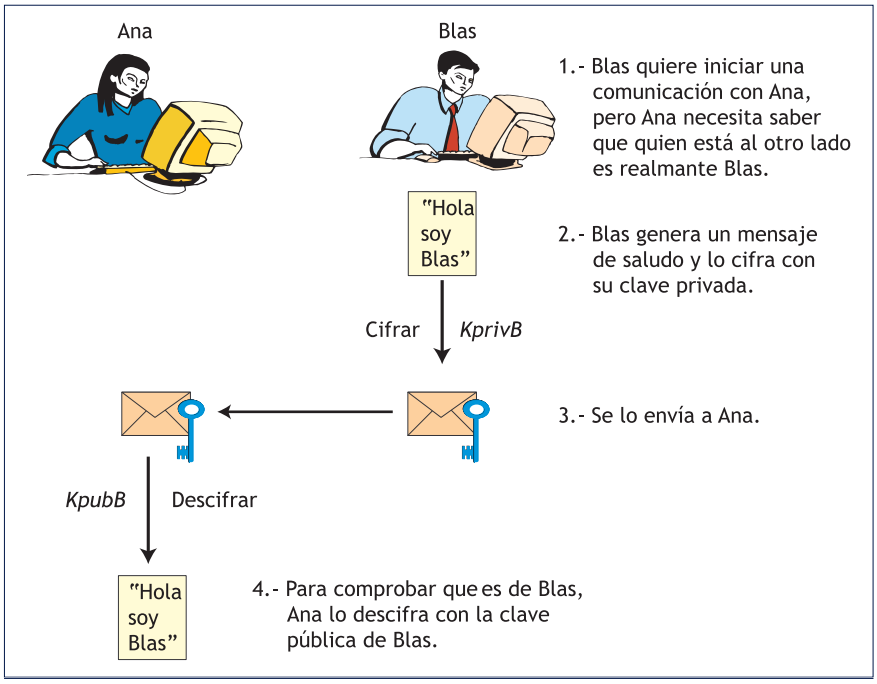
La criptografía asimétrica tiene dos usos principales:

– Autenticación.
– Confidencialidad.

3.1 > Autenticación con claves asimétricas

Para garantizar que el remitente de un mensaje es quien dice ser, este cifra el mensaje con su clave privada (no se cifra el mensaje completo, ya que esto supondría un mayor consumo de CPU, sino que se genera un mensaje *digest* que es el que se cifra). Todo el mundo que posea la clave pública de ese remitente podrá descifrar el *digest* y comprobar que procede de esa persona porque solo él, que es quien posee la clave privada, ha podido generar el mensaje.

Un ejemplo de este uso es el intercambio de claves SSH entre servidores.



4.6. Esquema de un sistema de autenticación mediante clave asimétrica.

Ejemplos

Intercambio de claves SSH entre servidores Debian

Queremos configurar un servidor de gestión de logs para que se conecte a otros servidores, recoja los ficheros de logs y los guarde en un repositorio centralizado para su análisis posterior. Se quiere que este proceso se realice de forma automatizada mediante *scripts* programados para ejecutarse a una determinada hora. Para ello, queremos habilitar un método seguro para que el servidor de logs pueda conectarse al resto sin necesidad de que haya un operador introduciendo las contraseñas en cada caso.

Los sistemas Linux suelen llevar instalado con la distribución el paquete openSSH, que permite realizar determinadas operaciones relacionadas con las claves privada y pública del servidor. Vamos a usar las utilidades de openSSH para realizar un intercambio de claves entre el servidor que va a recoger los logs (debian1) y el servidor donde se generan estos logs (debian2).

El primer paso es generar la pareja de claves SSH que identifican a debian1. Cada pareja de claves va asociada a un usuario del sistema operativo, por lo que deberemos generar las claves con el mismo usuario que van a utilizar los *scripts* para conectarse. Además, mediante openSSH podemos generar claves con el algoritmo RSA o DSA. Elegiremos DSA, mediante el parámetro —t, por ser más seguro:

```
debian1:~# ssh-keygen -t dsa
```

En el proceso nos pregunta dónde queremos guardar el par de claves (por defecto se guardarán en */root/.ssh/)*. También nos preguntará por una palabra de seguridad, pero en este caso deberemos dejarlo en blanco porque de lo contrario habrá que escribirla cada vez que queramos acceder al servidor destino. Comprobamos que nos ha creado correctamente el par de claves:

```
debian1:~# ls /root/.ssh/
id_dsa    id_dsa.pub
```

El primer fichero contiene la clave privada, el segundo la pública. Tendremos que incorporar el contenido de este segundo al fichero de claves autorizadas de debian2. Así, desde debian1, enviamos el fichero a debian2:

```
debian1:~# scp /root/.ssh/id_dsa.pub debian2:/tmp
```

En debian2, creamos su pareja de claves y añadimos el contenido del fichero de clave pública de debian1 al fichero de claves autorizadas:

```
debian2:~# ssh-keygen -t dsa
debian2:~# cat /tmp/id_dsa.pub >> /root/.ssh/authorized_keys
```

Si ahora nos logueamos en debian2 desde debian1, comprobaremos que ya no se nos pide contraseña:

```
debian1:~# ssh debian2
Linux debian2 2.6.26-2-686 #1 SMP Sun Mar 4 22:19:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jul 27 23:27:17 2012 from debian1.pruebas.es
debian2:~#
```

En cualquiera de los ficheros *id_dsa.pub* podrás ver el aspecto de una clave pública generada con DSA.

3.2 > Confidencialidad con claves asimétricas

Los sistemas de cifrado con claves asimétricas sirven para garantizar la confidencialidad del mensaje, al igual que la criptografía simétrica.

Cuando alguien quiera cifrar un mensaje dirigido a mí, utilizará mi clave pública (que es conocida) para cifrarlo, pero únicamente yo lo podré leer, ya que soy el único que posee la clave privada. Funcionaría de forma similar a un candado, cualquiera puede cerrarlo, pero solo quien tenga la llave de ese candado puede abrirlo.

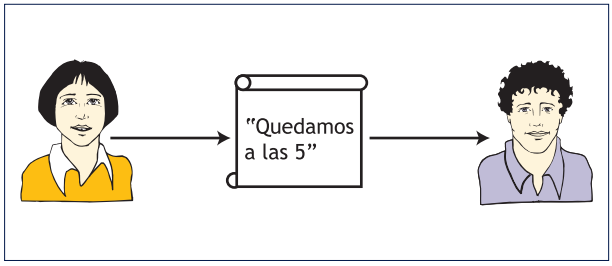
La clave pública tiene un valor, que es un número *(X)* que es el resultado de multiplicar dos números primos (*y*, *z*), que serían la clave privada. El valor de *X* es conocido, por lo que cualquiera que lo conozca puede cifrar un documento, pero solo quien conozca los valores de *z* e *y* podrá descifrarlo. Para que este método tenga éxito debe ser imposible hallar la clave privada a partir de la pública. ¿Cómo se consigue esto? Haciendo que los números primos utilizados sean muy grandes, lo que hará que el número *X* sea enorme, con lo que su factorización para poder averiguar la clave privada o el descubrimiento de esta, casualmente, sea una labor casi imposible. Por ejemplo, un valor de *X* aceptable para transacciones seguras es superior a 10^{300}.

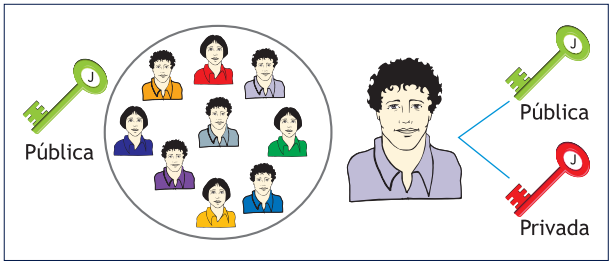
Ejemplos

Utilización de clave asimétrica

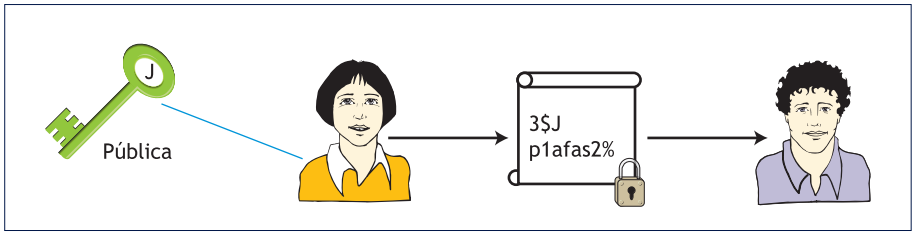
Vamos a ver el funcionamiento de la clave asimétrica a través de un ejemplo que muestra un proceso de comunicación segura entre dos usuarios.

Ana quiere enviar un mensaje secreto a Juan cifrándolo mediante una clave asimétrica. Juan dispone de una pareja de claves pública y privada y ha distribuido su clave pública de forma que cualquiera que quiera enviarle un mensaje pueda usarlo para cifrarlo.



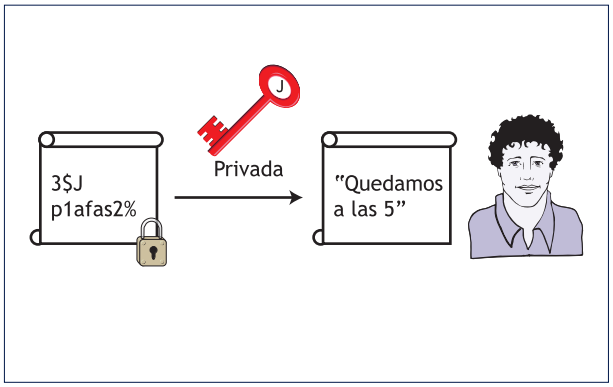


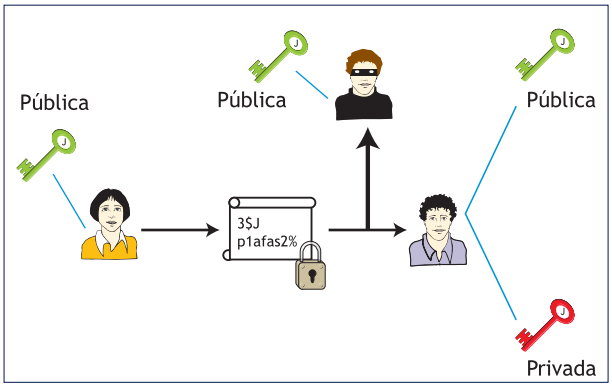
Como la clave pública de Juan es conocida, Ana la utilizará para cifrar el mensaje.



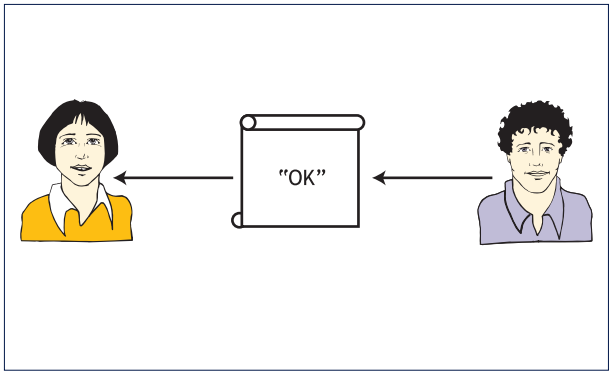
Una vez cifrado el mensaje con la clave pública, solo Juan podrá leerlo, porque él es la única persona que tiene su clave privada. Al estar cifrado con la clave pública, la privacidad del mensaje para Juan está garantizada, puesto que solo quien conozca la clave privada podrá descifrar el mensaje.

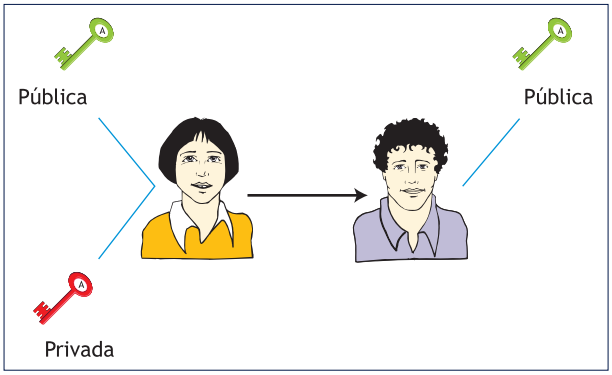
Por esto no hay ningún inconveniente para que la clave pública de Juan sea públicamente conocida, pues por sí misma no será suficiente para descifrar el mensaje. Lo realmente importante es que la clave privada esté a buen recaudo, pues si un intruso la averiguara, sí que podría acceder al contenido del mensaje.



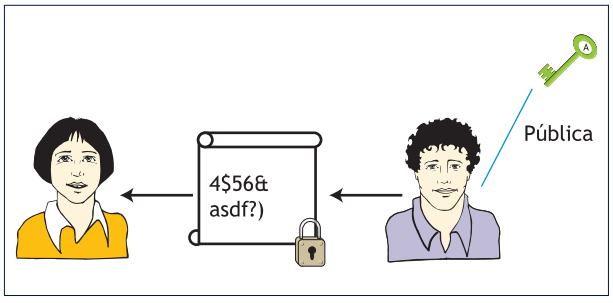


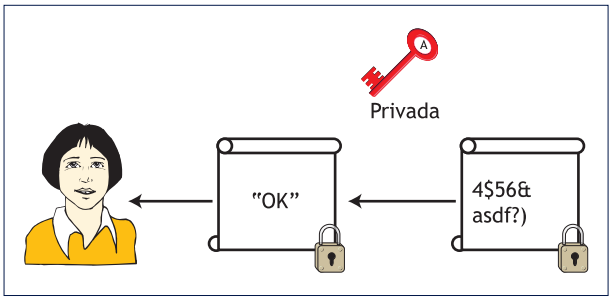
Ahora, supongamos que Juan quiere contestarle a Ana en secreto. Para cifrar el mensaje, Juan debe tener la clave pública de Ana. Por ello, Ana debe generar su propio par de claves pública/privada y enviar a Juan su clave pública.





Juan utiliza la clave pública de Ana para proteger el mensaje y solo Ana podrá leer el mensaje porque es la única persona que conoce la clave privada.





Ventajas e inconvenientes de los sistemas de cifrado asimétricos	
Ventajas	- La clave pública se distribuye libremente, por lo que ya no existe el problema del intercambio de la clave que había en los métodos simétricos. - Solo es necesario un par de claves por interlocutor, con independencia del número de estos, por lo que el espacio de claves es más manejable cuando los interlocutores son muchos.
Inconvenientes	- Requieren mayor tiempo de proceso que el cifrado simétrico. - Dan lugar a mensajes cifrados de mayor tamaño que los originales. - Para garantizar la seguridad, requieren claves de mayor tamaño que en el caso de los métodos simétricos. - Puesto que las claves públicas se distribuyen libremente, hace falta un esquema de confianza que garantice la autenticidad de las claves públicas (que la clave pública sea de quien dice que es, que no ha sido comprometida, etc.).

Infraestructuras de clave pública

Para que se genere un certificado personal (por ejemplo, el DNIe), es necesario ir en persona a una oficina para que el funcionario verifique nuestra identidad. Así se nos proporcionarán un par de claves asociadas a un certificado que dice que hemos sido correctamente identificados.

Un asunto importante es la autenticidad de las claves públicas, ¿quién nos garantiza que la clave pública del interlocutor es suya realmente?

Existen varios mecanismos para comprobar la autenticidad de las claves públicas, ya que es aquí donde radica la debilidad principal de estos sistemas:

– **Infraestructuras de clave pública (PKI):** utilizadas, por ejemplo, para verificar las claves públicas de los certificados del DNI electrónico y el resto de certificados generados por la Fábrica Nacional de Moneda y Timbre.
– **Listas de revocación de certificados**.

3.3 > Algoritmos de cifrado

Los algoritmos de cifrado asimétrico mas conocidos son los siguientes:

RSA *(Rivest-Shamir-Adelman)*

Fue creado en 1977 y es uno de los algoritmos más utilizados. Permite cifrar y firmar digitalmente, aunque es mucho más lento que DES y que otros sistemas de cifrado de clave simétrica. Es el sistema que desarrollamos en el apartado 3.2 y está basado en la factorización de números primos grandes.

DSA *(Digital Signature Algorithm)*

Algoritmo de firma digital, estándar del Gobierno Federal de Estados Unidos. Para entornos críticos, se ha demostrado que DSA es más seguro que RSA. Permite firmar digitalmente, sin embargo no permite cifrar la información. Una desventaja es que requiere más tiempo de cómputo que el algoritmo RSA.

ElGamal

Fue escrito por Taher ElGamal en 1984. Algoritmo de uso libre utilizado en software GNU Privacy Guard, en versiones recientes de PGP. Puede ser utilizado para cifrar y firmar digitalmente, con un tiempo de cómputo similar a RSA. Su nivel de seguridad está basado en la dificultad de calcular un logaritmo discreto.

Casos prácticos 1

Criptografía de clave asimétrica

•• Utilizando la aplicación de software libre Cryptophane para Windows, realiza las siguientes tareas:

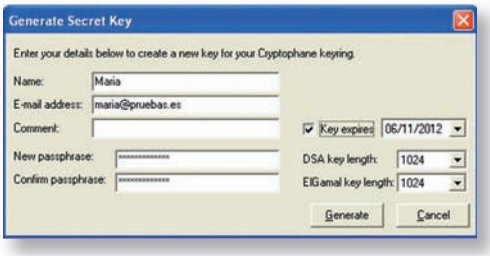
a) Genera un par de claves una para ti y otra para el destinatario de los mensajes, que será un compañero de clase.
b) Exporta e importa las claves públicas.
c) Crea un documento que deberás enviar a un compañero cifrado con la clave pública del destinatario.

Solución ••

a) Generación de pares de claves
Utiliza el menú *Keys /Generate Secret Key* para generar un par de claves. Te pedirá tu nombre, *email*, descripción y fecha de caducidad de la clave. Introduce la siguiente información:

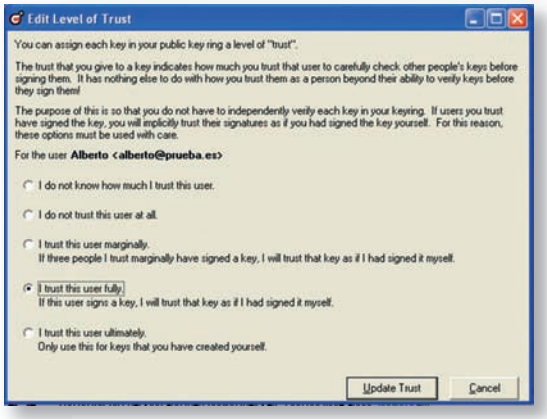
Caducidad de claves: un año.

Longitudes de clave: 1024 bits, que ya proporciona un nivel de seguridad elevado. A mayor longitud de clave, más seguridad, pero son necesarios más recursos para cifrar y descifrar.



En la ventana de la aplicación puedes ver la clave pública asociada a la clave privada que has creado. En la ventana principal, lo que se visualiza son todas las claves públicas de tus contactos. Para observar las propiedades de la clave, haz doble clic sobre una de ellas o bien haz clic con el botón secundario y selecciona *Key Properties*. A este repositorio de claves se le conoce como anillo de claves.

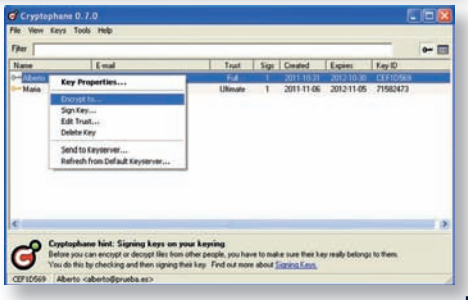
b) Exportación/Importación de claves públicas
Para exportar la clave pública debes ir al menú *File / Export Public Keys*. Exporta tu clave pública para pasársela a tu compañero. Tu compañero debe realizar la misma tarea y pasarte su clave pública a ti.



Para importar la clave pública de tu compañero debes ir al menú *File / Import Keys*.

Edita el nivel de confianza (*trust*) de la clave que has importado del compañero y, como te fías de ella, márcala como *I trust this user fully*. Con esta acción has dado el mayor nivel de confianza a la clave de tu compañero.

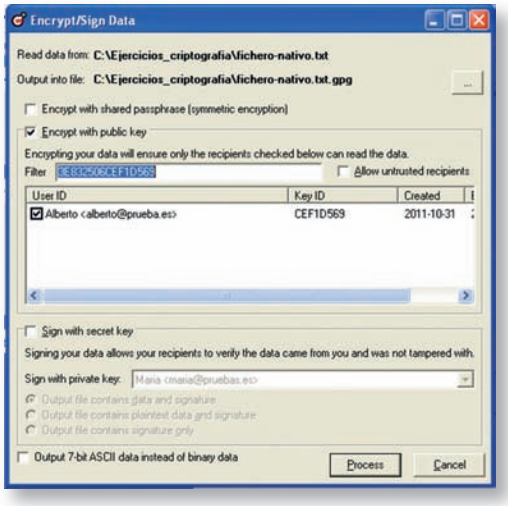
c) Cifrado de documentos
Crea en tu equipo un documento de texto (no hace falta que sea en .doc u .odt, con texto plano .txt es suficiente) llamado *Asimétrico.txt* y escribe un contenido para el compañero o compañera que va a recibir el documento cifrado.



Selecciona su clave, haz clic con el botón secundario y selecciona *Encrypt to...* En este momento estás cifrando el documento que enviarás a tu compañero usando su clave pública.

1

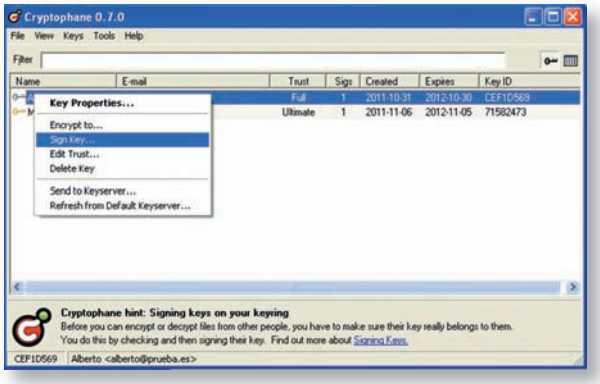
Selecciona el fichero que has escrito antes y marca en la casilla de verificación *Encrypt with public key* (cifrar con clave pública). Haz clic en *Process*. Puedes observar que la aplicación no te deja usar claves públicas de tu anillo hasta que firmes con tu clave privada.

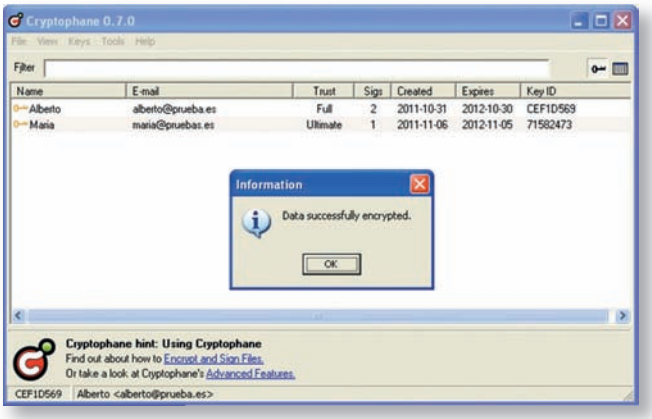


Verifica con el compañero a quien vas a enviar el mensaje su clave pública y fírmala utilizando tu clave privada. Para ello, utiliza el menú contextual que se abre al hacer clic con el botón secundario del ratón. Una vez firmada, el programa confía plenamente en esa clave pública.

Vuelve a intentar de nuevo cifrar el documento destinado a tu compañero y comprueba ahora que el programa ya te permite hacerlo. Envíale el documento cifrado al compañero y pídele que lo descifre con su clave privada. Haz lo mismo tú con el documento cifrado que él te pase.

Comprueba que se te pide la clave con la que has protegido tu clave privada para descifrar el documento.





Actividades propuestas

6·· ¿En qué consiste el cifrado de clave asimétrica? Cita algunos ejemplos, además de los indicados en el texto, de algoritmos de cifrado de este tipo.

4 >> Algoritmo de cifrado *hash*

Tan importante como la autenticación y la confidencialidad es la integridad de los mensajes. De nada sirve que el canal sea seguro si no es posible garantizar que el mensaje no ha sido alterado y se corresponde exactamente con el original.

Una función *hash* es un algoritmo que mapea un conjunto grande de datos de tamaño variable, llamados claves, en pequeños conjuntos de datos de longitud fija.

Los algoritmos *hash* resultan de vital importancia en la firma digital de documentos y mecanismos como el sobre digital. Garantizan la integridad dado que, con cambiar un solo bit del mensaje original, el resultado obtenido al aplicar la función *hash* será diferente.

Las propiedades más importantes de las funciones *hash* son:

- Independientemente del tamaño del mensaje original, al aplicarle la función *hash,* la huella resultante siempre tendrá el mismo tamaño.
- Con cambiar un único bit del mensaje original, la huella resultante será completamente distinta.
- **Resistencia a la preimagen:** si tenemos el resultado de aplicar una función *hash,* resulta computacionalmente imposible obtener el mensaje original a partir de este.
- **Resistencia a la segunda preimagen:** dado un mensaje *x*, no es posible encontrar otro mensaje *x'* que produzca el mismo valor *hash.*
- **Resistencia a colisiones:** no es posible encontrar dos entradas que den lugar al mismo valor *hash.*

Entre las aplicaciones de las funciones *hash* se destacan:

- Protección de contraseñas.
- Se utilizan como parte de algunos de los pasos de los algoritmos de cifrado simétrico y asimétrico vistos anteriormente.
- Es una parte fundamental del mecanismo de firma digital.
- Se emplea para garantizar la integridad de un flujo de datos, como por ejemplo el software que nos descargamos (es muy usado en sitios de software libre, en los que al lado del enlace al software suele encontrarse un enlace a la huella *hash* del archivo de forma que, antes de instalar, podamos comprobar que el software se ha descargado íntegramente y sin errores).

Como algoritmos *hash* destacados tenemos SHA, SHA-1, MD5 y RIPE-MD.

Sobre digital

El sobre digital es un mecanismo que garantiza las propiedades de confidencialidad de un documento. Utiliza criptografía simétrica y asimétrica.

Combinando los sobres digitales con las firmas digitales obtenemos un sobre digital firmado, garantizándose así las propiedades de integridad, confidencialidad y autenticación.

Encriptación de contraseñas

Una medida eficaz cuando trabajamos con sistemas de autentificación de usuarios mediante usuario y contraseña por Internet, por ejemplo, es encriptar las contraseñas con MD5, de forma que en caso de que alguien accediese a ellas solo pudiera ver su encriptación y no la contraseña.

Actividades propuestas

7·· Busca en Internet una web que permita cifrar *online* un texto usando el algoritmo MD5 (por ejemplo, la siguiente: http://www.cuwhois.com/herramienta-seo-genera-md5.php). Cifra el siguiente texto: "Buenos días, soy un alumno". ¿Cuál es el resultado de cifrar la cadena anterior?

8·· Realiza un breve resumen con las características más significativas de los algoritmos *hash* que se citan en el texto.

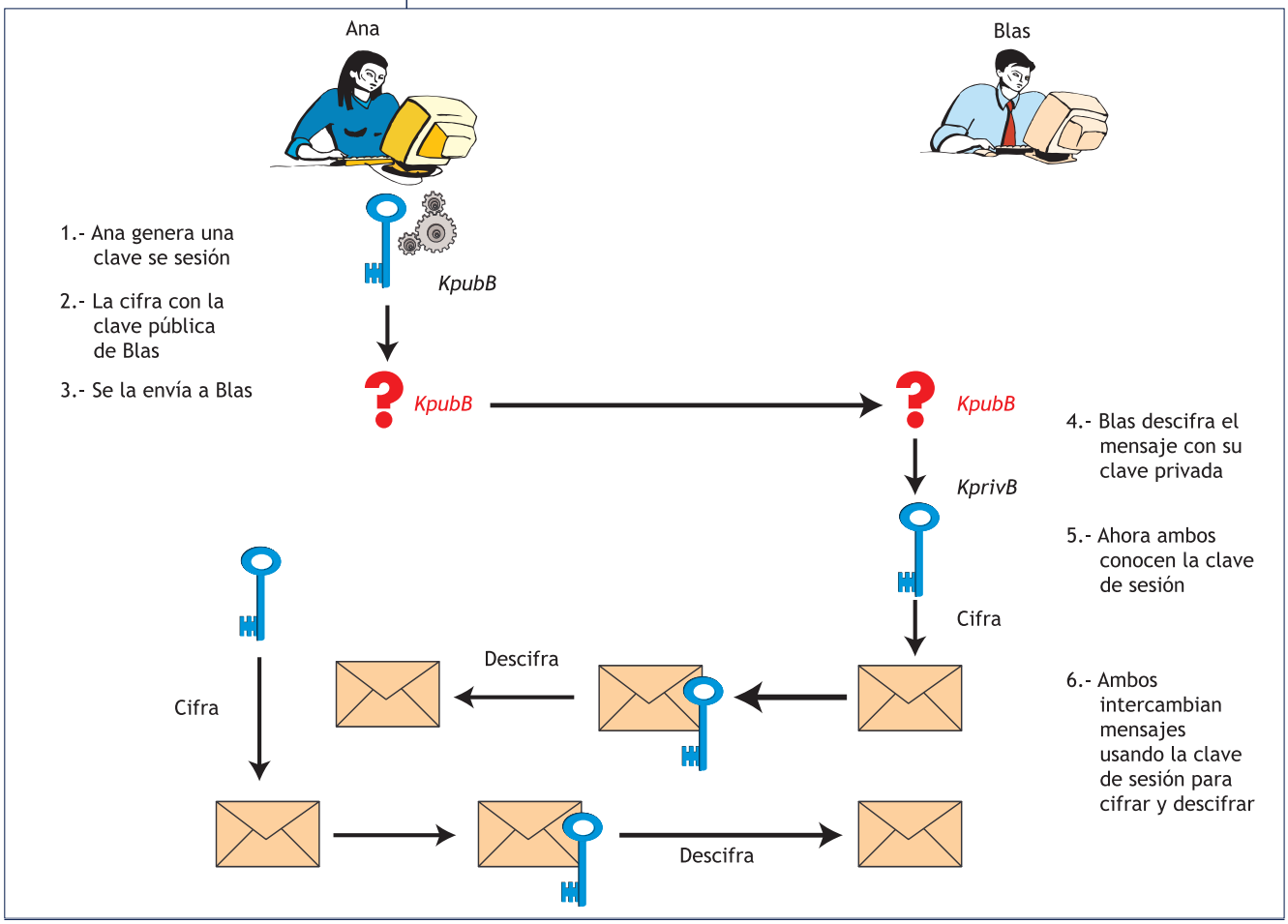
5 >> Sistemas híbridos

Como se ha visto en los apartados anteriores, tanto los sistemas simétricos como los asimétricos presentan ventajas e inconvenientes. Con los sistemas híbridos se pretende aprovechar la mayor eficiencia para cifrar y descifrar de los métodos simétricos solucionando al mismo tiempo el problema de la transmisión segura de la clave que presentan estos sistemas.

Para ello, cuando dos agentes quieren entablar una comunicación segura, en primer lugar establecen una conexión segura haciendo uso del sistema de clave pública.

A través de esta conexión securizada por métodos asimétricos, se intercambian una clave de tipo simétrico con la que realizarán el resto de la comunicación. De este modo, la penalización del rendimiento que supone el uso de claves asimétricas solo se da al inicio de la comunicación, cuando ambos agentes se ponen de acuerdo en la clave simétrica que van a usar.

Los criptosistemas híbridos tratan de aprovechar lo mejor de cada uno de los sistemas de cifrado de clave simétrica y asimétrica. Se trata de obtener un criptosistema rápido y eficiente que permita el intercambio de contraseñas en canales de comunicación inseguros.



4.7. Esquema de la transmisión de mensajes mediante sistemas de criptografía híbrida.

Los sistemas híbridos más importantes son: PGP, GnuPG y OpenPGP.

5.1 > PGP *(Pretty Good Privacy)*

Se trata de una herramienta sencilla, barata y potente desarrollada por Phil Zimmermann. Permite el cifrado de datos, archivos y mensajes mediante la utilización de codificación asimétrica junto con la simétrica. Su objetivo es proteger la información utilizando criptografía de clave pública y facilitar la autenticación de documentos mediante las firmas digitales.

Utiliza claves asimétricas que son almacenadas en el disco duro en ficheros llamados **llaveros**. Existe un llavero para las claves públicas utilizadas y otro para las claves privadas.

Sus aplicaciones más comunes son:

- Cifrado de ficheros, documentos y discos (PGPDisk).
- Firma digital y cifrado de correos electrónicos (PGPmail).
- Comunicaciones seguras (PGPNet).

El proceso de cifrado consiste en que la clave pública del receptor cifra la clave simétrica o clave de sesión con la que se cifra el mensaje a enviar. En el proceso de descifrado el receptor utiliza su clave privada para descifrar la clave de sesión secreta, la cual, a su vez, se utiliza para descifrar los datos comprimidos.

5.2 > OpenPGP

Su diseño está basado en la implementación PGP de Phil Zimmermann. El grupo IETF (*Internet Engineering Task Force*) creó el estándar de Internet OpenPGP basandose en el diseño de PGP. Se trata por tanto de un protocolo de encriptación de correo electrónico libre basado en criptografía de clave asimétrica.

Define formatos estándar para crear mensajes encriptados, firmas, certificados e intercambio de claves privadas. Actualmente, se considera el estándar a utilizar en la encriptación de correos electrónicos.

5.3 > GnuPG *(GNU Privacy Guard)*

Se trata de una herramienta de software libre y de código bajo licencia GPL utilizada para el cifrado y firmas digitales. Añade mejoras de seguridad y nuevas funcionalidades respecto a PGP.

Utiliza algoritmos no patentados, como son ElGamal, CAST5, TripleDES, AES y Blowfish. Se utiliza en algunos sistemas operativos, como FreeBSD, OpenBSD, GNU/Linux, Mac OS X o Windows, así como en algunos clientes de correo electrónico, como Kmail y en gestores de información personal, como Evolution.

Actividades propuestas

9·· ¿En qué se basan los criptosistemas híbridos?

10·· Indica algunas aplicaciones de los sistemas híbridos nombrados en el texto.

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿Qué es la criptografía y cuál es su finalidad? Explícalo con tus palabras.

2·· ¿De qué se compone un criptosistema?

3·· Indica en qué dos operaciones básicas se basan los sistemas criptográficos clásicos.

4·· ¿En qué consiste la transposición? Crea un mensaje utilizando dicha técnica.

5·· ¿En qué consiste la técnica de permutación o sustitución? Crea un mensaje usando dicha técnica.

6·· ¿Qué tipos de sistemas de cifrado se han visto en la unidad? Explica brevemente, utilizando tus propias palabras, en qué consiste cada uno de ellos.

7·· ¿Qué tipo de cifrado es el que se conoce como de clave secreta?

8·· ¿Qué desventaja crees que ofrece el método de cifrado simétrico?

9·· ¿Qué novedad aportan los sistemas de cifrado de clave asimétrica con respecto a los de clave simétrica?

10·· ¿Cuál de los dos sistemas de cifrado vistos es más rápido? ¿Por qué?

11·· ¿Qué garantizan los algoritmos de cifrado *hash*?

12·· Explica cómo se establece una comunicación entre dos interlocutores utilizando un sistema híbrido.

13·· ¿Qué ventajas ofrecen los sistemas híbridos?

.: APLICACIÓN :.

1·· Crea un mensaje utilizando la técnica de la transposición y, posteriormente, pásaselo a un compañero para que lo intente descrifrar.

2·· Cifra el mensaje "La máquina Enigma se usó en la segunda guerra mundial para cifrar mensajes" utilizando la técnica de la permutación o sustitución:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	J	M	L	O	N	A	Y	B	P	R	I	V	T	Z	W	Ñ	S	F	Q	U	G	D	E	H	C	K

3·· Te han encargado establecer un mecanismo de seguridad para proteger las contraseñas de una aplicación. Dicha aplicación almacena la información de los usuarios en una base de datos, concretamente en una tabla con los campos *Usuario* y *Contraseña*. Ahora mismo la contraseña se almacena tal y como la introduce el usuario. ¿Cómo podrías proteger los valores introducidos en el campo *Contraseña* para que un acceso a dicha tabla no descubra las contraseñas?

4·· Dados los siguientes mensajes cifrados con el sistema MD5:

a) 9be2d8141fb9aba6aaafb6ddf22c5ed4
b) 4d186321c1a7f0f354b297e8914ab240

¿Hay forma de saber la longitud del mensaje original? ¿Y de saber cuál fue el mensaje original?

5·· ¿Se pueden cifrar los mensajes de cuentas de correo como Gmail o Hotmail?

6·· ¿Es seguro indicar a los navegadores que recuerden las contraseñas cuando las utilicemos en páginas web, formularios, etc.? Elige un navegador y averigua dónde y cómo se almacenan las contraseñas.

Caso final 2

Protección en el correo electrónico

•• Gema y David son dos amigos que frecuentemente se envían mensajes relativos a sus respectivos negocios y les gustaría utilizar para sus comunicaciones un gestor de correo que permitiera cifrar sus comunicaciones mediante técnicas de cifrado asimétrico basadas en GnuPG. Hablan con una amiga común, Rosa, y les recomienda que utilicen el gestor de correo electrónico Thunderbird, por ser libre y muy sencillo de configurar y que añadan al mismo la extensión de seguridad Enigmail que permite cifrar correos electrónicos.

a) ¿Cómo instalarían Gema y David el software necesario?
b) ¿Cómo se llevaría a cabo el proceso de comunicación segura entre David y Gema?

Solución ••

a) El primer paso que deben llevar a cabo Gema y David será instalar el gestor de correo y el soporte para GnuPG en sus dos equipos.

El soporte GnuPG se puede encontrar en la web siguiente: ftp://ftp.gnupg.org/gcrypt/ Para instalar en Windows habrá que ir a la carpeta *binary*. La instalación es rápida y sencilla.

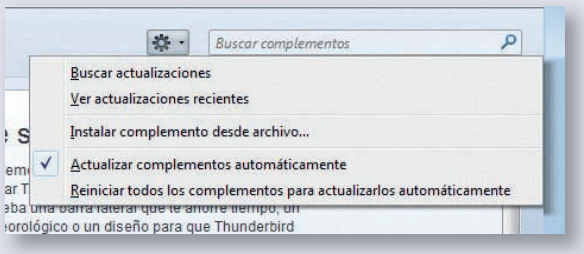
Una vez instalado el soporte GnuPG, deben descargar e instalar el gestor de correo Thunderbird, lo cual pueden hacer desde de la página web http://www.mozilla.org/es-ES/thunderbird/

Una vez instalado, deben configurarlo para que trabaje con una cuenta de correo real y comprobar que funciona la cuenta de correo enviando un mensaje a la misma y desde ella.

A continuación, deben instalar el gestor de correo Enigmail, que es una extensión de seguridad para Mozilla Thunderbird que permite escribir y recibir mensajes firmados y/o cifrados mediante el estandar GnuPG. Descargan la extensión Enigmail para Thunderbird desde la dirección: http://enigmail.mozdev.org/download/index.php.html.

Seleccionan el sistema operativo y la versión de Thunderbird instalada y, a continuación, desde la interfaz de Thunderbird seleccionan *Herramientas / Complementos (Tools - Addons)*.

Haciendo clic sobre el símbolo de configuración (esquina superior izquierda) aparece un menú en el que elegirán la opción *Instalar complemento desde archivo* y buscarán el archivo recientemente descargado, que contiene la extensión Enigmail. Aparecerá una ventana en la que se advierte que solo se instalen complementos de autores de confianza y se hace clic en el botón *Instalar ahora*.



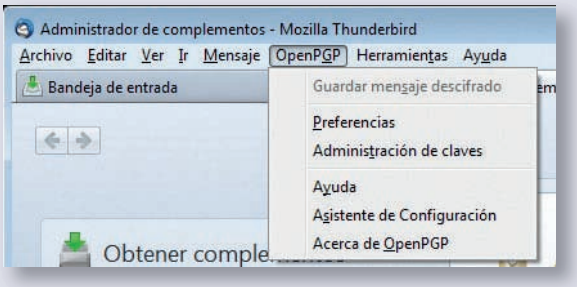
b) Una vez instalado el software necesario para llevar a cabo una comunicación segura, ya podrán enviar el mensaje cifrado. Para ello, si imaginamos que Gema va a enviar un mensaje a David, el proceso sería el siguiente:

- David debe crear un par de claves (una pública y otra privada).
- David debe pasarle su clave pública a Gema.
- Gema usará la clave pública de David para cifrar el mensaje.
- Cuando reciba el mensaje, David podrá descifrarlo con su clave privada.

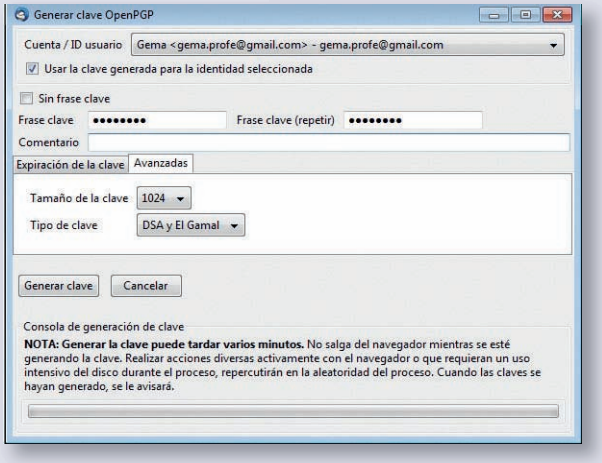
Para crear el par de claves, David selecciona en el menú de Thunderbird *OpenPGP-Administración de claves (OpenPGP-Key management)*.

2

Se muestra la ventana *Administrar claves OpenPGP*. En dicha ventana, selecciona la opción de menú *Generar / Nuevo par de claves*.

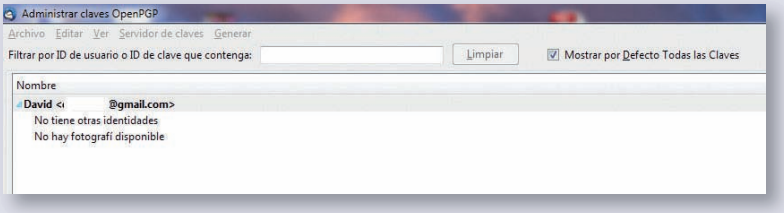


En la pestaña *Expiración de la clave*, selecciona *1 año*. A continuación, en la pestaña *Avanzadas* elige como tamaño de clave *1024 bits* y como tipo de clave *DSA*. Se pide además que se introduzca una "frase" (en realidad se trata de la clave). Esta frase o clave servirá para proteger la clave privada generada y deberá tener una longitud adecuada (8 caracteres o más), que incluya números, letras y caracteres especiales. Además se recomienda que no sea una palabra que exista en el diccionario ni una cadena de caracteres previsible (por ejemplo, "1234" no será una buena elección como frase). Una vez elegida la frase, selecciona el botón *Generar clave*.



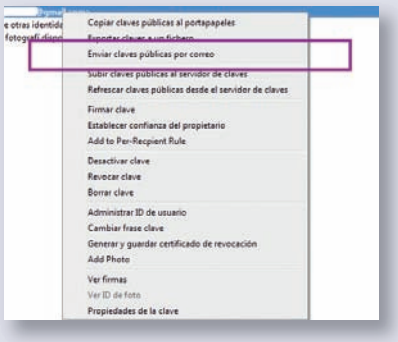
Una vez creados el par de claves, se indicará que es recomendable crear un certificado de revocación para esta clave. Por tanto, selecciona *Generar certificado*.

Si todo ha funcionado bien, en la ventana principal aparecen las claves creadas (*Administrar claves OpenPGP*). Si no es así, marca la opción *Mostrar por defecto todas las claves*.



Una vez que ha generado las claves, David deberá exportar su clave pública y pasársela a Gema, quien le enviará un correo cifrado. David podrá enviarle la clave pública por correo electrónico, colgarla en un servidor de claves, etc.

Si desea enviarla por correo electrónico bastará con que la adjunte a un mensaje mediante el botón *OpenPGP*. Para ello, irá a la ventana de *Administración de las claves OpenPGP* y, sobre su ID de usuario, hará clic con el botón secundario del ratón y seleccionará *Enviar claves públicas por correo*.

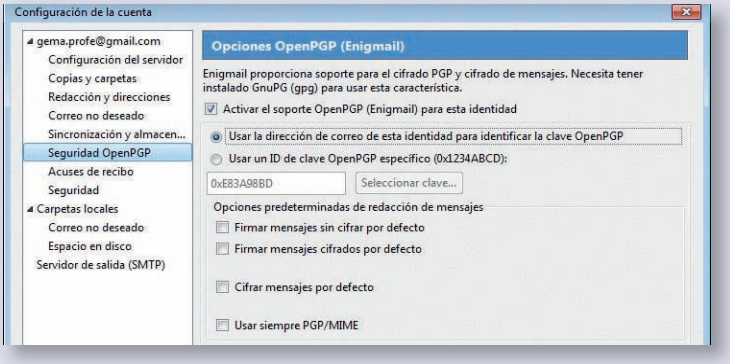


2

A continuación, escribirá el cuerpo de mensaje de correo y seleccionará *Enviar*. Tras hacer clic en este botón, la aplicación le pedirá que inserte la frase o clave. Una vez insertada y tras hacer clic en *Aceptar,* el mensaje de correo electrónico se enviará con la clave pública.

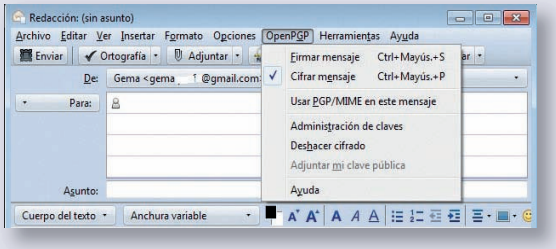
Para que Gema pueda enviarle un mensaje cifrado a David, tendrá que escribirlo y cifrarlo utilizando la clave pública de David, pero antes deberá importar la clave pública de este.

Antes de que Gema cree el correo para enviar a David, es conveniente que seleccione *Herramientas / Configuración de la cuenta* y, en el panel lateral, marque la opción *Seguridad OpenPGP*. En el panel de la derecha, marcará la casilla *Activar el soporte OpenPGP (Enigmail)* para esta identidad, si es que ya no lo estaba antes, y seleccionará la opción *Usar la dirección de correo de esta identidad para identificar la clave OpenPGP.*

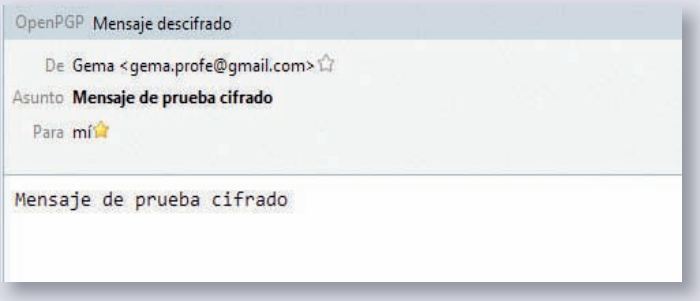


El proceso de importación de la clave de David lo realizará seleccionando *Administrar claves* y seleccionando *Archivo / Importar la clave desde un fichero* que le ha enviado David.

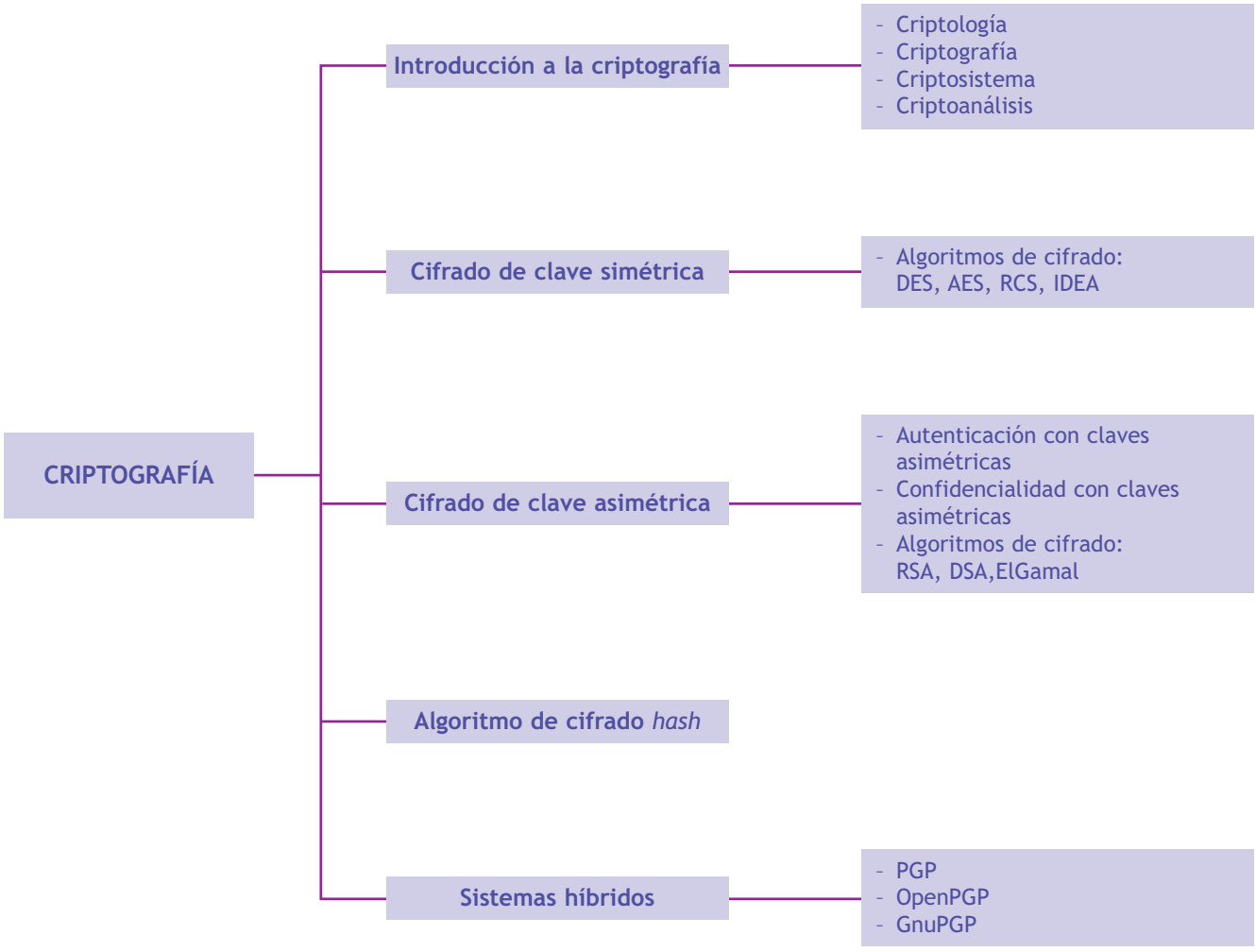
Ahora ya podrá crear y cifrar un correo electrónico mediante GnuPG. Para ello deberá ir a *Redactar* para seleccionar el destinatario y escribir el nuevo correo. Ahora aparece una nueva opción: *GnuPG*. Deberá seleccionar esta opción marcando que desea cifrar el mensaje y ya solo le faltará agregar el *Destinatario* y un *Asunto* y podrá enviarlo.



Cuando David reciba el mensaje cifrado y lo intente abrir, le aparecerá una ventana solicitando la inserción de la clave privada (la frase o clave de paso OpenPGP). Si David no introduce la clave privada, el *mail* se verá sin descifrar, como muestra la imagen de la izquierda; en cambio, al insertar la clave, el mensaje se puede leer ya descifrado, como se ve a la derecha.



Ideas clave


CRIPTOGRAFÍA
Introducción a la criptografía
- Criptología
- Criptografía
- Criptosistema
- Criptoanálisis
Cifrado de clave simétrica
- Algoritmos de cifrado: DES, AES, RCS, IDEA
Cifrado de clave asimétrica
- Autenticación con claves asimétricas
- Confidencialidad con claves asimétricas
- Algoritmos de cifrado: RSA, DSA,ElGamal
Algoritmo de cifrado hash
Sistemas híbridos
- PGP
- OpenPGP
- GnuPGP

El cifrado AES, ¿está roto o no?

Un equipo de investigadores ha encontrado la primera vulnerabilidad en el estándar de cifrado AES reduciendo la longitud efectiva de la clave en 2 bits. Esto implica que las longitudes habituales de 128, 192 y 256 bits se han visto reducidas a 126, 190 y 254 bits. ¿Significa que está roto?

AES *(Advanced Encryption Standard)* es en realidad el algoritmo Rijndael, que pasó a ser un estándar de cifrado aprobado por el gobierno de los Estados Unidos en 2003 para cifrar información clasificada. Su versión de 128 bits está permitido para información secreta mientras que para información *top secret* requiere claves de 192 o 256 bits. De hecho, fue el primer algoritmo público usado para cifrar información *top secret* gubernamental.

Andrey Bodgdanov de la Universidad Católica de Leuven, Christian Rechberger del ENS de París y Dmitry Khovratovich del departamento de investigación de Microsoft ya apuntan que el ataque no tiene una gran relevancia práctica. Aunque el descubrimiento es considerado un avance importante en la investigación de la seguridad del algoritmo AES, puesto que la experiencia dice que en ciertos algoritmos se avanza despacio hasta romperlos. Esta vulnerabilidad ha sido confirmada por los desarrolladores de AES, Joan Daemen y Vincent Rijmen.

Los investigadores emplearon un ataque *meet-in-the-middle,* una aproximación que ha sido principalmente empleada con algoritmos de *hashing*, combinándolo con un ataque *biclique.* Este método ha permitido a los investigadores calcular la clave de un par texto plano/texto cifrado más rápidamente que empleando un ataque de fuerza bruta en el espacio total de la llave. O sea, se ha reducido el número de claves que deben ser probadas. La fuerza bruta total con clave de 128 bits serían 2^{128} posibilidades. Con este ataque serían necesarias solo 2^{126}.

En el sentido estrictamente académico, en algoritmo está roto puesto que se ha reducido (aunque sea en 2 bits) el espacio de claves necesario para calcular la clave por fuerza bruta. Sin embargo, roto no significa que no pueda ser usado con seguridad todavía. Por ejemplo, un ataque contra una llave de 128 bits requiere diez millones de años empleando un parque de un billón de equipos probando cada

uno de ellos un billón de claves. Al reducir en dos bits dicha clave, el tiempo se reduciría a 3 millones de años.

Hasta 2005, el único ataque que se conocía contra AES contemplaba una reducción del número de rondas de cifrado, o sea, una modificación artificial en su implementación que no suele encontrarse habitualmente. Los detalles del ataque fueron presentados en la conferencia CRYPTO 2011 y pueden ser descargados desde la web de investigación de Microsoft.

Fuente: Borja Luaces y Sergio de los Santos. 24/04/2011. http://unaaldia.hispasec.com.

Actividades

1·· El algoritmo de cifrado AES, ¿se utiliza en criptosistemas de clave simétrica o asimétrica?

2·· ¿Qué longitudes de clave se utilizan para cifrar información secreta? ¿Y para cifrar información de tipo *top secret*?

3·· ¿Por qué se considera que el algoritmo está roto?

4·· A partir de la información del texto, ¿consideras que hay que dejar de utilizar este algoritmo de cifrado?

unidad 5

Aplicaciones de la criptografía

SUMARIO

- Firma digital
- Certificados digitales
- DNIe
- SSL y TLS
- Cifrado de archivos

OBJETIVOS

- Aprender qué es la firma digital y qué aplicaciones tiene.
- Conocer qué son los certificados digitales.
- Describir las funciones del DNI electrónico y conocer los mecanismos de seguridad que tiene.
- Estudiar los protocolos SSL y TLS para las conexiones seguras.
- Aprender a cifrar archivos y unidades de almacenamiento.

1 >> Aplicaciones prácticas de la criptografía

En la unidad anterior introdujimos los conceptos básicos de la criptografía y adelantamos su utilidad práctica como medida de seguridad en el almacenamiento, transporte y transmisión de datos. En esta unidad, mostraremos las aplicaciones cotidianas de la criptografía. En efecto, diariamente y casi sin darnos cuenta, utilizamos la criptografía en muchas de las gestiones que realizamos.

Desde marzo de 2006 se expide en España el DNI electrónico (DNIe), un documento que contiene un chip que almacena nuestra información y es capaz de identificarnos ante la Administración o cualquier entidad sin que otra persona pueda suplantar nuestra identidad. ¿Cómo es esto posible? Gracias a la criptografía. Como estudiaremos en esta unidad, el DNI electrónico posee mecanismos de protección que hacen que sea prácticamente imposible de falsificar, con lo que podemos estar convencidos de que la persona que utiliza el DNI es quien dice ser.

En una red potencialmente insegura como Internet, es crítico asegurarnos de la identidad de una persona o de que la información o aplicaciones a las que accedemos no hayan sido modificadas por terceros.

Pensemos por un momento que vamos a descargamos un antivirus para nuestro equipo o para nuestro teléfono móvil. En una red como Internet cualquiera puede crear una página web para que otros usuarios puedan descargarse sus archivos y aplicaciones. ¿Estamos seguros de que el archivo que nos descargamos es realmente la aplicación que estamos buscando? ¿Estamos seguros de que ese programa no ha sido modificado para darle el control de nuestra máquina a un atacante?

Imaginemos ahora que estamos navegando por la página web del fabricante de un producto y que vamos a descargarnos una aplicación directamente desde allí. ¿Estamos seguros de que un atacante no ha modificado la página web para que los servidores contengan una versión falsa de la aplicación?

Ante este tipo de situaciones es necesario, por tanto, establecer mecanismos que garanticen la confidencialidad de las comunicaciones, la identidad de otros usuarios en determinadas situaciones y que la información no ha sido modificada por terceras personas. En esta unidad estudiaremos la aplicación práctica de la criptografía y veremos cómo la firma digital y los certificados digitales permiten evitar que alguien se haga pasar por otra persona mediante técnicas criptográficas, cómo el DNI electrónico utiliza la criptografía para identificarnos y evitar que suplanten nuestra identidad, cómo establecer conexiones seguras a través de redes inseguras o cómo proteger archivos mediante herramientas de cifrado.

Actividades propuestas

1·· ¿Has solicitado ya algún certificado digital o posees el DNI electrónico? Si es así, ¿lo has empleado para realizar algún trámite o gestión ante la Administración?

2 >> Firma digital

En la unidad anterior vimos que, mediante técnicas criptográficas, pueden garantizarse tres propiedades vitales para la seguridad: **confidencialidad** (cifrado simétrico y asimétrico), **autenticación** (cifrado asimétrico) e **integridad** (funciones *hash*).

En el caso de la firma digital, se trata de resolver el problema de la autenticidad del mensaje, es decir, que el mensaje recibido es exactamente igual al original (integridad) y que además proviene de quien dice venir (autenticación de origen). A esto hay que añadir también la necesidad de garantizar el no repudio, es decir, que el emisor no pueda negar haber sido él quien generó el mensaje.

Hemos visto que dos personas pueden enviarse mensajes de forma segura utilizando criptosistemas de clave asimétrica, de modo que nadie pueda descifrar la información enviada y recibida, pero ¿qué pasa si otra persona envía un mensaje en nombre de uno de ellos? Los mecanismos de cifrado por sí mismos no son capaces de garantizar la autenticidad, por lo que se han tenido que desarrollar otros métodos.

La solución es la utilización de la **firma digital**, también denominada **firma electrónica**. La firma digital es un conjunto de datos que se añaden a un mensaje original y que permiten asegurar la identidad de la persona que ha firmado el mensaje, así como que el contenido de este no ha sido modificado por terceras personas.

2.1 > Firma digital con árbitro

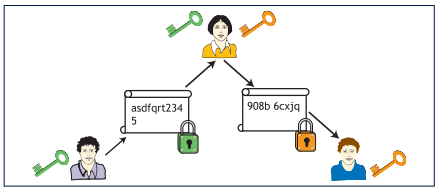
La firma digital con árbitro se utiliza en sistemas de clave simétrica, en los que se usa la misma clave para cifrar y descifrar los mensajes. Este mecanismo hace que dos usuarios que no confían entre ellos elijan a un tercer usuario, que cuenta con la confianza de ambos, y le otorguen el papel de intermediario en la transacción de datos.

El funcionamiento de este sistema se basa en que el árbitro conoce las claves de los otros dos usuarios. Este árbitro recibe el mensaje del emisor y lo descifra utilizando la clave de este. A continuación cifra el mensaje con la clave del receptor y se lo envía al mismo.

Ejemplos

Utilización de un árbitro para la firma digital

Juan y Pablo no se conocen y, por tanto, no confían entre ellos, pero deben intercambiar mensajes a causa de su relación comercial. En este caso, la solución es confiar en un tercer usuario de confianza mutua, llamado árbitro. Juan y Pablo solo enviarán y recibirán mensajes del árbitro.



Para que la comunicación sea segura, se utilizarán dos claves simétricas diferentes: el árbitro recibe los mensajes enviados por Juan codificados con su clave simétrica y los descifra. A continuación vuelve a codificar los datos pero esta vez con la clave de Pablo para posteriormente enviárselos.

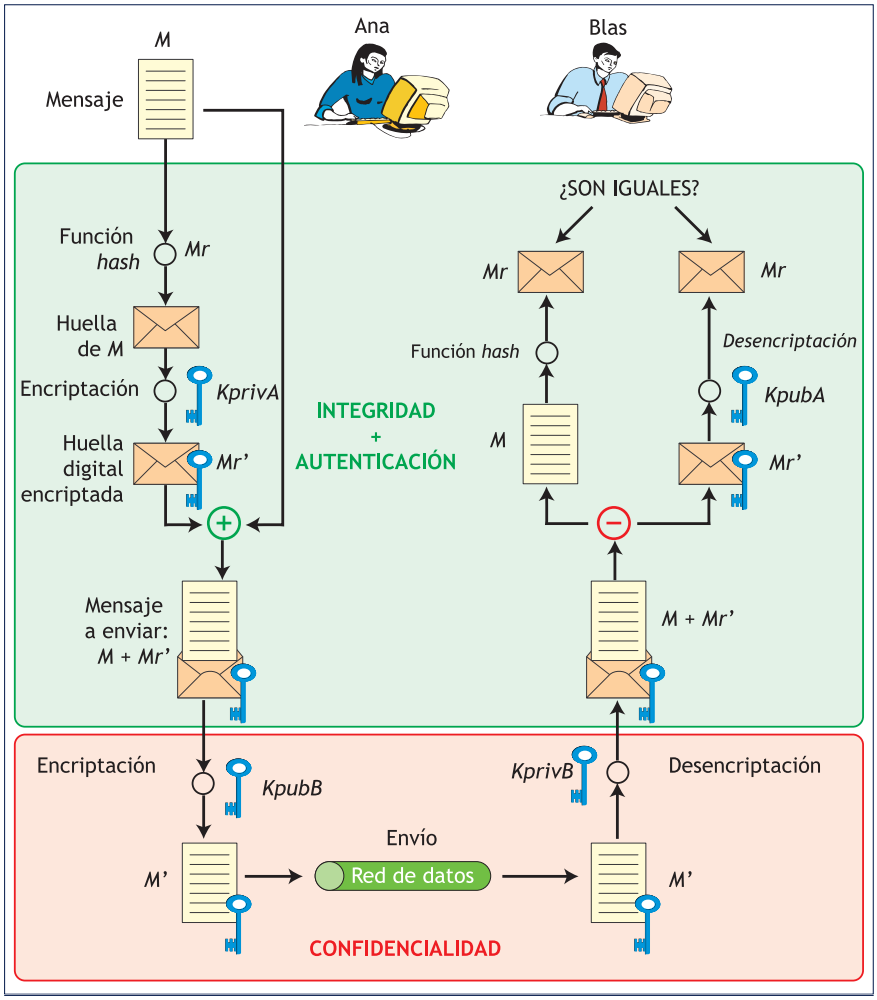
2.2 > Firma digital ordinaria

Actualmente, todos los métodos de firma emplean lo que se denomina firma digital ordinaria, que se basa en el uso de funciones *hash* y cifrado de clave pública. En este caso, no se utiliza un tercero de confianza (algo que presentaba bastantes problemas en un entorno distribuido tan heterogéneo como Internet), sino que el mecanismo garantiza la autenticidad en el envío desde el emisor al receptor de forma directa.

La función *hash* garantiza la integridad, el par de claves asimétricas del emisor garantizan la autenticación en origen y, si además se cifra usando la clave pública del receptor, también habría confidencialidad.

El proceso de firmado digital de un documento comienza cuando el emisor aplica una función *hash* al documento a firmar obteniendo un resumen del mensaje. A continuación, cifra el resultado anterior con su propia clave privada, obteniendo la firma digital del documento. Finalmente, adjunta la firma digital al documento a enviar. Si los datos se han cambiado, se obtendrá un resumen diferente.

El siguiente esquema ilustra el proceso:



5.1. Funcionamiento del proceso de firma digital.

¿Cómo se comprueba que la firma del mensaje es correcta?

El destinatario recibe el documento junto con el resumen, que ha sido encriptado con la clave privada del emisor, y aplica la función *hash* a los datos del documento, obteniendo un resumen del mensaje recibido. A continuación utiliza la clave pública del emisor para descifrar la firma y, de este modo, obtiene un resumen del mensaje original.

Si los dos resúmenes coinciden, la firma es válida, con lo que se puede asegurar que el mensaje procede de quien dice ser y además que no ha sido modificado. Si alguien ha modificado los datos o falsificado la firma, ambos resúmenes no coincidirán, con lo que el destinatario podrá advertir la manipulación.

2.3 > Clases de firma digital

La generalización del uso de las nuevas tecnologías como herramienta para poder transmitir información de forma rápida y segura ha posibilitado a la Administración la utilización de una nueva vía de comunicación con los ciudadanos. Cada día se pueden realizar más trámites y gestiones por Internet, gracias al uso de sistemas como el DNI electrónico y la firma electrónica.

La normativa básica que regula la administración electrónica es la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Asimismo, la firma electrónica está regulada por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Precisamente, la Ley 59/2003 distingue, a nivel legal, tres tipos de firma electrónica:

- **Firma electrónica:** es el conjunto de datos en forma electrónica que pueden ser utilizados como medio de identificación del firmante. Por ejemplo, sería cifrar un mensaje con nuestra clave privada.
- **Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- **Firma electrónica reconocida:** es avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Por ejemplo, es la firma mediante el DNIe. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

En ocasiones, además, es importante que en la firma esté consignado también el momento exacto en que se ha producido. Esto es necesario, por ejemplo, en trámites con la Administración o facturas electrónicas. Para ello, se hace uso de un mecanismo adicional denominado **sellado de tiempo** (*timestamping*), en el que un tercero llamado **autoridad de sellado de tiempo** certifica mediante su firma que la firma del usuario se ha producido en ese instante concreto de tiempo.

Casos prácticos 1

Firma digital

•• Utilizando la aplicación de software libre Cryptophane para Windows, realiza las siguientes tareas:

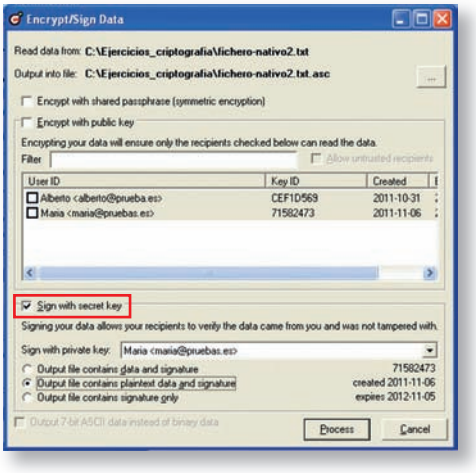
a) Firma digitalmente un documento de texto.
b) Cifra un documento con la clave pública del destinatario y fírmalo con tu clave privada.

Solución ••

a) Firma digital de un documento de texto

Comienza creando un documento de texto, dale un nombre y escribe contenido en él. En este caso, lo hemos llamado *fichero-nativo2.txt*. A continuación vas a firmar digitalmente el fichero, no a cifrarlo; con ello, lo que pretendes es que se pueda comprobar que has sido tú el autor del fichero, pero que el contenido de dicho fichero se pueda leer.

Una vez que has guardado y cerrado el documento de texto haz clic sobre él con el botón secundario del ratón y, en el menú contextual que te aparece, selecciona la opción, *Encrypt and/or Sign*. Se abre una nueva ventana, que ya vimos en la unidad anterior al cifrar los mensajes. Para firmar el mensaje sin cifrarlo, deberás marcar la casilla de verificación de firma (*Sign with secret key*), pero deberás desmarcar la casilla de encriptado (*Encrypt with Public Key*).



Si ahora abres el fichero con el Bloc de notas, podrás comprobar que no está cifrado, tan solo se le ha adjuntado tu firma digital para demostrar que tú eres el autor. Ya puedes enviarlo a quien quieras y esa persona sabrá que el archivo proviene de ti, pues contiene tu firma digital.

b) Firmar y cifrar documentos

Ahora crea otro fichero y escribe en él lo que quieras. En este segundo caso, cuando envíes a alguien ese archivo, lo que querrás es que su contenido quede cifrado y que, además, se pueda acreditar que tú eres el autor de dicho documento.

Para ello, debes firmarlo con tu clave privada como en el supuesto anterior y, además, cifrarlo con la clave pública del destinatario. Por tanto, deberás marcar tanto la casilla de verificación de firma (*Sign with secret key*), como la casilla de encriptado (*Encrypt with public key*).

Asegúrate de que el fichero firmado se guarda en texto plano para que pueda verse con un editor de texto (*Output file contains plainted data and signature*). Ya puedes enviarlo; cuando otra persona lo reciba, podrá desencriptarlo con Cryptophane a través de la opción *File* / *Decrypt* o la combinación de teclas <Ctrl> + <D>.

Actividades propuestas

2•• ¿Qué garantiza el uso de técnicas criptográficas?

3•• Busca información en Internet sobre, al menos, dos situaciones en las que puedas utilizar la firma digital basada en clave pública y ponlas en común con tus compañeros en clase.

3 >> Certificados digitales

Para solucionar el problema de la autenticación en las transacciones por Internet se buscó algún sistema identificativo único de una entidad o persona. Ya existían los sistemas criptográficos de clave simétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, solo conocida por el propietario.

El problema era asegurar que, efectivamente, la clave pública que se recibía era de la persona correcta y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin lugar a dudas a su emisor.

La solución a este problema vino con la aparición de los certificados digitales o certificados electrónicos, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales.

La misión principal de un certificado digital es garantizar, con toda confianza, el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

3.1 > Concepto y características

El certificado digital, certificado de clave pública o certificado de usuario, es un documento electrónico, identificado por un número de serie único y con un periodo de validez incluido en el propio certificado, que contiene varios datos. Está emitido por una entidad de confianza, denominada **autoridad de certificación** y vincula a su propietario con una **clave pública**.

Certificado digital reconocido

Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que compruebe la identidad y demás circunstancias de los solicitantes y la fiabilidad y las garantías de los servicios de certificación que presten.

Un certificado emitido por una autoridad certificadora, además de estar firmado digitalmente por esta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

Como el certificado está firmado por la autoridad de certificación, se garantiza que el mensaje no ha sido modificado (la firma garantiza la integridad del mensaje), que la clave pública pertenece al usuario con el identificador indicado y que el certificado es accesible para todos (para poder leer el certificado es necesaria la clave pública de la autoridad de certificación, que se pone a disposición de todo el mundo).

Para comprobar la autenticidad de un certificado, hay que tener instalado en el equipo el certificado raíz de la autoridad certificadora, mientras que su vigencia puede comprobarse consultando el propio certificado y acudiendo a la autoridad certificadora para cerciorarse de que el certificado no ha sido revocado.

Existen varios tipos de certificados, pero los más usados se rigen por el estándar UIT-T X.509. Su estructura es la siguiente:

– **Certificado:**
  - Versión.
  - Número de serie.
  - ID del algoritmo.
  - Organismo emisor.
  - Periodo de validez.
  - Información de la clave pública del usuario.
  - Otros campos opcionales (ID del emisor, ID del usuario, etc.).
– **Algoritmo** usado para firmar el certificado.
– **Firma digital** del certificado.

Los certificados no se emiten con carácter indefinido, sino que, como se ha indicado mas arriba, deben expresar su fecha de expiración, pasada la cual dejarán de tener validez. El periodo de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos, este periodo no podrá ser superior a cuatro años.

No obstante esto, un certificado puede ser renovado antes de que expire su periodo de validez.

También es posible revocar un certificado. Revocar un certificado significa privarle de validez antes de que finalice el periodo incluido en el propio certificado. Un certificado puede ser revocado por los siguientes motivos:

– Los datos que contiene han dejado de ser válidos.
– La clave privada ha sido comprometida o ha llegado a conocimiento de terceras personas.
– El certificado ha dejado de tener validez dentro del contexto para el que ha sido emitido.

3.2 > Autoridades de certificación

Una autoridad de certificación (AC o CA por sus siglas en inglés *Certification Authority*) es una entidad a la que uno o más usuarios confían la creación, asignación y revocación de los certificados digitales. Su misión es asegurar que un certificado es válido, está vigente y corresponde al usuario poseedor del mismo. Por tanto, permiten garantizar la autenticidad y veracidad de los datos que aparecen en los certificados digitales.

En resumen, las autoridades de certificación son responsables de la emisión y administración de los certificados y del mantenimiento de las listas de revocación de certificados.

Algunas autoridades certificadoras son:

– A nivel español: CERES, desarrollada por la Fábrica Nacional de Moneda y Timbre (FNMT); la Dirección General de la Policía (para la obtención del DNIe); la Autoridad de Certificación de la Abogacía (ACA), etc.
– A nivel internacional: Verisign, GlobalSign, Thawte Certification, GoDaddy, Comodo, etc.

Utilidad de los certificados digitales

Los certificados digitales se usan para:

- Identificación del interlocutor.
- Cifrado de datos digitales.
- Firma digital de datos (documentos, software, etc.).
- Seguridad de las comunicaciones.
- Garantía de no repudio (no es posible negar que cierta transacción tuvo lugar).

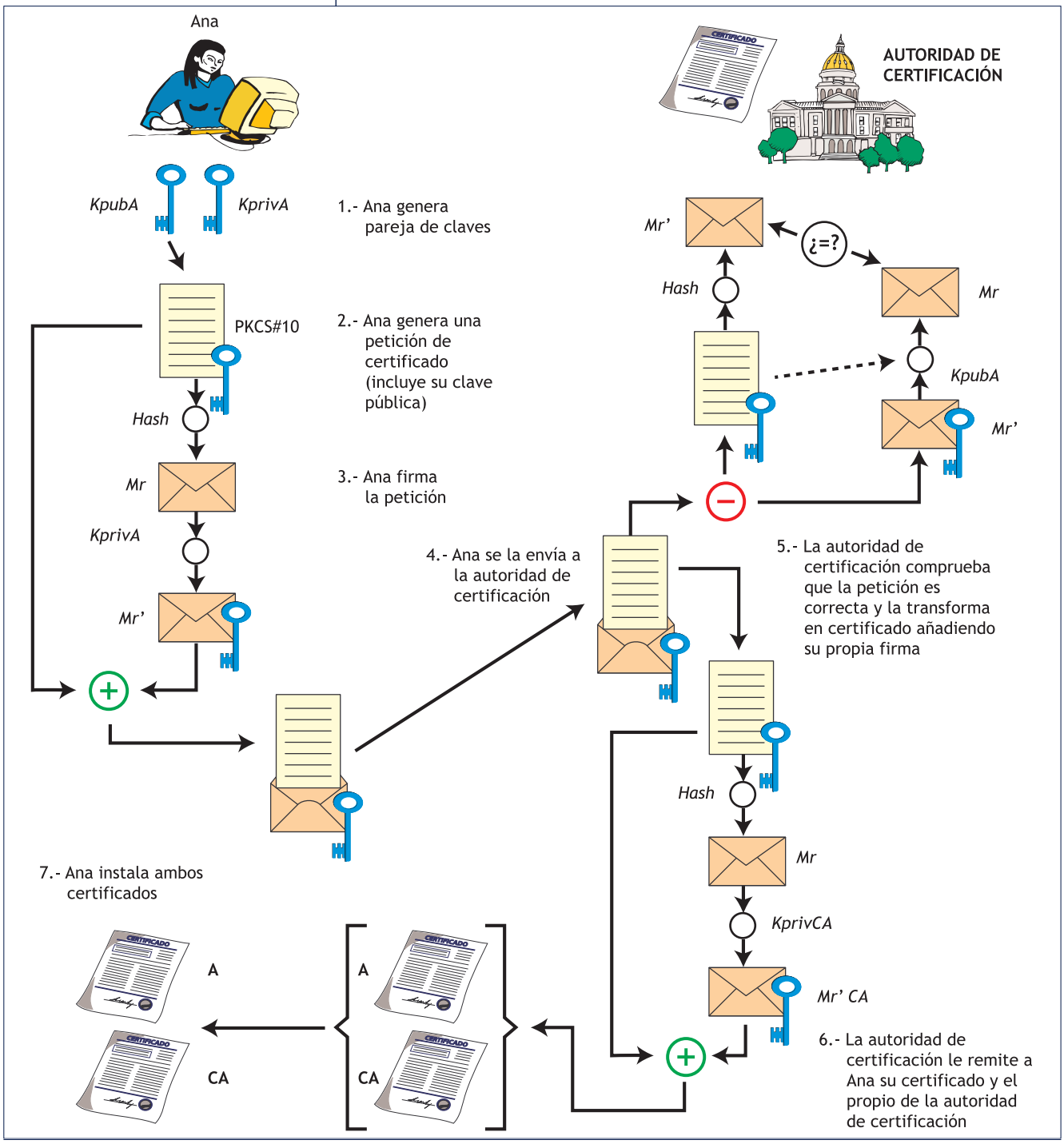
5.2. Conexión segura en Mozilla Firefox.

Autoridades de certificación privadas

Cualquiera puede crear una agencia certificadora y hacerse responsable de los certificados que emite. Por ejemplo, una empresa que quiera que todos sus trabajadores accedan a la aplicación de nóminas mediante un certificado podría generar sus propios certificados para que sus empleados los usen únicamente en el ámbito de la organización.

3.3 > Solicitud de certificados

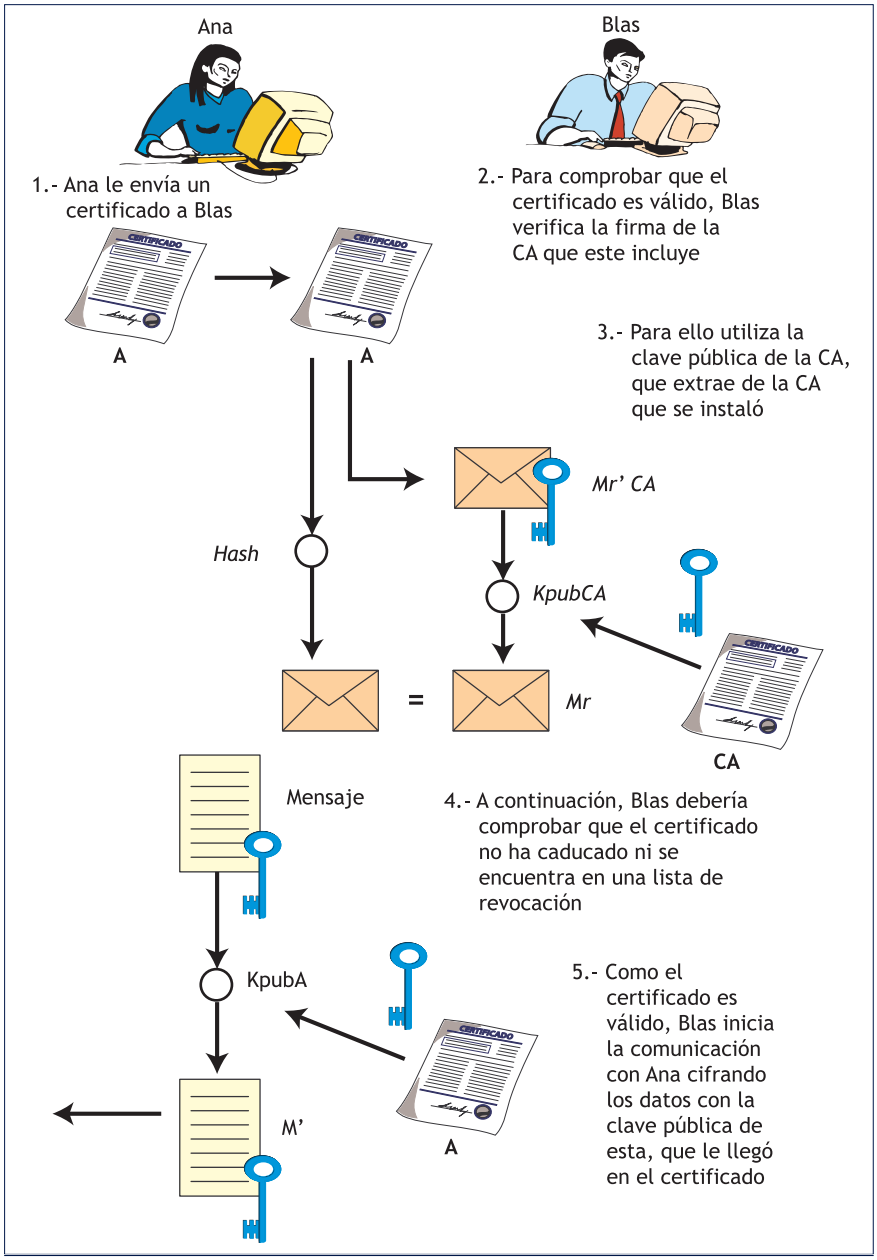
Cuando alguien quiere solicitar un certificado debe, en primer lugar, envíar sus datos a la autoridad de certificación, que verifica la identidad del solicitante antes de expedir el certificado. Al expedirlo, la autoridad certificadora lo firma con su clave privada, garantizando su validez y lo envía al solicitante. El siguiente esquema muestra todo el proceso.



5.3. Proceso de obtención de un certificado digital.

3.4 > Uso de los certificados

Los certificados de usuario pueden ser utilizados tanto para firmar documentos como para garantizar la confidencialidad en las comunicaciones. En este caso, los pasos del proceso serían los siguientes.



5.4. Funcionamiento de un certificado digital.

Todo este proceso, que puede parecer algo complicado, en realidad se realiza automáticamente en nuestros navegadores una vez que tenemos instalado el certificado de la autoridad de certificación. Cuando Blas se conecte con Ana, recibirá su certificado y, si tiene instalado el certificado de la autoridad de certificación, el navegador se encargará de todo el proceso de validación de forma automática.

3.5 > Clases de certificados

Existen multitud de clases de certificados digitales, que generalmente se diferencian en función de la entidad certificadora que los emite y de su finalidad.

Así, por ejemplo, CERES diferencia, atendiendo a sus destinatarios, entre certificados de persona física, de persona jurídica y de entidad sin personalidad jurídica.

Otros organismos reconocen otros certificados personales o corporativos, como por ejemplo los certificados de pertenencia a empresa, de atributo (profesión, cargo, etc.), de representación de empresa, etc.

También se distinguen distintos tipos de certificados atendiendo a su función:

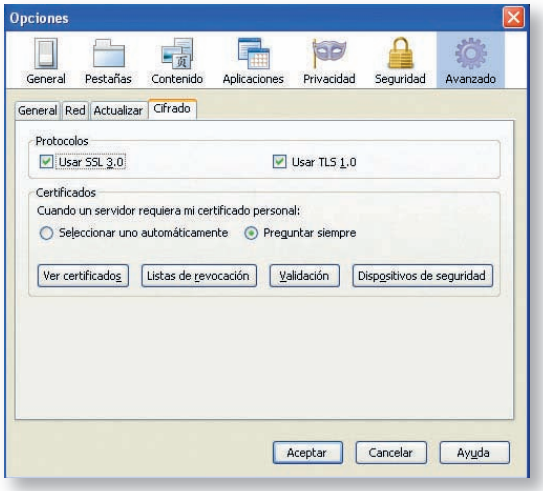
- **Certificados de servidor seguro:** identifican que una página web pertenece a una determinada persona o empresa y que la información transmitida entre el servidor y los usuarios de la web está cifrada y es segura.
- **Certificado de firma de código:** se usa para asegurar que el código que se ejecuta ha sido firmado por su desarrollador y no es malicioso.

Ejemplos

Instalación de certificados en Mozilla Firefox

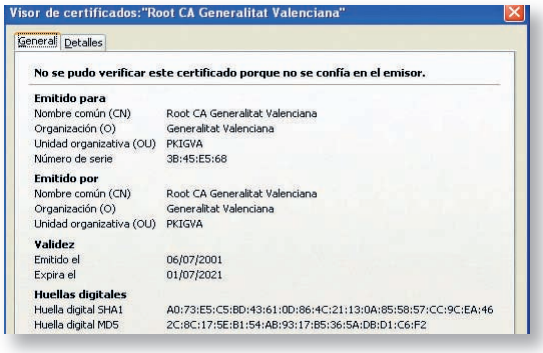
Los certificados digitales están incluidos en un archivo desde el que debemos instalarlos en el navegador que utilicemos; en este caso, Mozilla Firefox. El procedimiento para instalar certificados en este navegador variará un poco dependiendo de la versión del mismo que tengamos instalada, pero, en esencia, es muy similar al siguiente:

Para instalar un certificado en Mozilla Firefox, debemos acceder a *Herramientas* / *Opciones* / *Avanzado* y, en esta ventana, debemos seleccionar la pestaña *Cifrado*. Comprobamos que la opción *Preguntar siempre* esté marcada y hacemos clic en *Ver certificados*.



Se abrirá la siguiente ventana, en la que debemos hacer clic en *Importar* para cargar el certificado desde el archivo en que está contenido.

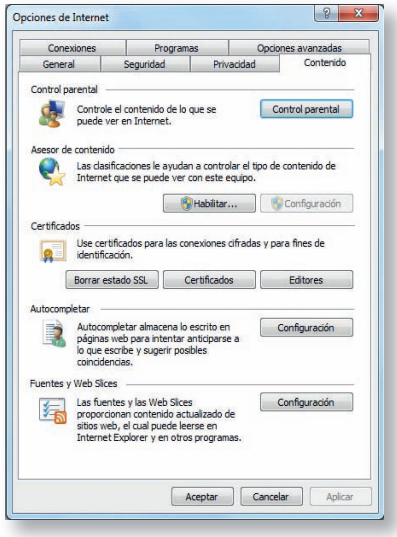
Buscamos el archivo que contiene el certificado a instalar y lo seleccionamos. Dependiendo de la versión de navegador, puede que se abra una nueva ventana. Si queremos inspeccionar el certificado podemos hacer clic en *Ver*. Se mostrará una ventana con toda la información referente al certificado.



Al finalizar el proceso, podremos comprobar que se ha instalado correctamente el certificado acudiendo a la ventana *Ver certificados*.

Ejemplos

Instalación de certificados en Internet Explorer



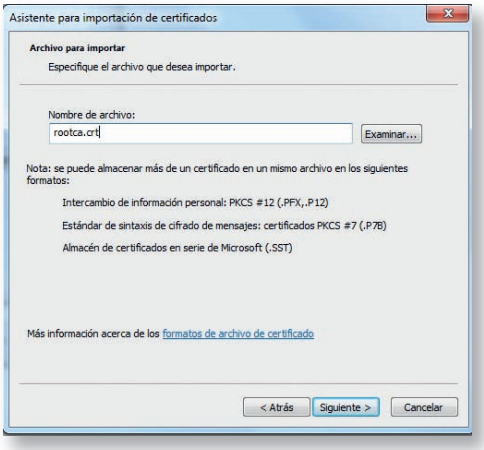
Como indicamos en el ejemplo anterior, los certificados digitales deben instalarse en el navegador web; por ello, su proceso de instalación será distinto en cada navegador.

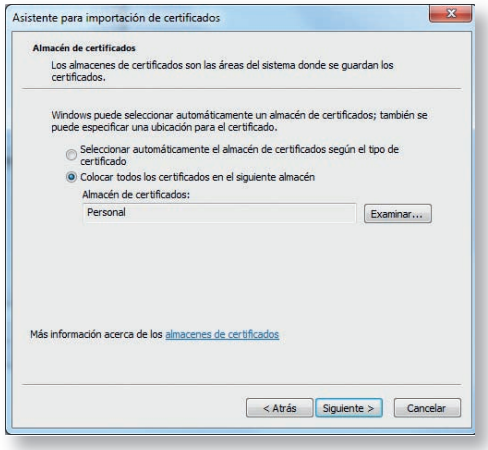
Ahora vamos a ver cómo se lleva a cabo ese proceso en Internet Explorer. Al igual que sucedía con Mozilla Firefox, este proceso puede variar dependiendo de las versiones del navegador, pero, en esencia, será el siguiente.

En primer lugar, hacemos clic en *Herramientas* / *Opciones de Internet*. En esa ventana, seleccionamos la pestaña *Contenido* y, dentro de esta, hacemos clic en *Certificados*.

Se abre la ventana *Certificados*. Seleccionamos la pestaña *Personal* y hacemos clic en el botón *Importar*, con lo que aparecerá el *Asistente de importación de certificados* que nos guiará en el proceso de importación.

Hacemos clic en *Siguiente* y nos pide que indiquemos la ubicación del archivo que contiene el certificado. Lo seleccionamos mediante el botón *Examinar*, hacemos clic en *Siguiente*. Seleccionamos el almacén automáticamente y volvemos a hacer clic en Siguiente.





Finalmente, se nos muestra un resumen y hacemos clic en *Finalizar*.

Actividades propuestas

4·· Busca en la página web de CERES (CERtificación ESpañola), perteneciente a la Fabrica Nacional de Moneda y Timbre, www.cert.fnmt.es, información sobre dónde podemos utilizar el certificado digital.

5·· Si no posees un certificado digital, solicítalo en la página web citada en la actividad anterior, siguiendo los pasos que allí te indican.

6·· Busca las iniciativas en materia de administración electrónica que existen en tu Comunidad Autónoma.

4 >> DNI electrónico

El DNI electrónico (DNIe) es un documento físico que incluye un chip en el que están almacenados los certificados digitales de su titular. Este documento se expide en España desde 2006 como una evolución del DNI anterior y está pensado para adaptar su uso a la sociedad de la información y para que sus portadores puedan utilizarlo en determinados servicios electrónicos.

El microchip incluye la siguiente información:

- **Datos de filiación** del titular.
- **Imagen digitalizada**, tanto de la fotografía como de la firma manuscrita.
- **Certificado de autenticación:** permite a su titular probar su identidad frente a terceros.
- **Certificado de firma electrónica avanzada:** permite a su titular firmar documentos y realizar trámites electrónicamente con validez. Sirve también para comprobar la integridad de los documentos firmados por el titular.
- **Par de claves** (pública y privada) de cada certificado electrónico.

En cuanto a las medidas de seguridad que incluye el documento, podemos distinguir entre las físicas y las electrónicas:

- **Medidas físicas:** relieves, tintas solo visibles con luz ultravioleta, etc.
- **Medidas digitales:** encriptación de los datos del chip, acceso a las funcionalidades a través de la clave privada de acceso (denominada PIN), etc.

Para la utilización del DNI electrónico es necesario disponer de diversos elementos, de hardware y software, que permiten utilizar los certificados incluidos en el chip:

- **Elementos de hardware.** Es necesario disponer de un ordenador y de un lector de tarjetas inteligentes compatible con la norma ISO 7816. Este lector puede ser externo al equipo o estar integrado en el mismo a través de una tarjeta o, incluso, a través de un lector de tarjetas incluido en el teclado.
- **Elementos de software.** El ordenador debe contar con tres elementos básicos: sistema operativo instalado (es compatible con los sistemas Microsoft Windows, Linux y Mac OS), navegador web (es compatible con los navegadores Internet Explorer, Mozilla Firefox y Chrome) y un programa controlador. Para poder interactuar correctamente con las tarjetas criptográficas en general y, en particular con el DNI electrónico, el equipo ha de tener instalado un software denominado módulos criptográficos.

Web

Puedes acceder a toda la información sobre el DNI electrónico en su página web: www.dnielectronico.es.

Actividades propuestas

7·· Enumera qué ventajas en materia de seguridad tiene el DNI electrónico frente al anterior.

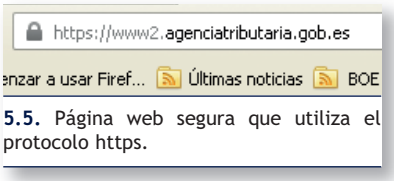
8·· Indica qué funcionalidades proporciona el DNI electrónico frente al DNI antiguo.

5 >> SSL y TLS

SSL y TLS son protocolos que proporcionan comunicaciones seguras en una red insegura, como Internet.

– **SSL:** *Secure Sockets Layer* o protocolo de capa de conexión segura.
– **TLS:** *Transport Layer Security* o seguridad de la capa de transporte.

En ambos casos existe un sistema híbrido que usa un canal seguro con cifrado asimétrico (Diffie-Hellman) para intercambiar las claves simétricas dinámicas (van cambiándose cada cierto tiempo) negociadas entre ambas partes. El cifrado de estos protocolos se produce sobre la capa de transporte.



5.5. Página web segura que utiliza el protocolo https.

Una de las principales aplicaciones prácticas de estos protocolos es formar **https** junto a **http**, garantizando el envío y recepción de información de forma segura mediante un navegador web. Todo esto permite confidencialidad en las comunicaciones, manteniendo la integridad de los datos al tiempo que se garantiza la identidad de las partes.

Toda comunicación mediante SSL o TLS consta de dos fases:

– **Fase de saludo**, correspondiente con los sistemas de criptografía de clave asimétrica, en la que se negocia entre las partes el algoritmo que se usará en la comunicación. También se produce el intercambio de claves públicas, autenticándose cada una de las partes mediante certificados digitales X.509. Los dos interlocutores eligen una clave de sesión.
– **Fase de comunicación,** correspondiente con los sistemas de criptografía de clave simétrica, en la que se produce el cifrado del tráfico basado en cifrado simétrico a partir de la clave de sesión y se van generando nuevas claves de forma dinámica.

En cuanto a las características de cada uno de estos protocolos, SSL es un protocolo abierto que puede ser empleado por cualquier fabricante de aplicaciones para Internet para asegurar la privacidad en el envío de información a través de la web. Se suele utilizar en servidores web y permite que la información transmitida entre un navegador web (cliente) y un servidor web esté cifrada. El servidor debe utilizar un par de claves así como un certificado.

SSL presenta las versiones 1 y 2 (en las que se proporciona autenticación de servidor) y 3 (en que se añade autenticación del cliente por medio de certificados digitales del cliente y servidor).

En cuanto al TLS, es un protocolo basado en SSL mejorado. Existen diferentes versiones que van corrigiendo vulnerabilidades detectadas en versiones anteriores. La última versión es TLS 1.2, definida en el RFC 5246.

Actividades propuestas

9·· Elabora una presentación sobre la herramienta Firesheep u otra similar. Indica, al menos:

a) En qué consiste y cuál es su objetivo.
b) Cómo funciona.
c) Cómo protegerse de ella.

6 >> Cifrado de información

El cifrado de datos o encriptación, como ya se ha visto, es el proceso en el cual una información legible es convertida, por algún algoritmo seguro, en una información que será ilegible a menos que se tenga la clave del cifrado.

La pérdida o robo de dispositivos móviles, como pueda ser el portátil, el móvil, una memoria USB o disco externo, puede llegar a ser un verdadero problema de seguridad.

Las medidas preventivas básicas recomendadas para reducir el impacto de la pérdida de estos dispositivos móviles suelen ser la concienciación y formación del usuario. Pero más allá de estas, no está de más que el usuario tome también medidas técnicas como pueda ser el cifrado de los dispositivos o utilizar dispositivos con tecnologías biométricas de autenticación. Todo ello acompañado del uso de contraseñas de calidad.

Hoy en día, también se ofrecen servicios externos que permiten el borrado remoto de los datos ante incidentes de este tipo.

Se pueden encontrar en el mercado multitud de herramientas para el cifrado de datos, entre las que encontramos **Bitlocker** para Windows 7 Utimatte, **Enterprise**, GnuPG (que permite cifrar archivos independientes) o **TrueCrypt**, que permite cifrar todo el disco duro, una partición, un conjunto de archivos o todo el contenido de un dispositivo extraíble, como el USB.

El inconveniente de cifrar todo un dispositivo USB es que solo podríamos utilizarlo en aquellos equipos donde tuviésemos permisos de administrador y estuviese instalado el programa de cifrado. Por tanto, es recomendable crear un volumen cifrado o contenedor dentro del dispositivo USB y no cifrarlo todo. De este modo, se podrá acceder al dispositivo en cualquier equipo excepto a la parte cifrada, que se verá como un archivo que ocupa parte del dispositivo.

Una vez cifrado un volumen, este aparece como un simple fichero que podría ser borrado, ya que estas herramientas de cifrado protegen de accesos indebidos, pero no de los borrados.

¿Encriptación o cifrado?

Encriptación es una pseudotraducción de la palabra inglesa *encrypt*. Por ello, es preferible utilizar la palabra "cifrado" en lugar de "encriptación".

Casos célebres de pérdida de información

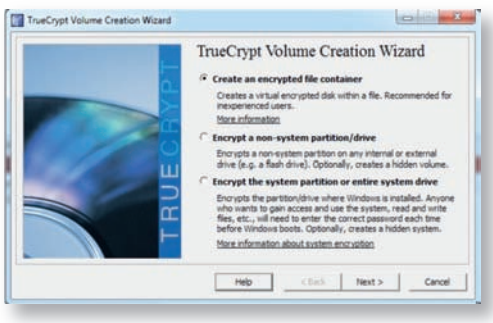
Un caso emblemático de pérdida de datos por no haberlos cifrado es la desaparición de 95 000 registros de alumnos de la Universidad de Berkeley, debido a la pérdida de un portátil.

La mayoría de estos datos acabaron vendiéndose en páginas de subastas *online*.

Ejemplos

Creación de un volumen cifrado y acceso al mismo con TrueCrypt

En este ejemplo, vamos a cifrar un volumen en una memoria USB utilizando TrueCrypt, por ello, el primer paso será tener instalada esta aplicación en el ordenador. Antes de empezar, es recomendable hacer una copia de seguridad de los datos del USB, por si hay algún error en el proceso de cifrado. A continuación, ejecutamos TrueCrypt y en la ventana que aparece seleccionamos *Create Volume*. Seguidamente seleccionamos la opción por defecto *Created an encrypted file container,* que permite cifrar un contenedor de archivos en el dispositivo.

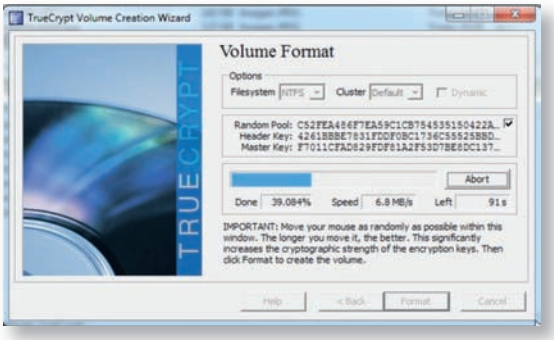


En la ventana siguiente elegimos la opción por defecto *Standard TrueCrypt Volume* y, en la que viene a continuación, *Select File* y marcamos como destino donde se va a crear el volumen cifrado o contenedor el dispositivo USB. Nos aseguramos de que hay suficiente espacio para crear un fichero y elegimos un nombre para el mismo, en este caso *Cipher*.

En la siguiente pantalla hay que elegir el algoritmo de cifrado. Se puede hacer cifrado por niveles, por ejemplo primero AES y luego Twofish. Vamos a dejar AES, que ya es más que suficiente para nuestro propósito.

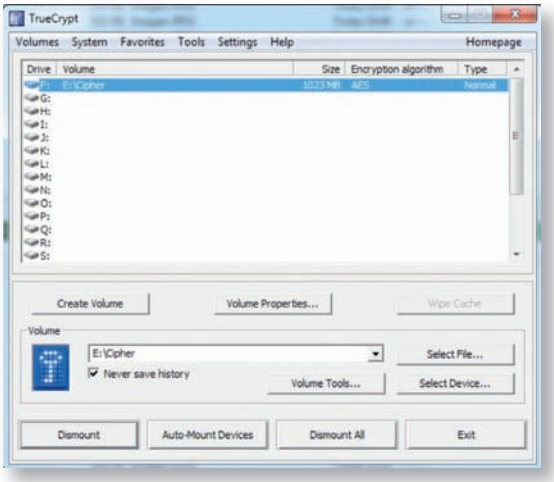
A continuación la aplicación pregunta el tamaño que queremos darle al volumen a cifrar. Se puede elegir que sea todo el USB o bien parte de este. Elegiremos, en este caso, que el volumen a cifrar sea de 1 GB de los 4 GB que tiene en total el dispositivo. Hay que tener en cuenta que si el dispositivo es FAT32 no se podrá crear un volumen de más de 4 GB.

En la siguiente pantalla se nos pide introducir la contraseña (si se van a cifrar ficheros mayores de 4 GB aparecerá una ventana que pregunta si se tiene la intención de almacenar ficheros mayores de 4 GB).



Empieza el proceso de cifrado, durante el cual se debe mover el cursor del ratón dentro de la ventana de TrueCrypt de la forma más aleatoria posible. Cuanto más se mueva el ratón, más crecerá la fortaleza criptográfica de la contraseña.

Una vez finalizado el proceso, aparecerá otra ventana indicando que todo ha ido como se esperaba. El volumen estará cifrado. Se podrá observar que se ha creado un fichero llamado *Cipher* de 1 GB, que representa la parte cifrada del dispositivo USB.



Ahora vamos a acceder a un dispositivo que contiene un volumen cifrado con TrueCrypt. En primer lugar, ejecutamos TrueCrypt y, en la primera ventana que se muestra, seleccionamos una de las unidades que aparecen libres. Mediante el botón *Selected File*, accedemos al fichero *Cipher* creado y almacenado en la unidad USB. Finalmente hacemos clic en el botón *Mount*.

Aparecerá una nueva unidad con la letra elegida, la cual mostrará el volumen o parte cifrada de los dispositivos USB. Introducimos la contraseña y se podrá observar cómo una nueva unidad de disco (en este caso la F:) aparece en el equipo con el tamaño de la parte cifrada y con la que se podrá trabajar.

Una vez se ha acabado de trabajar con el volumen cifrado, hay que desmontarlo. Para ello accedemos a la aplicacion TrueCrypt, seleccionamos la unidad a desmontar y elegimos el botón *Dismount*.

Actividades propuestas

10·· Busca en Internet otras aplicaciones que permitan cifrar información.

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿Cómo se puede saber a ciencia cierta que la clave pública de un usuario corresponde realmente a ese individuo y no ha sido falsificada por otro?

2·· ¿Quién verifica la identidad del poseedor de la clave pública?

3·· ¿Qué técnica puede certificar que un mensaje ha sido enviado?

4·· ¿Qué servicios de seguridad se implementan con la firma digital?

5·· ¿Qué información contiene un certificado digital?

6·· ¿Qué ventajas proporcionan los certificados digitales?

7·· ¿Qué puede provocar que un certificado sea revocado? ¿Cómo se revoca un certificado?

8·· ¿Quiénes son las autoridades certificadoras y qué objetivo tienen?

9·· ¿En qué consisten los protocolos SSL y TLS? ¿En qué se diferencian?

10·· ¿Para qué situaciones puede ser útil utilizar SSL o TLS?

11·· ¿Por qué razones recomendarías cifrar los datos en un dispositivo de almacenamiento externo?

12·· ¿Cómo puedes ver si una página web segura está realmente cifrada o no? ¿Dónde se indica el tipo de cifrado utilizado?

13·· ¿Qué ventajas plantea la utilización de OpenPGP en un gestor de correo?

14·· ¿Qué técnica de las vistas en la unidad es en la que se basa el sistema de voto electrónico para que funcione? ¿Por qué crees que este sistema no cuenta con las garantías suficientes para poder ser implantado a día de hoy?

15·· ¿Qué tipo de sistema de cifrado crees que es el más recomendable si se quiere conectar a una página segura para hacer alguna transacción que requiera seguridad?

16·· ¿Cómo puede un usuario malintencionado realizar ataques con éxito contra los protocolos SSL/TLS?

.: APLICACIÓN :.

1·· Explica los pasos que deberías seguir para obtener un certificado personal.

2·· Entra en la página web de la Agencia Tributaria e indica el procedimiento que debes seguir para obtener el borrador de la declaración de la renta utilizando el DNI electrónico.

3·· Al intentar acceder a una página web segura (https://), el navegador te advierte de que la página web a la que estás intentando acceder tiene un certificado desconocido. ¿Quiere esto decir que la página web es falsa o una amenaza?

4·· Vas a hacer una copia de seguridad de información personal (fotos, trabajos, etc.) de tu equipo y quieres guardarla en un DVD, pero no quieres que un desconocido pueda acceder a la esa información. ¿Qué puedes hacer?

5·· Quieres enviar correos cifrados a un compañero de clase de manera que solo él pueda ver su contenido. ¿Qué mecanismo tienes que utilizar?

6·· Vas a descargarte desde una página web un archivo llamado *programa.tar.gz* y observas que, junto a este, hay otro llamado *programa.tar.gz.sign*, con un tamaño significativamente inferior. ¿Significa esto que hay dos versiones del mismo archivo?

Caso final 2

Certificados digitales con XCA para un servidor web seguro

•• Utilizando dos equipos con Linux instalado, genera mediante XCA (interfaz gráfico de openSSL) certificados digitales para montar un servidor web seguro ficticio, cuya dirección será www.servidorseguro.com. Para ello:

a) Debes crear una autoridad de certificación.
b) Un equipo creará un borrador de certificado, el cual no será válido hasta que se lo envíe a una autoridad de certificación para que esta lo firme.
c) La autoridad de certificación firmará el borrador de certificado, convirtiéndolo en un certificado válido.

Solución •• Para la instalación de XCA, deberás ejecutar `yum install xca` en caso de Fedora o `apt-get install xca` en caso de Debian y derivadas.

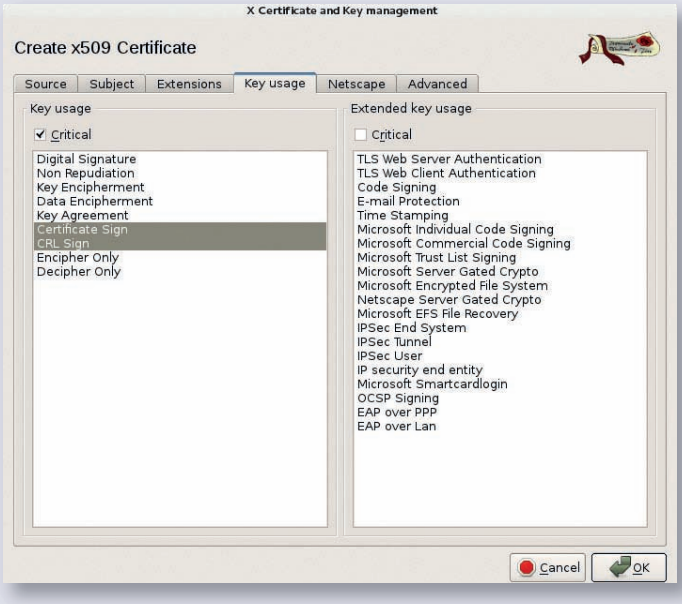
Antes de trabajar con el programa, los dos equipos deben crear una base de datos donde el programa guardará y gestionará todos los certificados que solicites o que crees. Esto se hace con *File / New Database*. Elige un nombre y una ruta (por ejemplo, en */home/usuario/CertDatabase*). El programa pedirá una contraseña para proteger los certificados y sus claves privadas.

a) Creación de una AC

Para constituir un equipo como una AC que podrá certificar y validar certificados digitales de otras personas o servidores web, debes ir a la pestaña *Certificates* y hacer clic en *New Certificate*.

En la ventana que aparece, en la pestaña *Source*, selecciona la plantilla *[default] CA* y haz clic en *Apply all*. La aplicación XCA dispone de una serie de plantillas (*templates*) para configurar parámetros por defecto en función del uso del certificado.

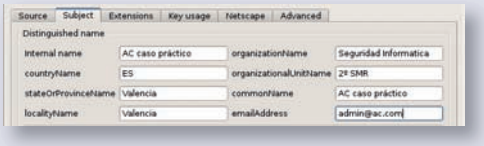
En esta misma pestaña observa que está marcada la opción *Create a self signed certificate with the serial*, lo que viene a decir que el certificado es un certificado raíz de certificación autofirmado, es decir, no hay jerárquicamente ninguna otra AC por encima que valide este certificado. Esto significa que cualquier certificado de servidor https que se firme con esta AC no va a ser aceptado por defecto en ningún navegador, a menos que se instale el certificado de la AC que estás creando.



En la pestaña *Extensions* está marcado *Certification Authority* como tipo de certificado y con una validez de 10 años porque en la plantilla por defecto se ha definido esa validez. No obstante, hay algunas AC como la GVA o la FNMT que tienen 20 de años de validez en sus certificados.

En la pestaña *Key Usage* (utilización de la clave), marca *Certificate Sign* y *CRL Sign*. Debes hacerlo así, pues este es el uso habitual de un certificado de una AC: firmar y revocar otros certificados. En el marco *Key Usage* selecciona la opción *Critical*.

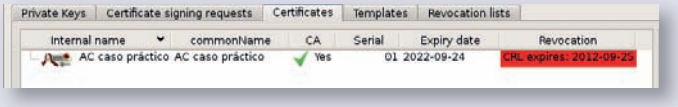
En la pestaña *Subject* (Sujeto) debes rellenar los campos que identificarán esta AC. En la siguiente imagen hay un ejemplo de los valores que puedes poner (evita usar acentos).



En esta misma pestaña debes crear un par de claves para el certificado. Recuerda que los certificados digitales utilizan la criptografía asimétrica o de clave pública y, por tanto, todo certificado va asociado a un par de claves. Para ello haz clic en *Generate a new key* y dale un nombre. Para mayor seguridad, puedes cambiar el tamaño de la clave de 1024 a 2048 bits o el tipo de clave (RSA, DSA), aunque en principio con los valores por defecto de RSA 1024 es suficiente.

Después de seleccionar el botón *Create*, vuelve a la pestaña *Subject*, donde podrás ver que se ha creado una clave para la AC.

Haz clic en *OK* y vuelve a la pantalla principal del programa. El certificado para esta autoridad certificadora aparecerá en la pestaña *Certificates*, que muestra la lista de certificados del programa.



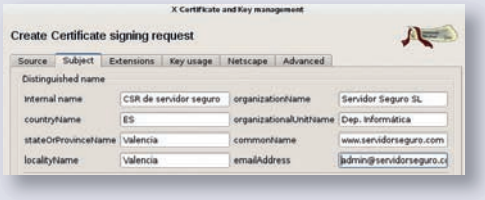
En este momento has creado una AC con capacidad de firmar y revocar certificados a personas o a servidores web para https. El siguiente paso es que un cliente envíe una petición de firma de un certificado (conocido como CSR: *Certificate Signing Request*), que podría utilizarse, por ejemplo, para montar un servidor https para un dominio, como ocurre en este caso práctico.

b) Creación de un borrador de certificado y envío a una AC para que lo firme

Todas las tareas anteriores las has realizado en un equipo. Ahora vas a utilizar el otro. Para empezar, crea en él una base de datos del mismo modo que en el apartado anterior. A continuación, vete a la pestaña *Certificate Signing Request* y haz clic en *New Request*.

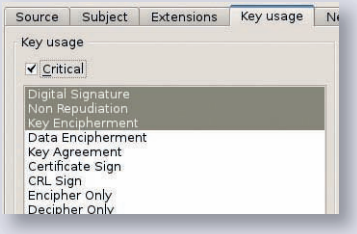
En la pestaña *Source* selecciona la plantilla *[default] HTTPS_server* y haz clic en *Apply all*, de una forma similar a lo que has hecho anteriormente para crear el certificado para la AC. Es importante remarcar que en el paso anterior se ha marcado la plantilla *[default] CA*, mientras que ahora estás marcando otra plantilla denominada *[default] HTTPS_server*, lo cual es lógico porque ahora mismo no estás creando una AC, sino un certificado para un servidor web seguro.

En la pestaña *Subject* rellena los campos que identificarán al servidor web. En la siguiente pantalla hay un ejemplo de los valores que podemos poner. Es fundamental que el *Common Name* sea correcto y se corresponda con el *FQDN* (nombre de dominio completo) que usará el servidor en Internet (www.servidorseguro.com) pues si no coinciden el navegador dará un aviso de seguridad.



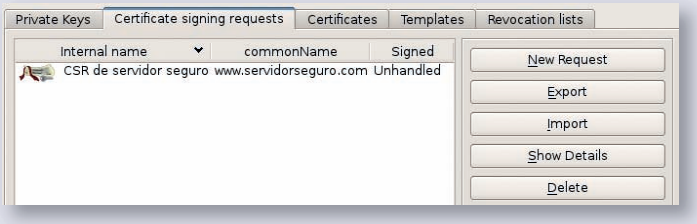
2

De forma análoga a la anterior, para crear el certificado para la AC, deberás crear un par de claves pública y privada marcando el botón *Generate a new key* y seleccionando la longitud de clave y el tipo de cifrado utilizado para las mismas.



En la pestaña *Key usage* verás que se han marcado automáticamente los usos del certificado y deberás seleccionar la opción *Critical*.

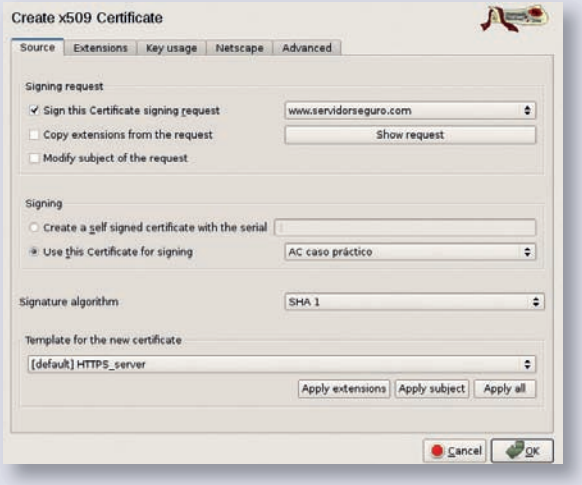
Haz clic en *OK*. Con ello habrás generado una petición de firma de certificado (CSR), *que es casi un certificado*, porque solo le falta que una AC lo verifique, lo autorice y lo firme. Para ello debes exportar el CSR haciendo clic en el botón *Export* en la pestaña *Certificate Signing Requests* y seleccionar el formato PEM. A continuación debes enviar este archivo a la AC para que lo firme.



c) La AC firma el borrador de certificado convirtiéndolo en un certificado válido

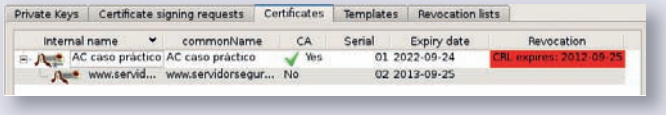
Lo primero que debe hacer una AC es comprobar la identidad de la empresa o persona que ha solicitado la firma de un certificado. Una vez verificada su identidad, se debe firmar la petición de certificado con la clave privada del certificado de AC.

Para ello, importa el CSR del otro equipo haciendo clic en el botón *Import* en la pestaña *Certificate Signing Requests*. Una vez importado, selecciónalo y, con el botón secundario, haz clic en *Sign* para firmarlo con el certificado de la AC.



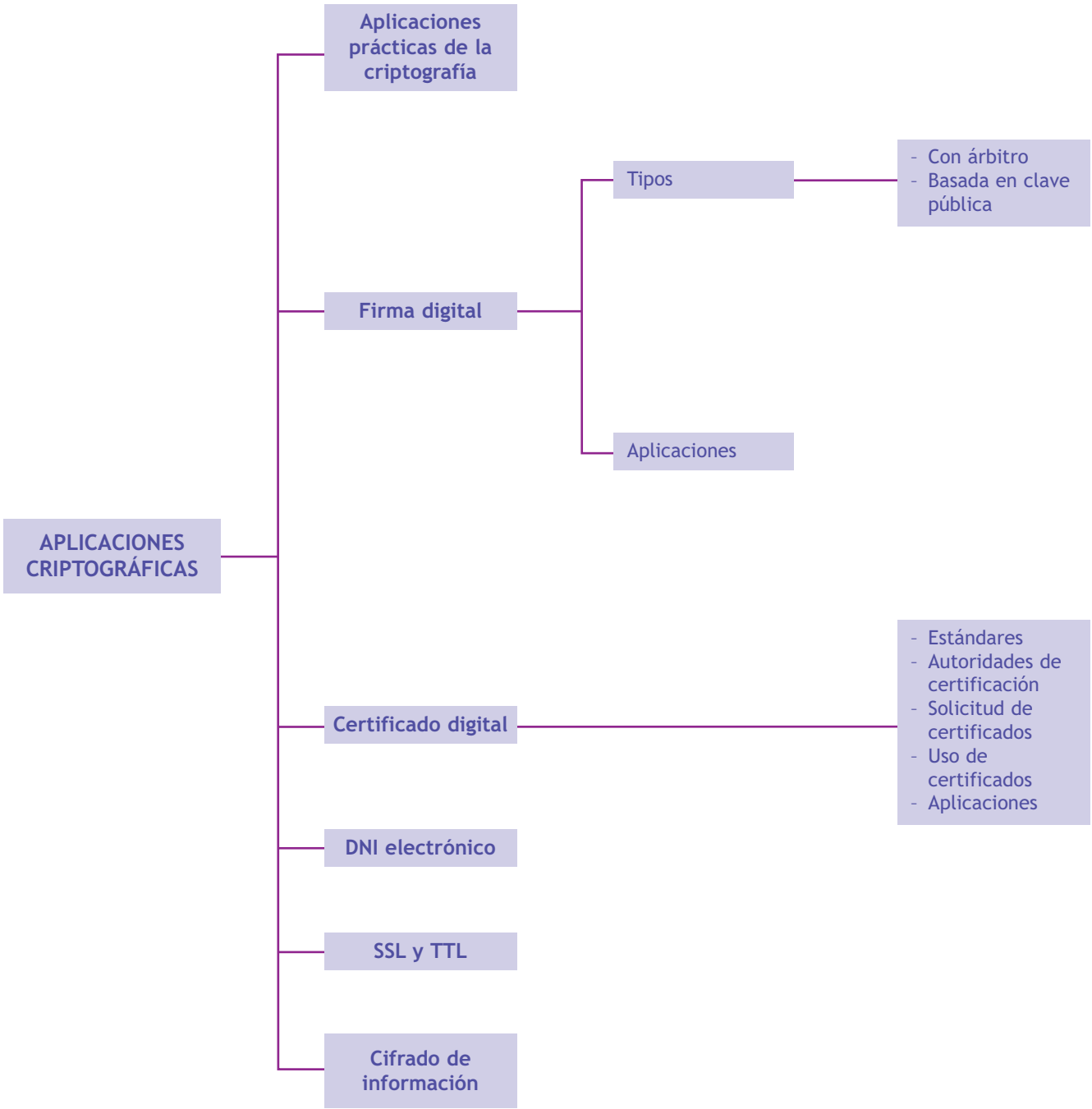
Se abrirá una ventana con información sobre el CSR que vas a firmar. En la pestaña *Source*, desmarca la opción *Copy extensions from the request* y selecciona *Use this Certificate for signing*. Como este certificado se va a utilizar para un servidor web seguro, selecciona la plantilla *[default] HTTPS_Server* y haz clic en *Apply all* como has hecho anteriormente para crear el CSR.

En la pestaña *Key Usage* marca la opción *Critical* y haz clic en *OK*. En la sección *Certificates* verás que el certificado se ha creado correctamente.



El último paso será exportar el certificado a un formato de codificación válido para un certificado, como PEM, DER, PKCS#7 o 12. Para ello debes ir a la sección *Certificates*, seleccionar el certificado y hacer clic con el botón secundario del ratón en *Export*.

Ideas clave


APLICACIONES CRIPTOGRÁFICAS
Aplicaciones prácticas de la criptografía
Firma digital
Tipos
- Con árbitro
- Basada en clave pública
Aplicaciones
Certificado digital
- Estándares
- Autoridades de certificación
- Solicitud de certificados
- Uso de certificados
- Aplicaciones
DNI electrónico
SSL y TTL
Cifrado de información

¿Qué es CERES?

La FNMT- RCM, a través de su departamento CERES ofrece el certificado electrónico FNMT Clase 2CA.

La revolución de la tecnología de información, conjuntamente con el desarrollo de la infraestructura de comunicaciones, está haciendo cambiar significativamente las relaciones entre individuos y organizaciones, tanto en España como en todo el mundo. Estas nuevas formas de comunicación abren un gran abanico de posibilidades tanto para ciudadanos como para empresas y permiten comercializar productos y servicios de una forma ágil y económica.

En España, las distintas Administraciones están apostando decididamente por Internet como vía de comunicación, creando webs con información de interés público a disposición de la ciudadanía.

La más ambiciosa de estas iniciativas puestas en marcha por la Administración es el denominado proyecto CERES (CERtificación ESpañola), que lidera la

Fábrica Nacional de Moneda y Timbre y que, en líneas generales, consiste en establecer una entidad pública de certificación que permita autenticar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y Administraciones Públicas a través de las redes abiertas de comunicación.

Las posibilidades de CERES cubren todas aquellas relaciones entre las distintas Administraciones (Central, Autonómica y Local) y los ciudadanos que necesiten ser securizadas en términos de garantía de identidad, confidencialidad e integridad. Para ello, CERES utiliza técnicas y sistemas criptográficos basados en lo que se conoce como sistema de clave pública, con dos características básicas:

- La identidad del usuario, al igual que su capacidad de firma, se encuentra, en el caso de máxima seguridad, almacenada en una tarjeta inteligente, que no puede ser accesible salvo por su propietario cuando introduzca el número de identificación personal, similar a la clave de una tarjeta de crédito. En caso de no utilizar tarjeta, el perfil criptográfico queda almacenado en un fichero, siendo necesario también un PIN de acceso.

- El sistema es completamente transparente para el usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje.

Fuente: Fábrica Nacional de Moneda y Timbre. "Proyecto CERES". www.cert.fnmt.es

Actividades

1·· ¿Qué certificado ofrece FNMT-RCM?

2·· ¿Cuáles son las necesidades que han llevado a la utilización de los certificados electrónicos?

3·· ¿En qué consiste el proyecto CERES?

4·· ¿Qué objetivos persigue el proyecto CERES?

unidad 6

Software malicioso

SUMARIO

- Tipos de software malicioso
- Denegación de servicio
- Publicidad y correo no deseado
- Ingeniería social
- Fraudes informáticos

OBJETIVOS

- Diferenciar entre los diferentes tipos de software malicioso que existen.
- Conocer los ataques de denegación de servicio.
- Distinguir entre publicidad y correo no deseado.
- Conocer en qué consiste la ingeniería social.

1 >> Concepto de software malicioso

En la actualidad casi todos conocemos o hemos oído hablar de los virus informáticos, pero ¿sabemos realmente qué es un virus?, ¿todos estos "ataques" están originados por virus informáticos? La respuesta es no.

Estos ataques proceden de un tipo de software que suele denominarse **software malicioso** (***malware*** en inglés, que proviene de las palabras ***MALicious softWARE***). El software malicioso puede modificar el funcionamiento de un equipo informático o alterar la información que procesa, ya sea borrándola, modificándola o enviándola sin nuestro conocimiento a terceras personas. Por lo tanto, el término software malicioso tiene un ámbito más amplio que el de virus informático y se utiliza para designar a cualquier software que pueda representar una amenaza al sistema o resultar molesto para el usuario. Así, un virus informático es una variedad más de software malicioso, como lo son los troyanos, el *spyware,* el *adware,* etc.

Generalmente, el *malware* se propaga a través de dos vulnerabilidades:

- **Vulnerabilidades del software:** se trata de explotar debilidades del sistema operativo o de algún programa. Algunos especímenes de *malware* son capaces de copiarse a sí mismos y enviarse automáticamente a través de la red para infectar a la mayor cantidad posible de equipos. Para evitar este tipo de infecciones conviene tener actualizados el sistema operativo y los programas utilizados.
- **Vulnerabilidades asociadas a las personas:** en la mayoría de ocasiones son las propios usuarios quienes, con su desconocimiento o exceso de confianza, contribuyen a la propagación del software malicioso. Podemos tener un equipo con el sistema operativo más seguro del mundo y con un antivirus actualizado, pero si las personas que lo utilizan son descuidadas tarde o temprano acabará infectándose. La primera recomendación que debemos tener en cuenta como usuarios es sentido común y prudencia.

Otro aspecto a tener en cuenta sobre el software malicioso es su difusión. Prácticamente la mayoría del *malware* desarrollado en la actualidad afecta a sistemas **Microsoft**, que son los más extendidos. Es un error muy común pensar que estamos protegidos por el simple hecho de no utilizar un sistema operativo de Microsoft, ya que existen variedades de *malware* diseñadas específicamente para aprovechar vulnerabilidades de otras plataformas, como **MacOS** y **Linux**. Por otro lado, el *malware* no solo afecta a los equipos informáticos y en la actualidad es fácil encontrar especímenes creados para dispositivos móviles que afectan a sistemas como **Android**, **Symbian** o **iOS**.

El primer virus

La mayoría de expertos considera que el primer virus informático fue ***Elk Cloner*** y fue creado por Rich Skrenta en 1982 cuando tenía 14 años. ***Elk Cloner*** no buscaba dañar equipos ni datos, sino molestar un poco al usuario, así que cada 50 arranques mostraba un poema en pantalla.

Actividades propuestas

1·· Busca información en la página web: http://cert.inteco.es sobre algún *malware* que haya ocasionado infecciones durante los últimos seis meses e indica a qué SO afectaba, cómo se propagaba y su nivel de peligrosidad.

2 >> Clasificación del *malware*

Existe una gran variedad de software malicioso y cada día se descubren nuevos programas de este tipo, por lo que no es fácil realizar una clasificación del *malware.*

Por ello, se pueden establecer distintas clasificaciones, en función del criterio elegido para realizarlas.

2.1 > Según el impacto producido sobre la víctima

Atendiendo a este criterio, distinguimos tres niveles de peligrosidad: **bajo, medio** o **elevado.**

Para evaluar el grado de peligrosidad de un espécimen, se estudia la gravedad de las acciones que produce sobre un equipo infectado, su velocidad y facilidad de propagación y la cantidad de infecciones producidas recientemente.

2.2 > Según su forma de propagación

Según la forma de propagarse, los tipos de *malware* más importantes son: virus, gusanos y troyanos.

Virus

Podemos definir un virus informático como:

> **Un virus informático es un software malicioso que tiene por finalidad alterar el funcionamiento de un equipo informático sin el conocimiento o consentimiento de su usuario, corrompiendo o destruyendo archivos.**

Su principal característica es que, cuando se ejecuta, se propaga infectando a otros ficheros. Por ello, para extenderse necesita de la intervención humana, pues tiene que haber alguien que ejecute el programa malicioso ya que el virus no se ejecuta automáticamente.

El funcionamiento de los virus es simple: cuando se ejecuta el software malicioso, el virus se instala en la memoria RAM del ordenador, desde donde infecta archivos ejecutables y graba los archivos infectados en el disco duro del equipo. De este modo, una vez en el disco, el virus se ejecutará cada vez que se utilice el programa infectado. Si se reinstala el programa afectado sin apagar el ordenador, el virus volverá a infectarlo (ya que sigue estando en la RAM).

En cuanto a sus efectos, en algunos casos las acciones resultantes de la ejecución de un virus parecen inofensivas, como cambiar carpetas por accesos directos ocultando los archivos originales, pero en otras ocasiones pueden llegar a modificar el registro de Windows con la finalidad de evitar el cortafuegos, permitiendo a un atacante controlar a su antojo el equipo de la víctima.

Su forma de propagación es muy variada: algunos tipos residen en ficheros ejecutables y se reproducen al ejecutarlos, otros se transmiten al visitar una página web que contiene código que enlaza a una página maliciosa, etc.

Rootkit

Malware que modifica el sistema operativo del equipo infectado para permanecer oculto ante el usuario y las aplicaciones de seguridad. En muchas ocasiones los antivirus no los detectan.

Algunas empresas han utilizado este tipo de *malware* en sus productos, como la empresa Sony, que desarrolló un sistema anticopia en sus CD que utilizaba técnicas avanzadas para evitar ser detectado por los antivirus, instalándose en el sistema.

Gusanos

Un *worm* o gusano es un tipo de *malware* que se propaga automáticamente sin necesidad de infectar otros archivos, ya que puede duplicarse a sí mismo. Por tanto, puede extenderse sin necesidad de intervención de los usuarios de los equipos infectdos.

Su finalidad no es destruir archivos o equipos, sino que están pensados para consumir recursos de un sistema o red de comunicaciones hasta saturarlo y provocar su caída.

Sus principales formas de difusión son las siguientes:

- Programas de mensajería instantánea o canales de chat.
- Recursos compartidos de una red local.
- Redes P2P (*peer to peer*). En estas redes un equipo puede descargarse archivos de cualquier otro equipo de la red y a su vez compartir archivos con los demás; por ello, todos los equipos pueden ser a la vez clientes y servidores. Esta es una de las vías preferidas de infección, puesto que los gusanos se camuflan como archivos con nombres atractivos para los usuarios, adoptando nombres de películas de actualidad o vídeos humorísticos.
- Correo electrónico. Pueden ir adjuntos al mensaje o bien camuflados dentro del código html de los mensajes, por lo que basta con previsualizar el mensaje para activarlos. En todos estos casos, los mensajes que los incluyen suelen tener un asunto interesante para captar la atención del destinatario y hacer que abra el mensaje (por ejemplo, el famoso gusano I love you, llamado así porque ese era el asunto del mensaje que lo incluía).

La desinfección de un gusano suele ser más sencilla que la de un virus porque los gusanos no modifican archivos, solo cambian algunos parámetros del sistema, como el registro o la lista de programas que se ejecutan al iniciar el ordenador, para, de este modo, ejecutarse cada vez que el usuario arranca el sistema.

Troyanos

Un troyano o caballo de Troya es un software malicioso que se introduce en un ordenador y se instala en él, aparentando ser un programa inofensivo, pero su finalidad es permitir a un usuario no autorizado tomar el control de la máquina infectada.

A diferencia de los virus, los troyanos ni infectan o corrompen archivos o programas y, a diferencia de los gusanos, no tienen capacidad de propagarse automáticamente, únicamente buscan permitir la administración remota del equipo a usuarios ilegítimos.

Las infecciones con este tipo de *malware* se suelen producir cuando el usuario ejecuta un programa infectado. El programa, aparentemente, funciona correctamente, pero en un segundo plano, de forma invisible, se instala el troyano. Una vez que se instalan, pasan desapercibidos para el usuario del ordenador infectado llevando a cabo diversas acciones, fundamentalmente con el objetivo de controlar ese equipo.

Caballo de Troya

El término de caballo de Troya proviene de la conquista de Troya por los griegos, narrada en la *Odisea* de Homero. Los griegos utilizaron un enorme caballo de madera como regalo a la ciudad de Troya y se ocultaron en su interior para poder conquistarla.

Un troyano, normalmente, está constituido por dos programas: un **cliente** en el equipo atacante, que es el que envía las órdenes, y un **servidor** que se instala en el ordenador infectado y es el que recibe las órdenes del intruso y las ejecuta, enviando la información solicitada. Habitualmente, la conexión entre estos dos programas se lleva a cabo de dos formas diferentes:

- **Conexión directa:** la más habitual, en que el cliente se conecta al servidor para enviarle órdenes.
- **Conexión inversa:** en que es el servidor el que envía directamente la información al cliente. Es mucho más efectiva, pues muchos *firewalls* no analizan la información saliente del ordenador.

Las especies mas habituales de troyanos son:

- ***Backdoor.*** Este tipo de *malware* es muy peligroso y permite el acceso remoto a un atacante sobre el sistema operativo, una aplicación, una página web o un recurso, de ahí el significado de su nombre ("puerta trasera"). Un equipo infectado con un *malware backdoor* permite, por tanto, que el atacante controle el equipo sin necesidad de autenticarse, por lo que tendría acceso total sobre cualquier archivo del disco para verlo, copiarlo o modificarlo; asimismo, podría robar cualquier información personal almacenada, transmitida o recibida desde ese equipo. Además podría utilizar el ordenador para cualquier finalidad, como por ejemplo, crear una red de "ordenadores *zombies*" o *botnet*.
- ***Keylogger.*** Un *keylogger* es un espécimen de *malware* que captura las pulsaciones de las teclas realizadas en el equipo de la víctima para proporcionárselas al atacante, con lo que se podría obtener las claves de sus cuentas bancarias o las conversaciones que ha tenido con otras personas. Para protegerse frente a este tipo de *malware*, algunas entidades bancarias utilizan un mecanismo que evita que el usuario tenga que teclear su clave, mostrando por pantalla un teclado virtual que el cliente deberá ir seleccionando para introducir su clave.
- ***Downloader.*** Por sí solos no son dañinos; su peligro reside en que su misión es descargar archivos maliciosos y ejecutarlos en el equipo infectado.
- ***Proxy.*** Sirven para que el intruso utilice la red infectada como un servidor *proxy,* accediendo a la web a través del mismo y encubriendo su verdadera identidad, pues si se rastrea cualquier acción que realice siempre se llegará hasta el ordenador infectado y nunca hasta el del intruso.

Este tipo de *malware* es especialmente dañino por las consecuencias que puede ocasionar para los usuarios infectados. Por ello, la primera medida es extremar las precauciones a la hora de descargarse archivos (haciéndolo solo de webs oficiales o de confianza), si bien, hay que tener en cuenta que, en ocasiones, el software legítimo ha podido ser reemplazado por algún *malware,* por lo que es conveniente utilizar alguna herramienta que detecte modificaciones en el software y garantice su integridad, como la firma digital. También es importante no abrir ni descargarse los adjuntos de un correo electrónico si no se está muy seguro de lo que contienen. Del mismo modo, siempre es conveniente disponer de un antivirus actualizado y un *firewall,* además de tener el sistema operativo actualizado con todos los parches de seguridad.

Botnet

Este término se utiliza para designar a una red de ordenadores controlados por el atacante (denominados "ordenadores *zombies*") a través de la red. La finalidad de estas redes de ordenadores suele ser el envío de *spam* o la realización de ataques de denegación de servicio sobre servidores.

La mayoría de *botnets* se forman a partir de troyanos camuflados bajo la apariencia de un software legítimo.

Reemplazo de software legítimo

En septiembre de 2011 un atacante consiguió remplazar los clientes Torrent por un *malware,* con lo que se estima que unos 28 000 usuarios se descargaron *malware* pensando que era software legímo.

2.3 > Según las acciones que realiza

También podemos distinguir varios tipos de software malicioso atendiendo a las acciones que efectua. Siguiendo este criterio, se puede diferenciar entre entre los especímenes que realizan acciones dañinas sobre las víctimas y tienen un impacto medio o alto, y los que realizan acciones no dañinas y permiten a los usuarios trabajar normalmente con su equipo.

Software malicioso no dañino

No todo el software malicioso realiza acciones dañinas para las víctimas. Se consideran no dañinas acciones tales como mostrar publicidad no deseada a los usuarios, mostrar información falsa o asustar a los usuarios mediante algún tipo de broma. Es el denominado *grayware*. Los principales tipos son:

- ***Spyware***. El término *spyware* proviene de la unión de dos palabras inglesas: *spy* (espia) y *software*. Por tanto, es un tipo de software que trata de conseguir información del usuario. A veces únicamente se trata de conseguir estadísticas de navegación (tiempo que un usuario está en una página o páginas visitadas), pero cuando trata de obtener un beneficio de la información conseguida para realizar algúna acción dañina dejará de ser *grayware* para convertirse en *malware*.
- ***Adware*.** El término *adware* proviene de la unión de dos palabras inglesas: *ad* (abreviatura de anuncio) y *software*. Este *malware* muestra publicidad al usuario de forma intrusiva, por ejemplo, en forma de ventanas emergentes (*pop up*). Aunque este tipo de software no representa una amenaza directa para el usuario, suele ser frecuente su utilización para camuflar la acción de otro *malware*. Es frecuente encontrar este tipo de programas combinado con *spyware* para conseguir información y enviársela a terceras personas. Otras veces, al instalar un programa legítimo de pago, se ofrece la posibilidad de usarlo gratuitamente instalando adicionalmente un programa de *adware*.
- ***Hijacking*.** Cambian la configuración del navegador, por ejemplo, modificando la página de inicio por una página web, que contendrá anuncios o publicidad. También pueden modificar los enlaces de la carpeta *Favoritos* o añadir nuevas barras de herramientas. La finalidad de este *malware* suele ser aumentar la cantidad de visitas que recibe una página web.
- ***Jokes* o bromas.** Consisten en un software malicioso que no realiza ninguna acción dañina sobre el equipo infectado. En algunos casos, su acción se limita a hacer creer al usuario que se va a borrar el contenido del disco o a enviar información personal por la red, pero no lo hace. Este software se considera un tipo de *grayware* porque no realiza ninguna acción dañina sobre el equipo, salvo tratar de asustar al usuario. Es muy frecuente confundir este término con algún otro tipo de *malware* como *rogueware* o *ransomware*.
- **Bulos o *hoaxes*.** Son un tipo de *malware* que suele propagarse por correo electrónico y alerta a los usuarios de alguna amenaza no real, como, por ejemplo, un virus, una estafa, un fallo de seguridad, etc. Utilizan técnicas de ingeniería social para lograr que los usuarios reenvíen el correo a otras personas.

Vocabulario

Grayware: se utiliza este término para denominar a cualquier programa malicioso que realiza acciones molestas o no deseables pero sin representar una amenaza directa sobre la seguridad del sistema.

Keylogger en *smarthpones*

Taplogger es un *keylogger* que captura las pulsaciones realizadas en la pantalla de los dispositivos Android, con lo que un atacante podría conocer las claves de las aplicaciones.

Como cada persona pulsa la pantalla de una forma particular, el programa necesita "aprender" cómo pulsa la pantalla la víctima. Para ello, el *keylogger* está camuflado en un troyano que simula ser un juego que el usuario se descarga. Al interactuar el usuario con la pantalla, obtiene información relacionada con su forma de pulsar la pantalla, y es capaz de obtener las contraseñas tecleadas en otras aplicaciones.

Software malicioso dañino

Como hemos visto en el apartado anterior, aunque una parte del *malware* no se considera especialmente dañino y se limita a mostrar publicidad molesta o información falsa a los usuarios, otras variedades de software malicioso representan una amenaza real y atentan contra la seguridad de los equipos, realizando acciones como, por ejemplo, obtener información privada (claves de las cuentas de correo electrónico o de las tarjetas de crédito, modificar o borrar información almacenada en el disco duro o incluso, amenazar a los usuarios para obtener un beneficio económico). Aquí es donde los desarrolladores de *malware* muestran todo su ingenio para sacar provecho de las vulnerabilidades de los sistemas y las aplicaciones instaladas.

Algunas variedades de *malware* consideradas como dañinas son:

- ***Ransomware.*** Este término proviene de la unión de las palabras inglesas *ransom* (rescate) y *software*. Este tipo de *malware* cifra archivos importantes del disco duro para exigir el pago de dinero a cambio de la contraseña para descifrarlos.
- ***Rogueware.*** El término *rogueware* proviene de *rogue*, que en inglés significa falso, y *software.* Esta variedad de *malware* hace creer al usuario que su equipo está infectado por algún virus (sin estarlo realmente) y que la única forma de desinfectarlo es adquiriendo una solución antivirus, por la que habrá que pagar una cantidad de dinero. En ocasiones, se indica al usuario que la única forma de eliminar el virus ficticio del equipo es descargar una solución antivirus entrando en un enlace que se visualiza por pantalla. Al descargar ese supuesto antivirus, se podría estar dando el control total a un atacante remoto, que podría ver todo lo que visualiza por pantalla la víctima o darle acceso a su disco duro.
- ***Password stealer.*** Los navegadores son la herramienta más utilizada para crear cuentas de correo o de redes sociales. Existen algunos especímenes de *malware* que se aprovechan de esta situación y modifican el navegador para que capture y envíe las contraseñas cuando la víctima las introduce, obteniendo los datos de sesión.
- **Bombas lógicas.** Se trata de un *malware* que se pone en marcha cuando se cumple alguna condición, como que sea un día concreto, que se cambie algún dato en una base de datos o que se modifique un archivo del disco duro.
- ***Keylogger* y *backdoor*,** que hemos desarrollado en un apartado anterior.

Actividades propuestas

2·· Busca información sobre algún espécimen de *rootkit*. ¿Cómo se mantiene oculto al sistema?

3·· Atendiendo a los criterios expuestos en este epígrafe, indica si el siguiente *malware* es un virus, gusano o troyano: Jerusalen, Sasser, Gingermaster, Bifrost, Barrotes, ILoveYou.

Realiza una tabla comparativa, especificando cómo se propaga cada uno de estos especímenes y cuál es su nivel de peligrosidad.

3 >> Denegación de servicio

Imaginemos por un momento que en nuestro equipo hemos recibido un correo de un conocido que nos invita a ejecutar un archivo que contiene código malicioso. Como desconocemos este dato, ejecutamos el archivo y al hacerlo nuestro equipo deja de responder, por lo que la única solución es reiniciarlo. Estamos ante un ataque de denegación de servicio, y lo peor es que hemos sido nosotros quienes hemos realizado el ataque sobre nuestro propio equipo. Esta situación puede no ser muy crítica en nuestro equipo personal, pero pensemos por un momento que hemos ejecutado el archivo en un equipo que atiende miles de peticiones de usuarios por hora.

La denegación de servicio o DoS (*Denial of Service*) se define como la imposibilidad de acceder temporal o permanentemente a un recurso o servicio por parte de un usuario legítimo.

Los ataques de denegación de servicio tratan, pues, de conseguir una degradación de un servicio o recurso, ocasionando que deje de ser accesible para usuarios legítimos.

Existen diferentes tipos de ataques DoS, que se pueden clasificar atendiendo a diferentes criterios. Según el origen de los ataques de denegación de servicio efectuado, distinguimos los siguientes:

- **Ataques internos.** Son provocados por usuarios legítimos de la organización que, ya sea por desconocimiento o de forma intencionada, provocan la degradación de un recurso o servicio, impidiendo su acceso a otros usuarios y a ellos mismos. Se pueden producir de forma **casual** (por ejemplo, al conectar un horno microondas cerca de un punto de acceso inalámbrico, se produciría una denegación de servicio que afectaría a la disponibilidad del dispositivo, impidiendo cualquier acceso a la red por parte de usuarios legítimos) o **intencionada** (ejecutando una aplicación que impida el acceso a la información almacenada en el equipo).
- **Ataques externos.** En este caso, el atacante es una entidad ajena a la organización, es decir, se trata de usuarios ilegítimos que no deberían tener acceso a los equipos que hay en ella. En este tipo de ataques se aprovechan vulnerabilidades existentes en el sistema, como *bugs* de los programas o la no autenticación de los usuarios, para acceder a él. Por ejemplo, cuando un punto de acceso emite en el mismo canal que otro punto de acceso de otra red. Esta denegación de servicio también puede ocurrir en entornos domésticos entre nuestra red y la del vecino.

La mayoría de ataques de denegación de servicio en la actualidad se realiza mediante las redes informáticas, en las que los atacantes llevan a cabo su actividad sobre otros equipos o redes de forma remota.

Condenas por ataques de denegación de servicio

El primer caso de sentencia por ataque de denegación de servicio en España fue en 2006. Un usuario español utilizó en 2003 un gusano informático para lanzar un ataque de denegación de servicio (DoS) que afectó a cerca de tres millones de usuarios de varios proveedores de servicios de Internet. Fue condenado a dos años de prisión.

Actividades propuestas

4·· Busca información sobre el software malicioso Zbot. ¿Qué es? ¿Para qué se utiliza?

4 >> Publicidad y correo no deseado

Llamamos correo no deseado a todo correo no esperado por el usuario que lo recibe. Este correo puede resultar muy molesto porque se trata de correo no solicitado que en algunos casos se envía de forma masiva, llegando a saturar la bandeja de entrada de nuestra cuenta de correo de información no deseada.

Las intenciones que hay detrás de estos correos son muy variadas. En algunas ocasiones, usuarios malintencionados envían correo no deseado a una gran cantidad de víctimas para propagar software malicioso que puede llegar a darle el control de la máquina al atacante. En otras ocasiones, contienen bromas o mentiras que los autores envían a un conjunto de usuarios con la intención de conseguir repercusión o notoriedad. No obstante, es muy frecuente la utilización de correo electrónico con intenciones comerciales o publicitarias.

El correo electrónico es una forma de comunicación rápida, gratuita y fácil de utilizar, por lo que muchas empresas lo utilizan masivamente para darse a conocer al público o presentar algún producto, constituyendo una nueva variedad de correo no deseado, el correo basura o *spam.*

Con frecuencia, se confunden los términos correo no deseado y *spam*, llegando a utilizarse indistintamente, pero es conveniente distinguirlos correctamente. Ambos están integrados por mensajes enviados al destinatario sin su consetimiento, pero aplicamos el término *spam* para el correo no deseado que tiene fines publicitarios o económicos.

Para facilitar el trabajo de los usuarios, algunos antivirus y servidores de correo ofrecen un servicio de detección de correo no deseado, redirigiendo este tráfico a una carpeta especial o eliminándolo directamente. Aunque estas herramientas suelen detectar correctamente el *spam*, el resto de correo no deseado es más difícil de distinguir porque en estos mensajes no se está vendiendo o anunciando ningún artículo. Es frecuente que los servidores de correo identifiquen como correo no deseado a correos enviados de forma legítima, por lo que se recomienda revisar la bandeja de correo no deseado regularmente.

En España, el correo electrónico no deseado está prohibido por la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE).** El artículo 21 de esta norma prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico que no hubieran sido solicitadas o autorizadas por sus destinatarios. El correo electrónico publicitario deberá incluir una dirección electrónica válida donde pueda exigirse el cese del envío de más comunicaciones.

Prevención y lucha contra el *spam*

La *Guía para la lucha contra el spam*, publicada por la Agencia Española de Protección de Datos, contiene unas recomendaciones muy útiles para reducir la recepción del *spam*. Esta guía puede descargarse gratuitamente desde la página web de la Agencia: www.aepd.es.

Sanciones en materia de correo no deseado

Las sanciones previstas por la Ley 34/2002 para el supuesto de envíos de correo no deseados pueden ser de hasta los 600 000 €.

Actividades propuestas

5·· Explica las diferencias que hay entre correo no deseado y *spam*. ¿Para qué se utiliza el *spam*?

6·· ¿Cómo pueden las empresas obtener beneficios a través del envío de correos electrónicos no deseados?

5 >> Ingeniería social. Fraudes informáticos

La mayor parte de las veces, los piratas informáticos no necesitan desarrollar complejos programas para conseguir las contraseñas o los datos bancarios de los usuarios, ya que son estos los que facilitan esta información a los atacantes. La ingeniería social es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras.

Los argumentos utilizados son muy convincentes y conviene estar muy alerta. Para extender estas estafas o fraudes, los atacantes utilizan una gran variedad de herramientas o técnicas. Aunque el correo electrónico es el método más empleado, también se suelen utilizar mensajes de texto, redes sociales o llamadas de teléfono.

Existe una gran variedad de técnicas destinadas a engañar a los usuarios: *phishing, vishing, smishing, grooming, ciber-bulling,* cadenas de correos o correos millonarios. Podemos dividirlos en las siguientes categorías.

5.1 > Suplantación de la identidad

La suplantación de identidad es un tipo de fraude que consiste en hacerse pasar por otra persona. Las tecnologías de la información han abierto nuevas formas de comunicarse de las que han sabido sacar provecho algunos atacantes para obtener las credenciales de otros usuarios y suplantarlos.

Phishing

En esta técnica, el atacante suele crear una página web falsa aparentemente idéntica a la de una empresa que requiere autenticación, por ejemplo, un banco. Cuando el cliente introduce datos confidenciales para entrar en la zona privada, como su contraseña, la numeración de la tarjeta de crédito o el PIN, el atacante obtiene la información que necesita para suplantar a la víctima. Para que la víctima no desconfíe, se suele mostrar un mensaje informando de que el servicio no está disponible temporalmente por algún motivo.

Para conseguir que las víctimas visiten estas páginas web falsas, los atacantes utilizan técnicas como el ***pharming***. También es frecuente el envío de correos haciéndose pasar por una empresa (como un banco) un organismo público, etc., invitando a los usuarios a visitar un enlace para realizar alguna acción.

El *pharming* es una técnica de fraude informático que suplanta el sistema de resolución de nombres de dominio (DNS), de manera que las peticiones a una página web legítima son redirigidas a una página web falsa para que, cuando la víctima introduzca una determinada dirección de Internet en su navegador, acceda a la página web del atacante. De este modo, el usuario puede, por ejemplo, llegar a introducir las claves de entidad bancaria pensando que se encuentra en la web del banco.

Existen diferentes técnicas de suplantación del DNS de una máquina: modificación del archivo *hosts* de la máquina, modificación de información en el servidor, etc.

¿Es delito suplantar la identidad en las redes sociales?

Existen varios supuestos distintos:

- Se crea un perfil falso pero no se utiliza información personal del suplantado ni se publica ninguna imagen. Solo se puede notificar a la red social para que se elimine el perfil.
- Se crea un perfil falso y se utiliza información personal del suplantado o una fotografía suya. Se produce un delito de usurpación de la identidad y podría ser penado con hasta tres años de cárcel.
- Se accede al servicio de un usuario y se hace pasar por él. Se infringe la ley porque se produce un delito contra la usurpación de la identidad.

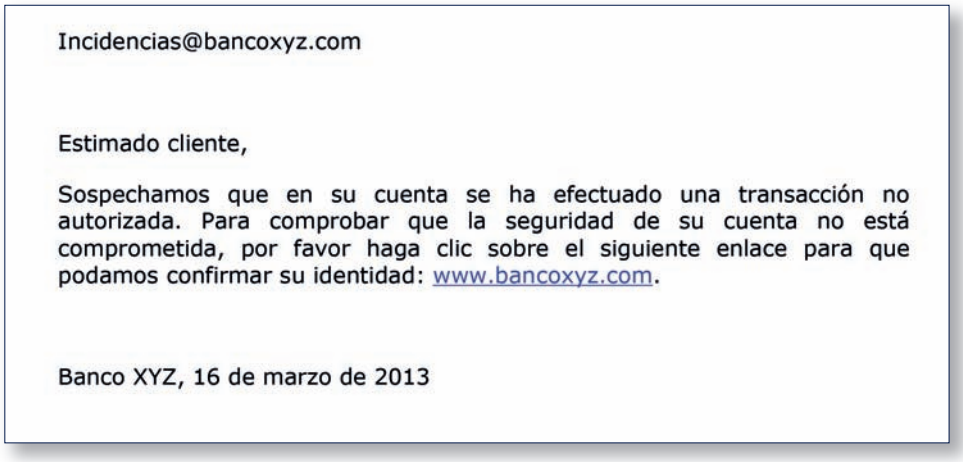
Ejemplos

Phishing

Veamos un ejemplo de *phishing* paso a paso.

Todo comienza con la recepción por parte de la víctima de un mensaje de correo electrónico que simula provenir de una empresa o institución real (banco, organismo público, etc.). Normalmente, si se utiliza un servicio de correo gratuito (Yahoo, Gmail, etc.), los filtros *antispam* enviarán este mensaje a la bandeja de *Correo electrónico no deseado*, pero puede que se escape de estos filtros y aparezca en la bandeja de *Entrada*, o bien que el usuario lo abra desde la carpeta de *spam*.

El mensaje tendrá un texto en el que se informa de alguna eventualidad que se ha producido con un cuenta bancaria, una tarjeta de crédito, multas de tráfico, etc., e indica a la víctima que haga clic en un enlace incluido para acudir a la página web de la empresa o institución para realizar los trámites que le indican. El mensaje puede ser como el siguiente:


Incidencias@bancoxyz.com

Estimado cliente,

Sospechamos que en su cuenta se ha efectuado una transacción no autorizada. Para comprobar que la seguridad de su cuenta no está comprometida, por favor haga clic sobre el siguiente enlace para que podamos confirmar su identidad: www.bancoxyz.com.

Banco XYZ, 16 de marzo de 2013

El usuario hace clic en ese enlace y es redirigido a una web del atacante que simula ser la página genuina. Es muy usual que, si se utiliza un navegador actualizado, aparezca una pantalla de advertencia que indica que se ha comprobado que esa web es falsa y avisa de las posibles consecuencias de seguir adelante.

Pero puede suceder que el usuario no tenga instalado un navegador actualizado, que decida ignorar la advertencia o que la web fraudulenta aún no haya sido reportada como tal. En estos casos, accederá a una página que visualmente simula ser la legítima y en la que se pide a la víctima que introduzca determinados datos necesarios para que los estafadores consigan su propósito (cuenta bancaria, número de PIN, número de tarjeta, etc.).

Una vez conseguidos estos datos, los atacantes podrían disponer de todo el saldo que existe en esas cuentas.

Vishing

Es una técnica muy similar al *phising,* pero que utiliza como vehículo el protocolo de voz sobre IP (**VoIP**). La víctima recibe una llamada en la que se le indica que debe teclear en su terminal un determinado dato (el código secreto del banco, el número de su tarjeta, el PIN, etc.) para realizar alguna acción.

Otras veces se le pide al destinatario que llame a un teléfono para realizar alguna gestión (a veces para dar mayor credibilidad, los estafadores contratan un número 901 o 902). Cuando llama, le contesta una voz grabada que parece provenir de la empresa a la que está llamando que le indica que debe verificar determinados datos (número de cuenta, número de la tarjeta, PIN, fecha de expiración de la tarjeta, etc.).

SMiShing

Se engaña a a las víctimas a través del envío de mensajes SMS a sus teléfonos móviles para conseguir sus contraseñas. En ellos se les pide que accedan a una determinada página web para, por ejemplo, desbloquear su tarjeta de crédito. Cuando acceden a la misma, se les pide que completen determinados datos personales, o bien que se descarguen un determinado archivo, que suele ser un troyano.

Grooming

Consiste en el acoso a menores por parte de un adulto que trata de ganarse su confianza o lo coacciona de alguna forma para que realice alguna acción de tipo sexual.

5.2 > Cadenas de correos

Las cadenas de correos son mensajes en los que se incita a su destinatario a difundirlos al mayor número de personas posible bajo promesas o amenazas, con el ánimo de conseguir direcciones de correo.

Los argumentos utilizados por parte del emisor del mensaje son muy variados, pero todos persiguen el mismo objetivo: conseguir que el destinatario acepte formar parte del juego o de la trama planteada y que reenvíe el mensaje al mayor número de usuarios posibles para, de este modo, aumentar la difusión del mismo.

- Es muy corriente recibir correos que contienen deseos de paz, amor, felicidad, etc., en los que al final se recomienda el reenvío a tus amigos o de lo contrario sucederán grandes desgracias.
- En otros mensajes se indica que se van a borrar cuentas de correo o que determinadas aplicaciones gratuitas serán de pago si no renviamos el mensaje a nuestros contactos.
- También suele ser frecuente recibir mensajes con alguna noticia falsa para alarmar a los usuarios, como la comunicación de que el Gobierno va a suprimir plazas de trabajo si no se actúa inmediatamente y así conseguir que sean los propios usuarios quienes se encarguen de la divulgación de esta información.

Detrás de estos correos suele haber una persona u organización interesada en obtener direcciones de correo válidas para posteriormente enviarles *spam*.

Ejemplos

¿Cómo se consiguen las direcciones de correo en las cadenas de mensajes?

Los correos electrónicos que se transmiten en cadena pueden llegar a propagarse en progresión aritmética o geométrica. Imaginemos que una persona quiere obtener direcciones válidas de correo que utilizar para enviarles *spam* o con otros fines.

El primer paso será redactar un mensaje con una noticia inventada pero atractiva y enviarla, por ejemplo a diez direcciones de correo. En ese mensaje se suele decir que si no se reenvía en un determinado plazo de tiempo a un determinado número de personas, al destinatario le ocurrirá alguna desgracia o expondrá a sus familiares y amigos a unas consecuencias negativas. Supongamos que el número de reenvíos que se le dice que debe hacer es de diez.

De esos los diez destinatarios iniciales, no todos reenviarán el correo, pero supongamos que dos o tres personas sí lo reenvían a otros diez destinatarios, lo cual normalmente harán sin borrar la lista de remitentes del correo. En este momento, el mensaje inicial se ha convertido en otro, que contiene unas 20 direcciones de correo válidas.

Si ahora cuatro o cinco usuarios reenvían el mensaje a otros diez conocidos, cada mensaje contendrá unas 30 direcciones de correo válidas. Y así sucesivamente.

Tal como se describe en la teoría de los seis grados de separación, tarde o temprano el creador del correo original lo volverá a recibir con miles o millones de direcciones de correo.

Teoría de los seis grados de separación

La teoría de los seis grados de separación fue formulada en 1930 por el escritor húngaro Frigyes Karinthy y sostiene que cualquier persona del planeta está conectada con cualquiera otra por medio de una cadena de conocidos de no más de cinco personas (seis relaciones).

En noviembre de 2011 la BBC publicó una noticia en la que se indicaba que, gracias a las redes sociales, se había reducido esta cifra a 3,74.

Para evitar contribuir a propagar estos fraudes informáticos, la recomendación más importante es romper estas cadenas de correos no reenviándolos sin haber comprobado antes su veracidad.

En el caso de que se decida reenviar algún mensaje de correo electrónico de forma masiva, las direcciones de los destinatarios se deben insertar en el campo *Copia oculta* (CCO) en lugar en en *Destinatario*. Con esto los distintos destinatarios no conocerán el resto de direcciones a las que va dirigido el correo. Otra recomendación que debemos tener en cuenta es revisar el contenido que vamos a reenviar, borrando las direcciones de correo procedentes de reenvíos anteriores.

5.3 > Correos millonarios

Otra forma de estafa informática muy común es la denominada “estafa nigeriana” o “carta nigeriana”, que consiste en el envío de correos prometiendo a los usuarios que pueden hacerse ricos fácilmente. Recibe ese nombre porque, en un principio, eran mensajes que simulaban proceder de Nigeria y que llevaban un texto como el siguiente: “Soy una persona muy rica en Nigeria, pero necesito trasladar una cantidad de dinero al extranjero. A cambio le daré un porcentaje sobre la cantidad transferida, pero necesito un número de cuenta en un país europeo para hacer la transferencia. ¿Podría pasarme su número de cuenta?”.

Actualmente, los reclamos son muy diversos: desde un millonario que ha fallecido sin dejar herederos y de cuya herencia las víctimas recibirán una parte si pagan una cantidad de dinero, hasta un premio de lotería que se ha ganado (sin haber participado), pasando por el envío de dinero a un familiar que está en el extranjero, etc.

Actividades propuestas

7·· Lee el siguiente artículo y responde a las preguntas que se hacen a continuación del mismo.

El ataque a la RSA se produjo a través de un *zero day* en Flash

Según la RSA, el atacante envió dos correos en un periodo de dos días a dos pequeños grupos de empleados. RSA concreta que "no se consideraría a estos usuarios particularmente de perfil alto u objetivos valiosos". ¿Quiere decir con esto que se encontraban menos protegidos que el resto? Dentro de una organización de este calibre, todos los usuarios con acceso a la red deberían ser considerados de alto riesgo y protegidos por igual. Se les envió un correo con el asunto "2011 Recruitment Plan" con un Excel del mismo nombre adjunto. Uno de los usuarios, incluso, rescató el *email* de la carpeta de correo basura. Según RSA, es porque el correo estaba muy bien construido. Una buena política de seguridad debería prohibir y entrenar expresamente a los usuarios para no abrir archivos no solicitados, sin excusas.

El Excel contenía en su interior un fallo no conocido hasta el momento en Flash que permitía la ejecución de código. De hecho, Adobe anunció el 14 de marzo que sabía que una vulnerabilidad desconocida estaba siendo aprovechada para atacar sistemas. Si bien no hacía mención explícita a RSA, parece que la vulnerabilidad apareció a causa de este ataque. Adobe ya lo ha solucionado con un parche emitido fuera de su ciclo habitual.

De esto se deduce que, aunque RSA hubiera mantenido todo su software actualizado, el atacante hubiese igualmente conseguido ejecutar código. En estos casos, es en los que se echa de menos el uso de herramientas como DEP, ASLR o cualquier otro software que prevenga los desbordamientos de memoria. Es irrelevante el uso de Office, LibreOffice o Flash... si los atacantes han tenido acceso a un *0-day* en Flash, podrían haberlo conseguido de cualquier otro programa.

Una vez dentro

Luego los atacantes instalaron una variante del conocido RAT (herramienta de administración remota) Poison Ivy y crearon una conexión inversa hacia un servidor propio del atacante. RSA afirma que "esto lo hace más difícil de detectar", pero no es del todo cierto. Lo que hace más difícil de detectar estas conexiones es el hecho de que suelen estar cifradas, ofuscadas y en puertos estándares que no levantan sospechas, no el hecho en sí de que sean "inversas". En realidad, esto está asumido como estándar. La opción contraria, establecer una conexión desde fuera a la máquina infectada, está descartada desde un primer momento en la mayoría de los escenarios y es una opción que los atacantes serios ni siquiera contemplarían. En este punto hubiesen sido necesarios inspectores de tráfico e IDS, aunque es cierto que el nivel de éxito de esta medida podría ser menor si los atacantes realmente se lo proponen.

El atacante más tarde transfirió muchos ficheros RAR protegidos por contraseña desde el servidor de la RSA hacia un tercero externo y comprometido. Descargó la información, la borró de ese servidor... y se quedó con ella.

Fuente: Sergio de los Santos. www.hispasec.com

a) Investiga qué es la RSA y a qué se dedica.

b) ¿De qué tipo de *malware* habla el artículo? ¿Cómo pudo este *malware* infectar los equipos?

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿Qué diferencias hay entre virus y *malware*?

2·· Explica qué tipos de *malware* existen atendiendo a su forma de propagación.

3·· Razona cómo puede una empresa beneficiarse mediante el envío de correo electrónico no deseado. ¿Qué podemos hacer para evitarlo?

4·· ¿Cómo puede un atacante suplantar la identidad de una víctima en una red social?

5·· ¿Un programa que espía las páginas web que visita un equipo está considerado como un software dañino?

6·· ¿Puede un estafador falsificar un correo para que parezca proceder de otra persona? ¿Qué nombre recibe este tipo de estafa?

7·· ¿En qué se diferencia el *spyware* del *adware*?

.: APLICACIÓN :.

1·· Hemos recibido un correo electrónico del banco en el que nos indican que la cuenta está a cero, por lo que tenemos que comprobar si ha habido algún uso indebido. A continuación nos piden la contraseña y el usuario para que ellos puedan entrar al sistema y comprobar que todo funciona correctamente.

¿Qué debemos hacer en este caso?

2·· Has decidido comprarte un ordenador personal, pero no dispones de mucho dinero ahorrado, por lo que te estás planteando adquirir uno de segunda mano. Después de investigar en varias páginas web, has encontrado un auténtico chollo en una página web de anuncios de particulares. Te pones en contacto con el anunciante, que te indica que es un regalo que no puede devolver, pero que quiere deshacerse de él porque no lo utiliza. A continuación avisa de que debes hacer el pago antes de realizar el envío del equipo y que, cuando lo recibas, podrás verlo y decidir si quieres quedártelo o devolverlo, en cuyo caso te retornará el dinero pagado. Te dice que el envío se realizará a través de una empresa de la que no has oído hablar nunca, pero en un correo electrónico hay un enlace a la página web de la empresa transportista.

¿Puedes estar seguro de la veracidad de este anuncio? ¿Por qué?

3·· Tienes un teléfono móvil que quieres vender por un portal de venta de artículos como eBay. Has tenido suerte y alguien ha pagado una cantidad muy superior de la esperada. A continuación te envían un correo para pedirte los datos de la cuenta de PayPal, que es un método muy utilizado en estas páginas web y que ofrece seguridad al comprador y al vendedor. Lo normal suele ser que el comprador rellene los datos necesarios para realizar el pago por PayPal al realizar la compra, pero en este caso te indican que tienen un problema al hacerlo y que necesitan los datos de la cuenta para efectuar el pago. Después de darle los datos, recibes un correo de confirmación del pago, que parece provenir de PayPal, donde se te indica que, por seguridad, el pago será transferido al realizar el envío del teléfono.

¿Puedes estar siendo víctima de una estafa? ¿Por qué?

4·· Has contratado un servicio de Internet a través de un proveedor y has cambiado la contraseña del punto de acceso inalámbrico para que no puedan utilizarlo intrusos. Como el punto de acceso es un aparato con algunos cables, decides ocultarlo detrás de la televisión, en un hueco que tiene el mueble. Después de unos días ves que, en ocasiones, el punto de acceso no funciona correctamente y decides llamar al proveedor de servicios para estudiar si existe algún problema, pero todo parece estar en orden.

¿Qué puede ocurrir? ¿Cómo puedes solucionarlo?

Caso final 1

Instalación de una herramienta *antimalware* en Windows

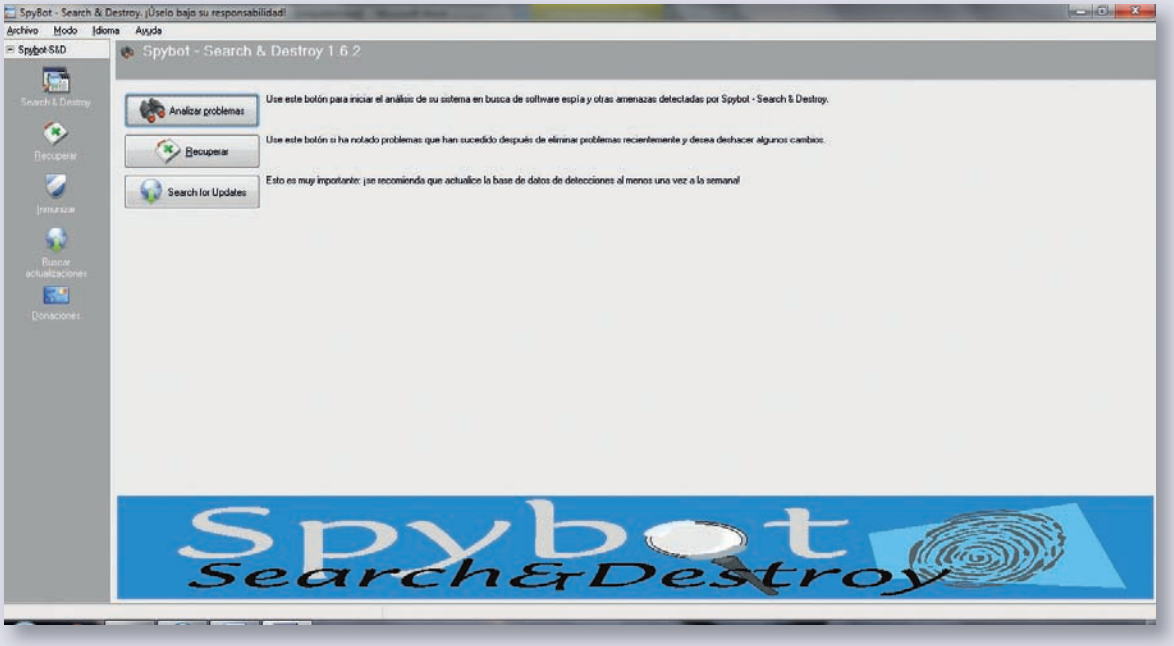
•• Tienes un ordenador que funciona bajo el sistema operativo Windows y quieres instalar una herramienta que detecte si está infectado con alguna variedad de *spyware* y que, además, lo inmunice contra futuras infecciones y te informe de cualquier modificación sobre el registro de Windows para que seas consciente de si un programa intenta modificarlo para realizar algún tipo de cambio.

¿Cómo deberías llevar a cabo la instalación de esta herramienta? ¿Cómo detecta el *malware?*

Solución •• Existen múltiples herramientas *antimalware* para entornos Windows; como ejemplo, podrías utilizar Spybot - Search & Destroy. Se trata de una herramienta que permite detectar infecciones por *spyware*, así como proteger el equipo de futuras amenazas.

Se puede descargar desde la página web www.safer-networking.org, que pone a disposición de los usuarios una versión profesional, de pago, para usos corporativos y otra gratuita para uso personal (aunque se puede donar, voluntariamente, una cantidad de dinero para permitir que el producto siga desarrollándose en el futuro). En este caso, descárgate la versión gratuita.

Una vez descargado el programa, ejecútalo y te saldrá la pantalla de bienvenida:

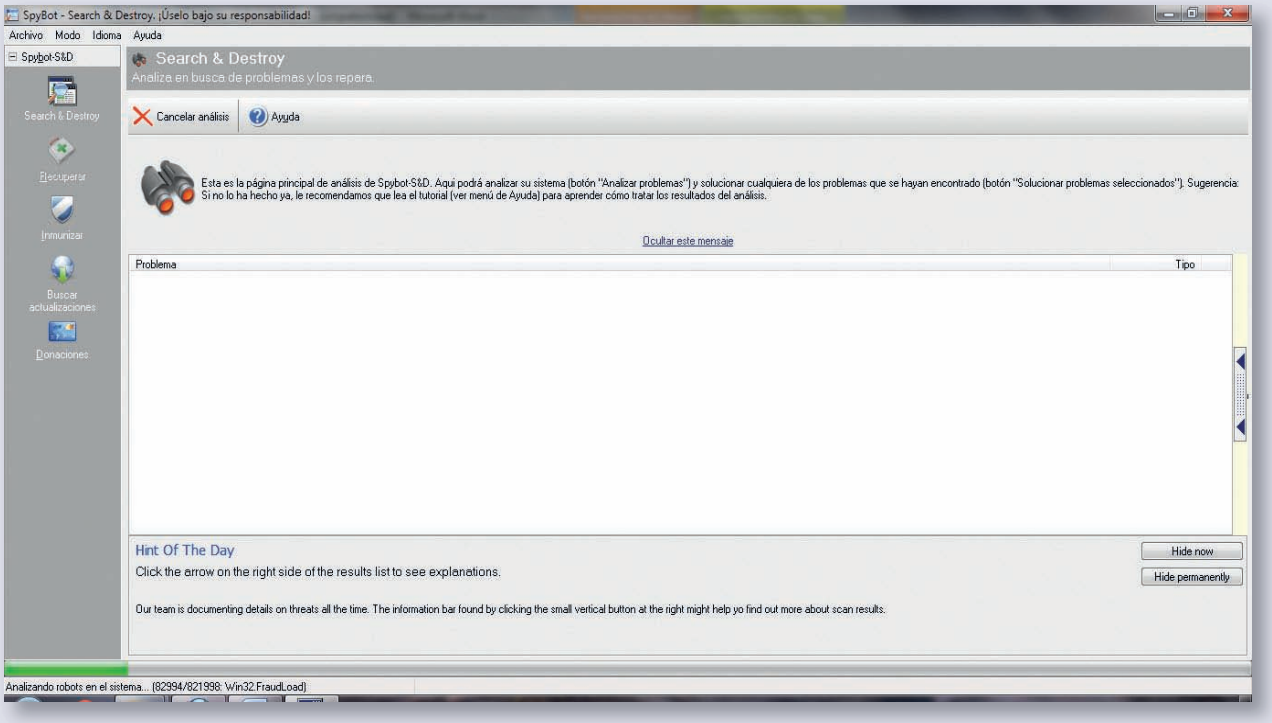


Cuando lo hayas instalado, el primer paso será comprobar si hay algún software malicioso instalado en el equipo; para ello debes hacer clic en el primer botón: *Analizar problemas*.

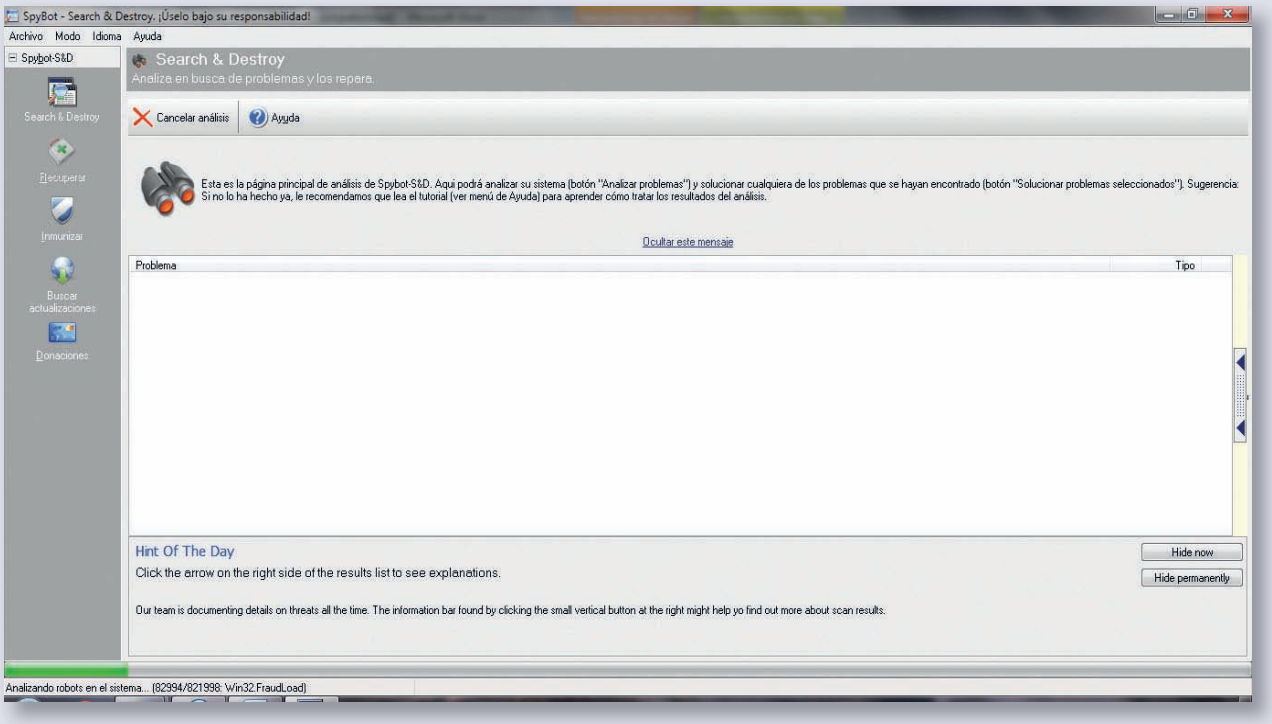
El programa escaneará el sistema y, en primer lugar, detectará los archivos temporales existentes en el directorio de archivos temporales de Windows. Es conveniente borrar regularmente el contenido de este directorio, pues puede llegar a ocupar mucho espacio en el disco y ralentizar el funcionamiento del sistema.

1

A continuación, el programa mostrará la pantalla principal de análisis en la que te informará de cualquier amenaza existente en tu equipo. En la parte inferior podrás ver el progreso del análisis.

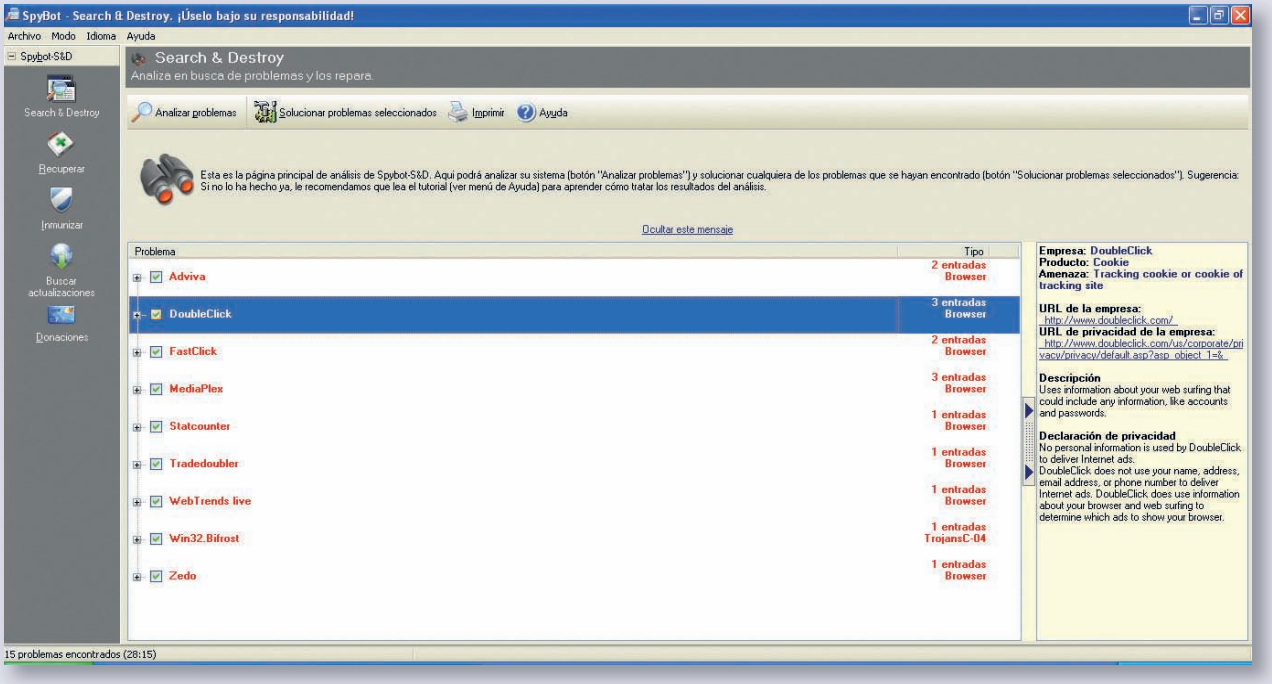


Cuando finaliza el análisis, se muestra información sobre las amenazas detectadas.

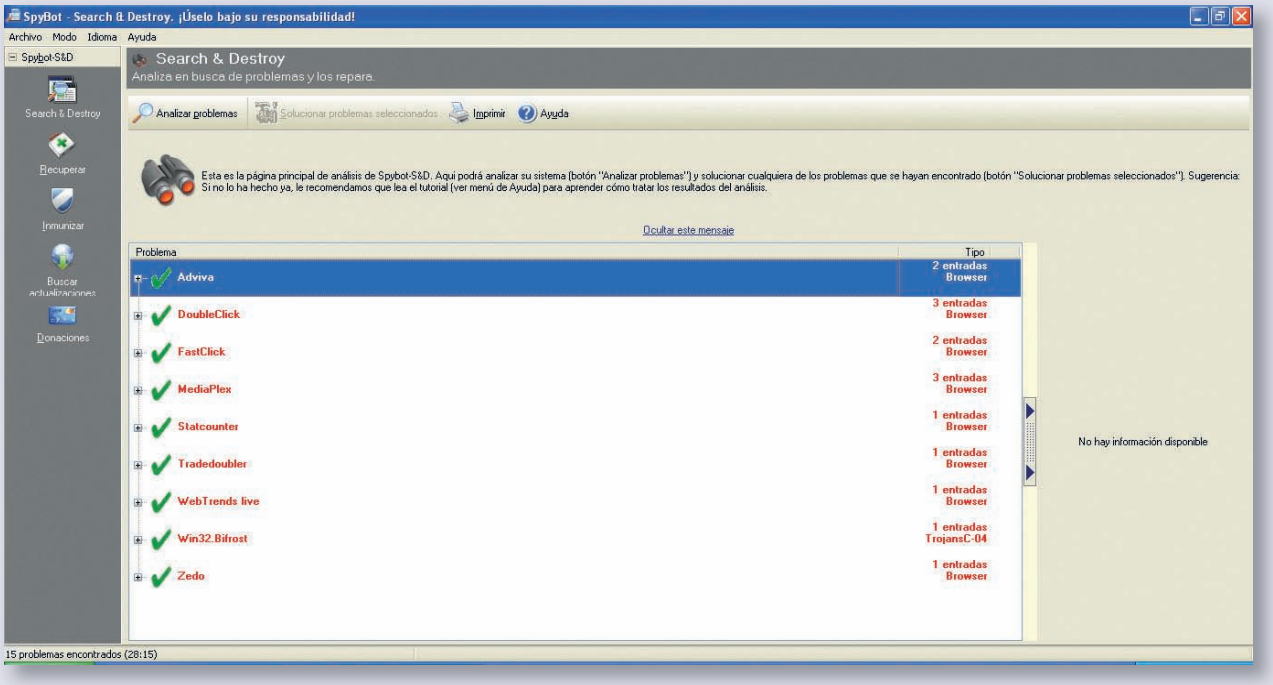


1

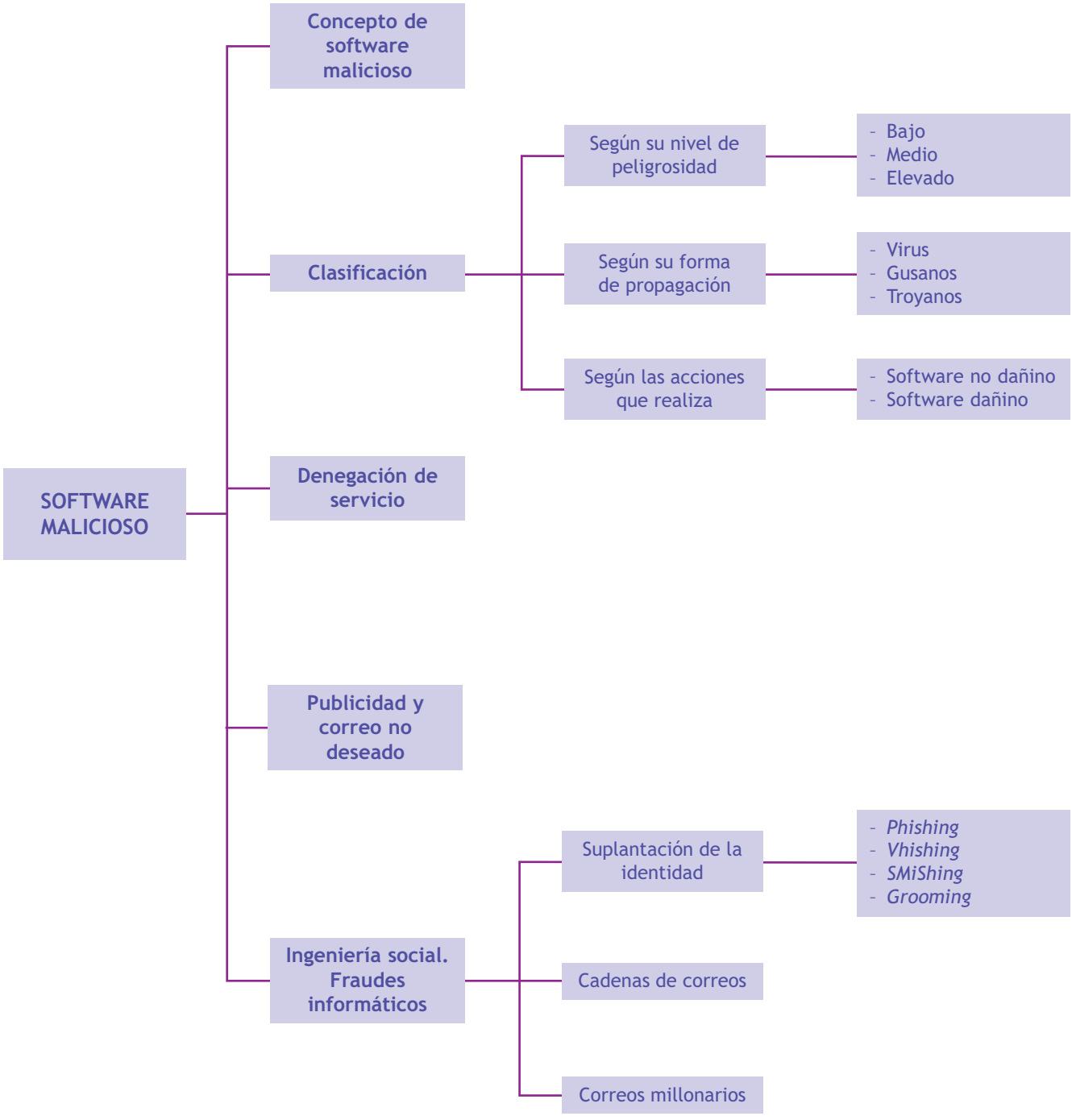
Si haces clic sobre una de ellas, podrás ver información de la amenaza en la parte derecha. En este caso, vemos que la amenaza denominada DoubleClick hace referencia a una *cookie* de seguimiento que puede capturar información introducida en un navegador, como por ejemplo nombres de usuario y contraseñas.



Si haces clic en la opción *Solucionar problemas seleccionados*, se intentará eliminar este *malware* y se mostrará una ventana informativa indicando si se ha podido llevar a cabo la eliminación.



Ideas clave


SOFTWARE MALICIOSO
Concepto de software malicioso
Clasificación
Según su nivel de peligrosidad
- Bajo
- Medio
- Elevado
Según su forma de propagación
- Virus
- Gusanos
- Troyanos
Según las acciones que realiza
- Software no dañino
- Software dañino
Denegación de servicio
Publicidad y correo no deseado
Ingeniería social. Fraudes informáticos
Suplantación de la identidad
- *Phishing*
- *Vhishing*
- *SMiShing*
- *Grooming*
Cadenas de correos
Correos millonarios

Los peligros del *pharming*

Se ha dado en llamar *pharming* al ataque que consiste en modificar la resolución de dominios a través del archivo *hosts*. El sistema operativo acude primero al archivo *hosts* a intentar resolver un dominio. Luego al primer servidor DNS configurado. Si el primer servidor DNS está caído (y solo si está caído, no porque no encuentre el dominio en él... esto es algo que muchos confunden) acude al segundo servidor DNS a intentar resolver el dominio.

La idea es crear pequeños programas que modifiquen el archivo *hosts*. El usuario infectado intentará ingresar en su banco y, como el sistema le lleva hacia otra dirección IP, acabará en una especie de *phishing* donde el atacante capturará sus credenciales.

Variantes

En principio, es un ataque muy simple. La víctima ejecuta un troyano y su archivo *hosts* es modificado, por ejemplo, con esta entrada: 6.6.6.6 www.banco.com

Cuando el usuario acuda a banco.com, en realidad irá a 6.6.6.6 donde le espera una página copia de banco. ¿Qué ocurre cuando la dirección IP 6.6.6.6 cae? La víctima escribirá en su navegador www.banco.com, acudirá a 6.6.6.6 y no irá a parar a ningún sitio.

Descargar el archivo *hosts*

Los atacantes pronto se dieron cuenta de que sería mucho más efectivo que la asociación 6.6.6.6 con www.banco.com fuese, de alguna forma, dinámica. Que el propio troyano controlara hacia dónde resuelve el dominio para cuando la dirección IP no estuviese disponible. Así que comenzaron a programar un sistema por el que, en vez de integrar directamente en su código la dirección IP donde se aloja la copia, el *malware* acude a una URL que controlan los atacantes y descarga un archivo *hosts* que sustituye al original.

En ese archivo *hosts*, van actualizando la asociación IP/dominio. Así, si cae la dirección IP, pueden colgar en la url datos actualizados para que los nuevos infectados acudan. Es como un pequeño sistema de "nuevas versiones" del *malware*.

Instalar un servidor web en la víctima

El atacante, cansado de que se le echen abajo las direcciones IP donde alojan sus *phishings*, decide simplemente que el servidor sea la propia víctima. El troyano instala un pequeño servidor web y pone a escuchar en el puerto 80. Luego modifica el archivo *hosts* con esta entrada: 127.0.0.1 www.banco.com

La solución contra el *pharming*

Resulta curioso que existan ya dos soluciones casi definitivas contra el *pharming* y todavía sea tan popular. Son muy sencillas:

- Comprobar los certificados de las páginas a las que se accede. Si los usuarios comprobasen que el sitio al que acceden está bajo SSL y además la ruta de certificación es válida, este tipo de troyanos no tendrían éxito.
- Protección del archivo *hosts*. Modificar los permisos del archivo *hosts* para que no pueda ser modificado previene el *pharming*.

Fuente: Sergio de los Santos. Extracto de artículo publicado el 11/01/2012 en www.hispasec.com

Actividades

1·· Debate con tus compañeros sobre las técnicas de *pharming* y las recomendaciones que se ofrecen en el texto como medida de protección frente al mismo. ¿Os parecen sencillas de cumplir? ¿Se cumplen a menudo?

unidad 7

Medidas de protección contra el *malware*

SUMARIO

- Medidas preventivas
- Medidas paliativas
- Antivirus personales
- Antivirus corporativos
- Protección ante *malware* en correo electrónico

OBJETIVOS

- Conocer cómo se puede proteger un equipo para evitar infecciones de *malware*.
- Aprender a actuar ante una infección por *malware*.
- Diferenciar entre antivirus personales y corporativos.
- Aprender a evitar infecciones en correos corporativos.

1 >> Medidas de protección contra el software malicioso

Como se ha visto en unidades anteriores, existe una gran variedad de especímenes de *malware* diseñados con la finalidad de realizar acciones maliciosas sobre algún dispositivo electrónico. Atrás quedaron los tiempos en los que el *malware* solo afectaba a los equipos informáticos, y en la actualidad podemos encontrar especímenes que aprovechan vulnerabilidades que presentan los dispositivos móviles, las *tablets* o incluso televisores de última generación que utilizan Internet para ofrecer algún servicio a los usuarios.

Muchas personas son conscientes de la importancia de utilizar algún mecanismo que les proteja contra las acciones de personas no autorizadas y, aunque muchos conocen la existencia de los antivirus y tienen uno instalado en sus equipos, pocos son conscientes de que es vital mantenerlos actualizados o de que existen otros mecanismos que contribuyen a mejorar la seguridad.

En efecto, muchos usuarios piensan que con tener el navegador actualizado es suficiente pero no es así, ya que los *plugins* y complementos que utilizan se deben actualizar de forma manual. Por ejemplo, solo un porcentaje mínimo de los usuarios aplica actualizaciones y parches de seguridad de Java en los tres primeros meses de la aplicación y alrededor del 60% de los usuarios nunca tiene la versión de Java actualizada a la última versión.

Por lo tanto, hay que establecer mecanismos que protejan a los equipos informáticos contra los efectos del *malware*. En la actualidad, existe una gran variedad de herramientas desarrolladas con esta finalidad y conviene conocer cómo funcionan y en qué casos se deben utilizar.

Según su momento de actuación, distinguimos dos grupos de medidas contra el *malware:* **medidas preventivas**, que tratan de evitar infecciones por *malware* y **medidas paliativas o correctoras,** que minimizan el impacto producido por una infección.

1.1 > Medidas preventivas contra el *malware*

Las medidas preventivas contra el *malware* (también llamadas medidas de seguridad activa) están constituidas por el conjunto de acciones que los usuarios realizan para evitar infecciones por *malware.* Si bien no es posible que un equipo esté protegido frente al 100% del *malware*, proporcionan un nivel razonable de seguridad.

Cuando hablamos de seguridad activa en general, estamos hablando de técnicas que detectan y previenen un incidente de seguridad. Además, este término abarca no solo a las medidas que previenen contra incidentes de seguridad relacionados con el *malware*, sino también a medidas que previenen contra otras amenazas como accesos no autorizados o la utilización inadecuada de recursos del sistema.

En este punto nos ocuparemos de las herramientas que evitan que los sistemas se infecten con *malware* como antivirus, *antispyware*, *antirootkit*, etc. y que se suelen llamar **herramientas *antimalware*.**

Suites de seguridad

Un antivirus es, tal vez, la medida de protección más conocida entre los usuarios. Se trata de un programa desarrollado con una doble finalidad: por un lado, permite evitar infecciones por *malware* y, por otro, sirve para desinfectar los equipos afectados. Para ello, detecta ataques realizados por programas maliciosos y, en muchos casos, los elimina. La aparición de nuevas amenazas ha hecho que los antivirus hayan evolucionado y sean capaces de reconocer otros tipos de *malware,* como *spyware, rootkits*, etc. y han pasado a llamarse ***suites* de seguridad**.

Dado que una *suite* de seguridad es una suma de varios programas de seguridad, suele ofrecer: antivirus, *antispyware, antirootkit, antiphishing, antispam,* cortafuegos, herramientas de control y protección al navegar como filtros de contenido o control parental, etc.

Actualmente se pueden encontrar algunas soluciones de seguridad que ofrecen, además de estos contenidos, otros complementarios como pueden ser el cifrado de datos, la creación de copias de seguridad, servicios de virtualización, etc. Para bastantes usuarios, todos estos servicios adicionales pueden resultar útiles, pues les permiten centralizar muchas tareas en un solo software, si bien seguramente los usuarios avanzados prefieran utilizar herramientas específicas para llevar a cabo estas tareas.

Además, cada vez más, las soluciones antivirus se apoyan en los servicios en la nube. Cuando la *suite* de seguridad detecta una amenaza, envía un informe a los servidores de la empresa creadora del antivirus. De este modo, todos los equipos que tengan instalada esa solución, cuando consulten la nube, podrán ver esa amenaza. Con ello, por un lado, las actualizaciones de amenazas y firmas de *malware* pueden ser muy rápidas y, por otro, se pueden instalar en la nube ficheros con las firmas y agilizar el funcionamiento de los equipos que utilicen el servicio. El inconveniente que presenta esta modalidad es que, lógicamente, cuando los equipos no están conectados a Internet y no pueden acceder a la nube, su efectividad se reduce enormemente.

Estos programas combaten el *malware* de dos formas:

- **Protegiendo** el equipo, en tiempo real, contra la instalación de *malware*, escaneando todos los datos procedentes de la red en busca de *malware* y bloqueando todo lo que suponga una amenaza.
- **Detectando y eliminando *malware*** que ya ha sido instalado en el equipo. Para ello, escanean el contenido del registro de Windows, los archivos del sistema operativo, la memoria y los programas instalados en el ordenador. Al terminar el escaneo, muestran al usuario una lista con todas las amenazas encontradas y permiten escoger cuáles de ellas eliminar.

Estamos, por tanto, ante una medida de seguridad preventiva y paliativa, ya que contribuye a la prevención de infecciones por *malware* y, en caso de estar infectados, contribuye a desinfectar al equipo afectado. Así pues, hemos considerado oportuno incluir esta medida dentro de las preventivas porque su principal objetivo es evitar infecciones.

Las soluciones de seguridad detectan el *malware* usando varias técnicas:

- **Comparación con firmas:** se comparan los archivos sospechosos con una base de datos con las firmas de todo el *malware* conocido hasta la fecha. Estas bases de datos deben actualizarse periódicamente.
- **Métodos heurísticos:** aunque la base de datos de firmas esté actualizada, no es posible contener información sobre todo el *malware,* por lo que se debe "deducir" si el equipo está infectado utilizando técnicas para detectar *malware* sin tener su firma en la base de datos. Para ello, los motores *antimalware* de las *suites* de seguridad utilizan técnicas como las siguientes:
  - **Firmas genéricas:** no buscan una coincidencia al 100% pero sí una similitud con una firma, para detectar mutaciones de virus.
  - **Desensamblado:** se obtiene el código en lenguaje ensamblador del *malware* y se estudia el código con técnicas conocidas.
  - **Desempaquetado:** algunos virus han sido empaquetados y comprimidos para evitar que sean detectados. Los antivirus los desempaquetan y analizan.

La mayoría de equipos utilizan una ***suite* de seguridad personal.** Se trata de una aplicación antivirus que se instala en un ordenador o en una pequeña red doméstica. Esta solución de seguridad actualiza periódicamente su motor y base de datos de firmas a través de Internet.

En los **entornos profesionales y empresariales,** en cambio, este sistema de instalación y actualizaciones es poco eficaz. Imaginemos una empresa que dispone de treinta equipos, los cuales utilizan la misma herramienta de seguridad. Cada uno de los equipos deberá actualizarse periódicamente, descargándose de Internet la última versión, consumiendo mucho ancho de banda.

En lugar de tener treinta equipos descargándose la misma versión desde un servidor de Internet, resulta mucho eficaz que un equipo se descargue la última versión y el resto de equipos se actualice a partir de la información que contiene este equipo. Al estar en la misma red, las operaciones de actualización serán más rápidas, mejorando el consumo de ancho de banda. Esta es la idea en la que se basan **las *suites* de seguridad corporativas,** donde existe un servidor que descarga la última versión del programa y además recoge los informes y alertas de detección e infección de todos los ordenadores de la organización.

De esta forma, un administrador de red puede tener centralizadas todas las actualizaciones, así como toda la información relativa a *malware* detectado o eliminado en los clientes de la red. También se puede intervenir remotamente en los equipos en los que se ha detectado una infección y no se ha podido eliminar.

El abanico de *suites* de seguridad disponible en la actualidad es muy amplio y en muchos casos el tipo de protección ofrecido es muy similar. Algunos ejemplos son: Avast! Internet Security, AVG Internet Security, Panda Internet Security, Eset Smart Security, Norton Internet Security, Avira Premium Security Suite, Kaspersky Internet Security y McAfee Windows Defender.

Firmas de virus

Las firmas son una pequeña secuencia de bytes del código del virus que las soluciones antivirus utilizan para identificarlos.

Soluciones *antimalware* específicas

En el caso de descubrir en un equipo algún tipo de *malware* no detectado por la *suite* de seguridad, se puede complementar esta con una herramienta diseñada especialmente para eliminar ese tipo de *malware* como: HijackThis o Spybot - Search & Destroy.

Ejemplos

Instalación de un antivirus en Linux

Vamos a aprender a utilizar ClamAV, un antivirus que se distribuye bajo licencia GPL para sistemas Unix/Linux, en este caso en un sistema que funciona con una distribución Fedora.

Para instalar el programa podemos ejecutar la siguiente orden en un sistema Fedora:

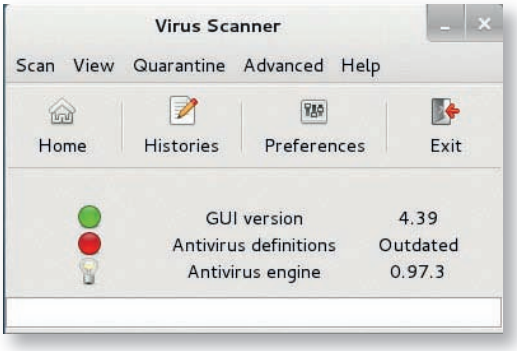
```
$ yum install clamav
```

Para facilitar el manejo del programa instalaremos una interfaz gráfica con la siguiente orden:

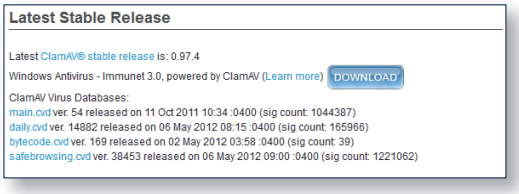
```
$ yum install clamtk
```

Para descargarnos el código fuente del programa para otras distribuciones Linux, podemos acudir al siguiente enlace: www.clamav.net

Si todo ha ido bien, en *Accesorios* nos aparecerá un nuevo programa llamado Clamtk. Al ejecutar el programa, veremos la pantalla principal del antivirus. Como la base de datos de firmas no está actualizada, aparece un icono en rojo y el texto *Outdated* junto al apartado *Antivirus definitions*.



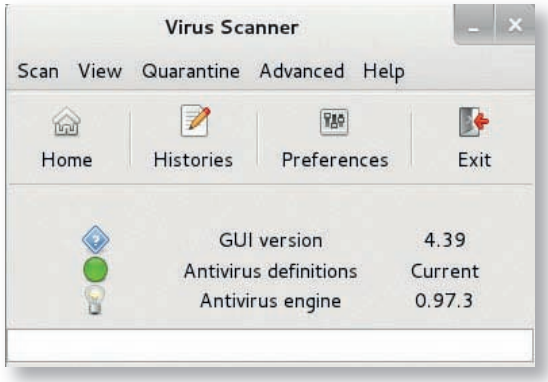
Por ello, antes de utilizar el programa, habrá que actualizarlo descargándonos la última versión de la base de datos de virus de la página web: www.clamav.net.



Nos descargaremos los archivos *main.cvd* y *daily.cvd*. El siguiente paso será copiar estos archivos al directorio donde se ha instalado el programa (*/var/lib/clamav*).

Volvemos a ejecutar el programa y vemos que la pantalla principal ha cambiado y la base de datos de definiciones de virus está actualizada *(Current)*.

Ya podemos analizar el sistema. Para ello seleccionamos *Scan / Recursive scan* y elegimos el directorio que queremos analizar. Podemos seleccionar la raíz del sistema (directorio /), con lo que se analizarían todos los archivos del sistema.



Cortafuegos

Un *firewall* o cortafuegos es un dispositivo software o hardware que forma parte de un equipo o dispositivo de una red y está diseñado para proteger dicho sistema bloqueando accesos no autorizados y permitiendo solo los que deban ser permitidos cumpliendo con las directrices definidas en la política de seguridad de la organización.

Todos los mensajes que entren o salgan del equipo o la red pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

Para permitir o denegar el tráfico, los cortafuegos suelen definir una **política por defecto** que se aplica sobre todos los paquetes que llegan a ellos. Distinguimos dos tipos de políticas:

- **Políticas permisivas:** se deniega explícitamente el acceso a la red por parte de algunas aplicaciones, servicios, equipos o redes, permitiéndose el acceso al resto de aplicaciones. Esta política puede presentar problemas de seguridad porque cualquier aplicación no denegada explícitamente estará autorizada a acceder.
- **Políticas restrictivas:** por defecto está prohibido el acceso a los recursos del sistema, debiendo autorizarse de forma explícita y caso a caso. Esta política es la más adecuada para la mayoría de situaciones, porque si nos olvidamos de indicar alguna condición por defecto se rechazará su acceso, con lo que no constituirá un riesgo de seguridad.

Además de la política por defecto, la mayoría de cortafuegos definen **reglas** que son un conjunto de condiciones que deben cumplir los mensajes para que el *firewall* permita o rechace su paso.

Estas reglas suelen contener información como la siguiente:

- Equipo o red que ha enviado el mensaje.
- Dirección IP del equipo o red que recibirá el mensaje.
- Protocolo utilizado (TCP, UDP, ICMP).
- Puerto del equipo destinatario o emisor del mensaje.
- Acción a realizar sobre el paquete (aceptar, rechazar informando al emisor del motivo por el que se rechazó el mensaje, rechazar sin informar al origen, etc.).

Si, por ejemplo, tenemos un servidor web, definiremos una regla para que acepte solo el tráfico que vaya al puerto 80 TCP, y otra para que se rechace el resto de tráfico que llega al equipo.

Algunos ejemplos de cortafuegos comerciales son: Agnitum Outpost Firewall, AnalogX PortBlocker, Ashampoo Firewall, Comodo Firewall, DroidWall, MailControl, Sunbelt Personal Firewall y Zone Alarm. La mayoría de estos programas suele ofrecer alguna versión gratuita con una funcionalidad reducida.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. Es necesario combinarlo con otros sistemas como herramientas *antimalware*, sistemas *antispam*, detectores/preventores de intrusos (IDS/IPS), *proxies*, etc.

Iptables

Iptables es el cortafuegos por defecto de los sistemas Linux y permite filtrar paquetes, realizar tareas de enrutamiento redirigiendo tráfico a equipos concretos, realizar traducción entre direcciones de red (NAT/PAT) y mantener registros de log.

Es una herramienta libre muy potente que conviene conocer para administrar sistemas Linux.

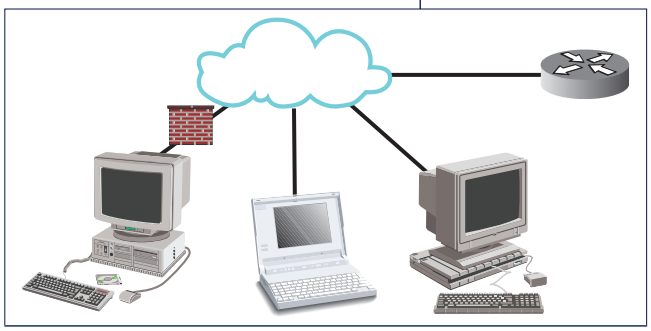
Para facilitar su administración, se han desarrollado interfaces gráficas que simplifican su utilización, como fwbuilder.

Tipos de cortafuegos

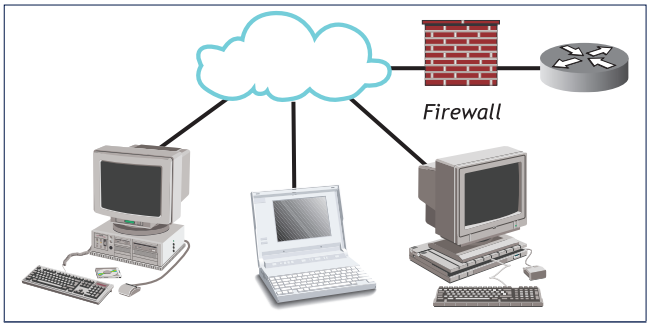
Se puede clasificar los cortafuegos atendiendo a diferentes criterios, como su ubicación y su modo de funcionamiento:

Según el lugar en que se ubica el cortafuegos, podemos diferenciar entre:

- **Cortafuegos de equipo o de *host*.** Se instala en el equipo que se desea proteger. Analiza todo el tráfico que llega al equipo o sale de él y permite establecer qué aplicaciones pueden enviar y recibir información a través de la red.
- **Cortafuegos de red o perimetrales**. Este tipo de cortafuegos se ubica en un punto de entrada común a la red, como un *router* y actúa como barrera entre la red interna de nuestra casa u organización y la externa (Internet). Este tipo de cortafuegos se estudiará con más detalle en la unidad dedicada a la seguridad en redes.



7.1. Cortafuegos de equipo. Solo el equipo de la izquierda filtra el tráfico.



7.2. Cortafuegos de red. El *router* filtra el tráfico de todos los equipos.

Tipos de cortafuegos según su funcionamiento	
Cortafuegos de filtrado de paquetes	También llamados "cortafuegos sin estado", filtran el tráfico mirando únicamente direcciones IP de origen y destino, puertos TCP/UDP o protocolo usado, pero sin llevar un seguimiento de conexiones o ver si forman parte de una secuencia anterior (estado). Este tipo de cortafuegos suelen permitir filtrados según campos de nivel de transporte, como el puerto origen y destino, o a nivel de enlace de datos como la dirección MAC.
Cortafuegos de aplicación	Cortafuegos que actúan sobre la capa de aplicación del modelo OSI, con lo que pueden entender ciertas aplicaciones y protocolos. Permiten detectar si un protocolo no deseado se filtró a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.
Cortafuegos de estado	Tienen en cuenta el estado de un paquete, esto es la colocación de cada paquete individual dentro de una serie de paquetes, ya que mantienen registros de todas las conexiones que les atraviesan y son capaces de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente o es un paquete erróneo. Este tipo de cortafuegos puede ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio. Un ejemplo de cortafuegos de estado es iptables.

Ejemplos

Utilización del *firewall* de Windows 7

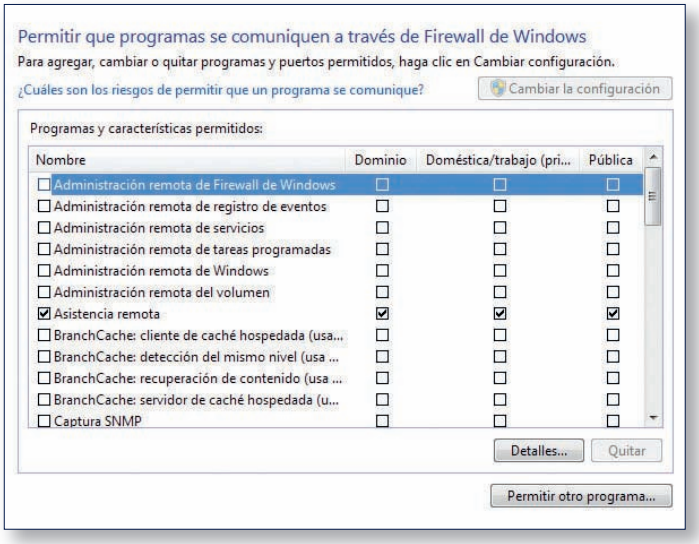
Vamos a presentar la utilización básica del cortafuegos que viene instalado por defecto en los sistemas Windows 7.

Para ello, en primer lugar hacemos clic en el botón de Inicio / *Ejecutar…* (o pulsamos <tecla Windows> + <R>) y escribimos *firewall.cpl*

También podemos acceder desde el botón de Inicio / *Panel de control* / *Sistema y seguridad* / *Firewall de Windows*.

Se abrirá una ventana con información general sobre la configuración de las redes privadas y públicas del equipo. Para modificar la configuración del cortafuegos de Windows, seleccionamos *Permitir un programa o una característica a través de Firewall de Windows* en la esquina superior izquierda.

Se abrirá una nueva ventana en la que se pueden ver las aplicaciones instaladas en el equipo y el tipo de acceso permitido para cada una de esas aplicaciones: permiso para la red privada o para la red pública.



Para permitir o denegar el acceso a una aplicación, basta con marcar o desmarcar la casilla correspondiente. En el caso de que queramos darle acceso a una aplicación que no se encuentre en el listado de programas, tendremos que hacer clic en *Permitir otro programa…* y buscar la aplicación que deseamos incluir a la lista principal.

Protección ante *malware* en correos electrónicos

Una de las principales formas de propagación utilizadas por el *malware* es el correo electrónico. Tenemos que ser conscientes de que cualquier correo recibido puede contener archivos adjuntos que incluyan software malicioso y que, aunque quien nos envíe el correo electrónico sea un conocido, existe riesgo al utilizar los archivos adjuntos en los correos puesto que esa persona puede habernos enviado un archivo infectado sin saberlo.

En ocasiones, somos nosotros quienes propagamos *malware* sin ser conscientes de ello, enviando archivos infectados. Otras veces un atacante consigue suplantar la identidad de una cuenta de correo electrónico, pasando a controlarla.

También podemos ser víctimas del robo de nuestra cuenta de correo, que es una práctica muy extendida y lucrativa en la actualidad. Los atacantes utilizan una gran cantidad de métodos, generalmente basados en técnicas de ingeniería social, para obtener acceso a cuentas de correo existentes y suplantar la identidad de las víctimas.

A continuación comentamos algunas medidas que podrían protegernos contra el *malware* en correos electrónicos:

- Ante todo, la medida básica a observar es actuar con prudencia antes de abrir archivos adjuntos, aunque el emisor sea de confianza. Si se quiere verificar la seguridad de un archivo adjunto antes de abrirlo, se recomienda guardar el archivo adjunto en una carpeta y pasar un antivirus sobre esa carpeta antes de abrirlo.
- Configurar el correo para que el antivirus compruebe los mensajes.
- No reenviar un mensaje sin antes borrar la lista de direcciones de correo electrónico, provenientes de anteriores reenvíos, que se van arrastrando de unos mensajes a otros.
- No reenviar mensajes que formen parte de cadenas.
- No hacer clic en las direcciones web que aparecen en un correo electrónico a no ser que el correo sea de confianza.
- Denunciar el correo abusivo o fraudulento informando al titular del correo desde donde ha partido el mensaje.

Uso de la copia oculta

Cuando se realizan envíos masivos de correos electrónicos, no se debe utilizar el campo *Destinatario* para insertar las direcciones, sino el campo *Copia oculta (CCO)*. De esta forma, cada destinatario recibirá una copia del mensaje pero sin conocer las direcciones de correo de los demás destinatarios.

Actividades propuestas

1·· ¿Por qué es importante tener actualizados los componentes de los navegadores? Busca información en Internet sobre vulnerabilidades encontradas en los últimos seis meses.

2·· Busca información sobre algún *antirootkit* y explica cómo puede ayudar a proteger un equipo informático contra este tipo de *malware*.

3·· Explica qué se puede hacer para disminuir el riesgo de infección por *malware* mediante correo electrónico en un equipo informático.

4·· Has recibido un correo electrónico en inglés de un amigo diciéndote que entres en una página web que le ha gustado mucho. Este amigo nunca te envía mensajes en inglés. ¿Qué harías en esta situación?

1.2 > Medidas paliativas contra el *malware*

Las medidas de seguridad paliativas o correctoras contra el *malware* constituyen todo el conjunto de acciones que los usuarios realizan para eliminar *malware* que ha conseguido infectar al equipo.

De forma análoga a lo que hemos visto en las medidas preventivas, a este tipo de medidas también se las suele denominar como medidas de seguridad pasivas, aunque hay que puntualizar que no todas las medidas de seguridad pasivas son medidas correctoras.

Seguridad pasiva es un término más amplio, que abarca todo el conjunto de técnicas que permiten solucionar un incidente de seguridad que se ha producido. Por lo tanto, seguridad pasiva no solo hace referencia a las medidas que corrigen incidentes de seguridad relacionados con el *malware,* sino también a otras medidas como la corrección de pérdidas de la información, ya sean accidentales o no (roturas de discos o datos borrados).

Algunas medidas de seguridad paliativas son las copias de seguridad, el software congelador, los sistemas RAID o las herramientas de recuperación de datos borrados. La mayoría de estas medidas de seguridad se estudiarán en la unidad dedicada a la gestión de almacenamiento.

Es importante mencionar que no existe una solución mágica ante una infección o incidente de seguridad. Por ello, en cada caso, deberá estudiarse la gravedad y el alcance de la infección para decidirse por una opción u otra. Para estar informado de las últimas amenazas y la forma más conveniente de desinfección se propone la suscripción a listas de distribución de seguridad (como, por ejemplo, www.hispasec.com) o conectarse a páginas de respuesta ante amenazas, como los CERT o CSIRT, que veremos en el próximo epígrafe.

Copias de seguridad

Las copias de seguridad son una medida de seguridad paliativa muy importante y que consiste en guardar una parte o toda la información del sistema para poder recuperarla en el caso de que se haya producido una pérdida de la información.

Es muy importante que la información salvaguardada se encuentre almacenada en un dispositivo diferente del original, quedando la información a salvo en el caso de que se produjera algún incidente sobre el dispositivo que contenía los datos originales. Algunos medios de almacenamiento utilizados para guardar copias de seguridad son cintas, DVD, *Blu-rays,* discos virtuales u otros discos.

Se pueden establecer diferentes clasificaciones de copias de seguridad, pero atendiendo al tipo de información almacenada distinguimos entre:

- **Copias de seguridad del sistema:** permiten restaurar un equipo a un estado operacional después de un desastre.
- **Copias de seguridad de datos:** permiten restaurar algunos ficheros después de que hayan sido borrados o dañados accidentalmente.

Existe una gran variedad de software que permite realizar copias de seguridad: ZendalBackup, Cobian, Norton Ghost, Acronis, Clonezilla, etc.

¿Qué hago si mi equipo está infectado?

No existe una fórmula válida para desinfectar todos los equipos. Lo más común, aunque no siempre es efectivo, es utilizar una herramienta de desinfección, como una *suite antimalware*, pero en otras ocasiones no son capaces de detectar todos los especímenes de *malware* o no pueden eliminarlos del todo.

La primera tarea a realizar es determinar el tipo de *malware* si es posible. Para ello se puede utilizar la información de las listas de suscripción de seguridad o visitar los CSIRT o CERT para determinar cómo podemos eliminarlo.

Software "congelador"

El software "congelador" es un software especial, del tipo "reinicie y restaure" (*reboot and restore*). Cuando se instala, permite "congelar" el estado del equipo en un momento determinado, con la configuración y contenidos exactos que el equipo tenía en ese momento. Cada vez que se inicie el equipo, estará en el mismo estado en el que quedó "congelado".

Este software, que recibe su nombre de la traducción literal de su denominación en inglés (*freezer*), permite al usuario realizar acciones como instalar programas, realizar cambios en la configuración, enviar y recibir correos, recordar contraseñas, etc. y, al reiniciar el equipo, todos estos datos se pierden y este vuelve al estado en que quedó "congelado".

La congelación es una medida de protección que se utiliza habitualmente en ordenadores a los que acceden muchas personas, como los existentes en locutorios, cibercafés, aulas de centros académicos, etc. En estos casos, la utilización de este tipo de programas proporciona varios beneficios:

- Se contribuye al anonimato de los usuarios, ya que un usuario malintencionado no puede acceder a información previa a la sesión actual, al borrarse el historial, las *cookies* y las contraseñas que hayan podido quedar almacenadas por algún descuido.
- Se protege a los equipos frente a infecciones por software malicioso, ya que durante el proceso de restauración se elimina cualquier *malware* que haya infectado al equipo.

No obstante, hay que tener en cuenta que la información generada por los usuarios en cada sesión será automáticamente eliminada al reiniciar el equipo, por lo que para almacenarla hay dos opciones: usar dispositivos externos de almacenamiento (CD / DVD, *pendrive*, etc.) o particionar el disco y "congelar" únicamente una de las particiones, utilizando las no congeladas como espacio de almacenamiento.

Pese a las enormes ventajas que ofrece este software, hay tener en cuenta que, como el sistema se restaura al mismo punto una y otra vez, las actualizaciones del sistema operativo y las distintas aplicaciones tampoco se guardan, por lo que el sistema quedará desactualizado al poco tiempo, siendo más vulnerable al *malware*. Para solucionar este inconveniente, algunas soluciones comerciales permiten que las actualizaciones que afectan al sistema operativo y las aplicaciones no sean borradas al restaurar el equipo. Esta posibilidad deberá tenerse muy en cuenta a la hora de elegir entre una u otra herramienta.

La herramienta más conocida es Deep Freeze, válida para Windows, Linux y Mac, que permite actualizaciones. Otras herramientas de este tipo son: Clean Slate, DriveShield o Custodius.

Windows SteadyState

La empresa Microsoft ofrece Windows SteadyState, una aplicación gratuita disponible para usuarios que dispongan de un sistema operativo Windows original.

Actividades propuestas

5·· ¿Qué es un sistema RAID? Investiga sobre el RAID 5. ¿Crees que constituye una medida paliativa contra el *malware*?

2 >> Centros de protección y respuesta frente a amenazas

A lo largo de esta unidad se han estudiado algunas medidas que contribuyen a evitar o minimizar los daños producidos por el software malicioso. No obstante, el mundo del *malware* evoluciona constantemente y cada día surgen nuevas amenazas que conviene conocer y de las que conviene estar protegidos.

Para satisfacer esta necesidad de informar a los usuarios y proporcionarles mecanismos para protegerse frente a amenazas relacionadas con el *malware* surgen los centros de información y respuesta ante amenazas e incidencias de seguridad, como por ejemplo CERT o CSIRT, entre otros. Estos centros son organismos compuestos por expertos en desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Estos organismos estudian el estado de seguridad global de redes y ordenadores, proporcionan servicios de respuesta ante incidentes a víctimas de ataques en la red, publican alertas relativas a amenazas y vulnerabilidades y ofrecen información que ayude a mejorar la seguridad de estos sistemas.

Ofrecen, por lo tanto, dos tipos de servicios:

- **Preventivos**:
  - Avisos de seguridad.
  - Búsqueda de vulnerabilidades.
  - Auditorías o evaluaciones de seguridad.
  - Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras.
  - Desarrollo de herramientas de seguridad.
  - Propagación de información relacionada con la seguridad.
- **Reactivos**:
  - Gestión de incidentes de seguridad (análisis, respuesta, soporte y coordinación de incidentes de seguridad).
  - Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas).

CERT y CSIRT

Las siglas **CERT** vienen del inglés *Computer Emergency Response Team* (Equipo de Respuesta ante Emergencias Informáticas). Mientras que **CSIRT** proviene de *Computer Security Incident Response Team* (Equipo de Respuesta ante Incidentes de Seguridad Informáticos).

Básicamente, sus funciones son las mismas. Su diferencia se refiere al ámbito de actuación: los CERT suelen actuar a nivel de país (por ejemplo, INTECO-CERT de Red.es: http://cert.inteco.es), mientras que los CSIRT funcionan a nivel de organización o entidad (por ejemplo el de la Comunidad de Valencia, CSIRT-CV: https://www.csirtcv.gva.es/).

Actividades propuestas

6·· Entra en la página web www.hispasec.com y anota los distintos servicios que ofrece esta página. Explica en qué consiste y cómo funciona el servicio *Una al día* que puedes encontrar en esta web.

7·· Visita el CERT de Red.es (http://cert.inteco.es/):

a) ¿Qué contenidos se ofrecen en la sección *Útiles gratuitos?* ¿Frente a qué tipos de software malicioso se ofrece protección?
b) ¿Qué diferencias encuentras entre la sección titulada *Para usuarios técnicos* y la sección *Para usuarios no técnicos?*
c) ¿Qué consejos de seguridad (buenas prácticas) puedes encontrar?

3 >> Buenas prácticas para protegerse del *malware*

Como hemos visto, no existe un sistema totalmente seguro pero se pueden minimizar los riesgos llevando a cabo unas prácticas seguras que siempre se basan en el sentido común y que, en muchos casos afectan al eslabón de seguridad más débil y más frecuentemente olvidado: las personas que utilizan el sistema.

Habitualmente las infecciones no se producen por tener más o menos herramientas de seguridad, sino por el uso que se hace del sistema o las decisiones que se toman al navegar por Internet o abrir un mensaje de correo electrónico. Entre las medidas de protección que se pueden llevar a cabo, están las siguientes:

Recomendaciones frente al *malware*	
Actualizar el sistema operativo y aplicaciones	Es fundamental actualizar periódicamente el sistema operativo y todas las aplicaciones, especialmente las críticas (navegador web y sus *plugins)*.
Protección *antimalware*	Se debe instalar una *suite antimalware*, así como un cortafuegos y mantenerlos actualizados, configurándolos para que se actualicen automáticamente. También podría ser conveniente la utilización de un sistema de detección y prevención de intrusos IDS/IPS.
Cuentas de usuario	Conviene usar cuentas de usuario con privilegios limitados para el uso diario del equipo y utilizar la cuenta de administrador solo cuando sea necesario cambiar la configuración o instalar un nuevo programa.
Políticas de contraseñas	Se deben diseñar políticas que incluyan la definición de contraseñas complejas, tanto para usuarios del equipo como para aplicaciones en red.
Datos personales y claves	Es muy importante no facilitar datos personales, ni claves, ni códigos PIN solicitados por correo electrónico u otro medio (SMS, teléfono, etc). Esta información solo deberíamos introducirla en páginas web en las que estamos seguros de su procedencia y que establecen un canal de comunicación seguro como https.
Precaución al navegar	No se debe navegar por páginas web sospechosas, no confiables o que ofrezcan regalos o promociones dudosas. También se recomienda desactivar la interpretación de Visual Basic Script y únicamente permitir JavaScript, ActiveX y *cookies* en páginas web de confianza.
Correo electrónico	Se deben observar las recomendaciones expuestas en esta unidad, en el apartado dedicado al correo electrónico.
Instalación de aplicaciones	Se debe tener precaución al instalar o ejecutar programas procedentes de Internet, así como evitar la descarga de software de redes P2P, pues se desconocen su contenido y procedencia reales. Debe pasarse el antivirus a los medios extraíbles, como CD o memorias USB, antes de utilizarlos, porque son una fuente de propagación de *malware* muy común.
Reciclaje constante	Los administradores de sistemas deben mantenerse actualizados: suscribiéndose a boletines de seguridad, consultando periódicamente web de información (por ejemplo, CERT), etc.
Copias de seguridad	Se deben hacer regularmente copias de respaldo a medios extraíbles de los documentos importantes para poderlos recuperar en caso de infección.
Otras medidas	Otras posibles medidas son la realización periódica de auditorías de seguridad y la concienciación de los usuarios en cuestiones de seguridad informática.

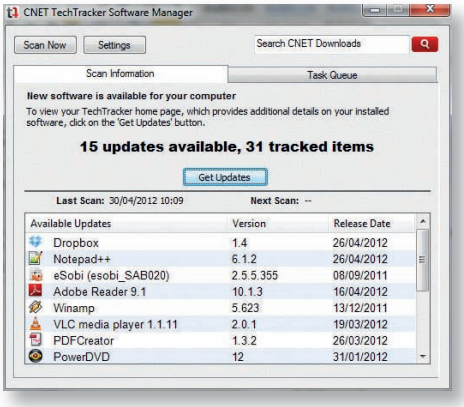
Ejemplos

Instalación de una herramienta para actualizar automáticamente aplicaciones en un entorno Windows

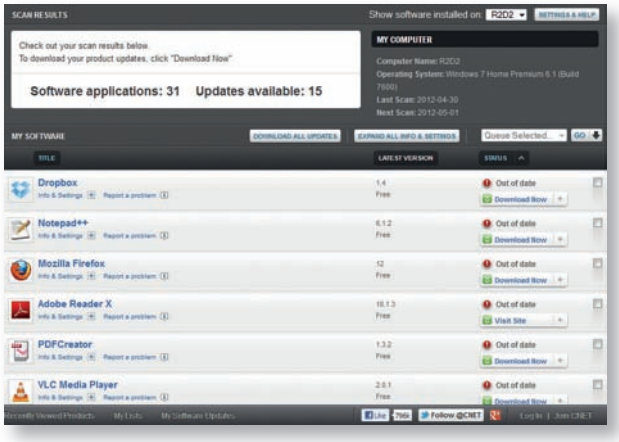
Vamos a instalar en un ordenador que funciona bajo Windows una herramienta para gestionar la descarga automática de actualizaciones de las distintas aplicaciones.

Para ello, usaremos el programa gratuito TechTracker, que se puede descargar desde la página web http://www.cnet.com/techtracker-free/.

Una vez descargado el programa, lo ejecutamos y se inicia un escaneo de programas no actualizados. Al finalizarlo, TechTracker muestra una lista de los programas instalados en nuestro equipo que necesitan actualización. Podemos ver la última versión disponible para cada uno de estos programas y la fecha de publicación de esa versión.



Al hacer clic en el botón central *Get Updates*, se abre el navegador y muestra una página web en la que se da más información y se desglosa la lista de todos los programas instalados en el equipo indicando si la versión instalada está actualizada o no (*Up to date*, actualizada, y *Out of date*, no actualizada).



Si deseamos actualizar alguna de las aplicaciones instaladas, seleccionamos la opción *Download Now* que figura al lado del estado de la versión. Si queremos descargar todas, hacemos clic en el botón *DOWNLOAD ALL UPDATES*. Una vez seleccionadas las aplicaciones que queremos descargar, haremos clic en el botón *GO* y las aplicaciones seleccionadas se actualizarán a la última versión existente. Si abrimos otra vez el programa, podremos ver el progreso del proceso de descarga haciendo clic en el botón *Task queue*.

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿Qué diferencias existen entre un antivirus y una *suite* de seguridad?

2·· ¿Qué es un centro de protección y respuesta ante amenazas?

3·· Describe los dos tipos de políticas por defecto disponibles para los cortafuegos. ¿Qué ventajas e inconvenientes presenta cada una de ellas?

4·· Enumera los tipos de cortafuegos que pueden encontrarse atendiendo a su ubicación en la red.

5·· ¿Qué ventajas presenta un cortafuegos de estado sobre uno de filtrado de paquetes? ¿Y uno de aplicación sobre uno de filtrado de paquetes?

6·· ¿Por qué es importante mantener las aplicaciones actualizadas? ¿Y los *plugins* del navegador?

7·· ¿En qué se diferencia un CERT y un CSIRT? Cita tres ejemplos de cada uno de estos centros.

8·· ¿Qué es un software congelador? Indica las principales ventajas e inconvenientes de su uso.

.: APLICACIÓN :.

1·· Un amigo se ha comprado un portátil que tiene instalado el cortafuegos que trae por defecto el sistema operativo. ¿Qué consejos le darías a tu amigo para evitar infecciones por *malware?* ¿Y para evitar la pérdida de información en caso de que algún *malware* haya infectado el equipo?

2·· Describe al menos cinco buenas prácticas que podemos seguir para minimizar riesgos de infección en nuestro dispositivo móvil.

3·· Has recibido un mensaje de correo electrónico de un conocido dirigido a muchas personas, que forma parte de una cadena de mensajes y en el que se adjunta un archivo. Al observar el mensaje ves que ha sido reenviado anteriormente por muchas personas y que se te sugiere que lo reenvíes a tus conocidos. ¿Cómo deberías proceder para minimizar el riesgo de infección por *malware* en tu equipo? ¿Qué consejos podrías darle a tu amigo para contribuir a reducir riesgos de infección en correos electrónicos?

4·· Has decidido instalar un software congelador en un cibercafé, pero no dispones de dinero para adquirir una versión comercial. ¿Existe algún programa que se adapte a tus necesidades? ¿Qué ventajas aporta la utilización de este tipo de producto?

5·· Un cliente te dice que cree que su ordenador portátil "está infectado por un virus" porque le aparece una pantalla en la que le dice que la policía nacional ha detectado que ha hecho un uso fraudulento de ese equipo y que tiene que pagar una multa, cuando la realidad es que él no ha realizado ningún uso anómalo del mismo. También te comenta que no puede entrar en el sistema con normalidad, con lo que no puede guardar un trabajo en un dispositivo de almacenamiento externo. El cliente no dispone de ninguna otra copia de este trabajo pero es muy importante recuperarlo.

¿Qué podrías hacer para solucionar esta incidencia?

6·· Después de solucionar el problema expuesto en la actividad anterior, intentas buscar el trabajo del cliente, pero descubres que el *malware* que ha infectado al equipo ha borrado muchos archivos del disco duro, entre ellos el trabajo. Decides utilizar una herramienta de recuperación de datos y consigues recuperar el trabajo. Indica qué consejos le darías al cliente para no volver a sufrir este tipo de situaciones.

¿Podrías recomendarle alguna herramienta que sea gratuita y fácil de utilizar?

Caso final 1

Instalación y configuración de un *firewall* personal para Linux

Un amigo, que tiene un ordenador con sistema operativo Linux (distribución Fedora), quiere instalar en su equipo un *firewall* que no sea muy complicado de utilizar y te pide ayuda para elegir uno que sea adecuado para sus necesidades, así como para llevar a cabo la instalación y configuración del mismo.

Después de estudiar la propuesta, te decides por fwbuilder, una herramienta que proporciona una interfaz gráfica que permite administrar fácilmente el cortafuegos de Linux. Este programa también hace las funciones de *router* y NAT a una red aislada con direccionamiento IP privado.

Instala y configura fwbuilder.

Solución •• Para instalar y configurar fwbuilder debes seguir los siguientes pasos:

1. Desactivar el *firewall* que viene instalado por defecto en Linux.
2. Instalar fwbuilder.
3. Crear un objeto cortafuegos.
4. Definir reglas.
5. Aplicar los cambios en el cortafuegos.

Vamos a ver uno por uno.

1. Desactivar el *firewall* que viene instalado por defecto en Linux

En primer lugar debes ejecutar:

`$ iptables –F`: borra todas las reglas que haya en la tabla *filter*.

`$ iptables -t nat –F`: borra todas las reglas que hubiera en la tabla *nat*.

Cada vez que se reinicia el equipo, se aplican las mismas reglas de Fedora. Esto es así por un *script* de inicio que se llama iptables y se encuentra ubicado en */etc/init.d/iptables*.

Para que este servicio de Fedora no se interponga con el *firewall* que vas a configurar, hay que desactivarlo del arranque con:

```
$ chkconfig iptables off
```

La orden anterior no desactiva el uso de iptables en el sistema, lo que hace es modificar la configuración inicial de iptables, que carga el sistema operativo Linux (Fedora en este caso) al arrancar. Si quisieras volver a activarlo una vez finalizada la práctica, lo podrías hacer ejecutando el siguiente comando:

```
$ chkconfig iptables on
```

2. Instalar fwbuilder

Ejecuta `$ yum install fwbuilder fwbuilder-ipt`

Para comprobar que está bien instalado, desde una consola puedes buscarlo en los programas de Fedora o lanzarlo desde la consola ejecutando el comando `$ fwbuilder &`.

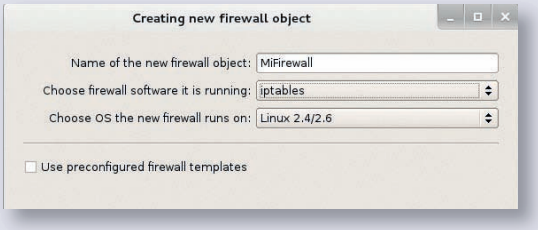
La herramienta fwbuilder se organiza en varios paneles donde se pueden consultar los objetos (redes, servicios, direcciones, puertos, etc.) que se pueden administrar, las reglas que se puede crear y el editor para modificar reglas y objetos.

»

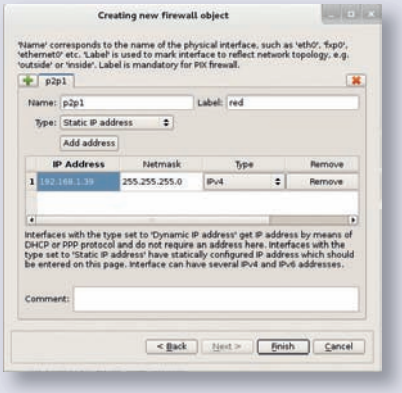
3. Crear un objeto cortafuegos

Puedes marcar el icono *Create new firewall* en el panel central o hacer clic con el botón secundario del ratón en *Firewalls* y seleccionar *New Firewall*.

Ponle un nombre al cortafuegos y elige como software para el *firewall* iptables y como sistema operativo Linux 2.4/2.6, que es el kernel de la distribución Fedora para la que estás configurando el cortafuegos.

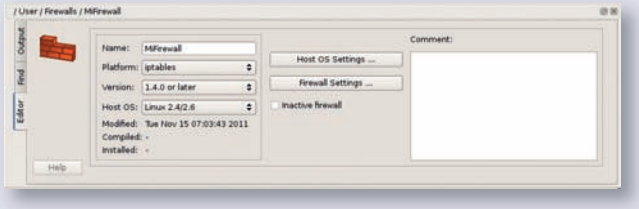


A continuación, configura manualmente las interfaces. Para ello debes introducir los datos de la tarjeta ethX (eth0, eth1 o como aparezca en el sistema), que es la tarjeta que con la que el equipo se conecta a la red y a Internet. En la imagen del margen tienes un ejemplo. Al hacer clic en *Finish* verás el cortafuegos que acabas de crear en el panel de objetos junto con su lista de interfaces.



Haz doble clic sobre la interfaz que acabamos de crear y marca la casilla *Management interface*.

Haz clic sobre el objecto *MiFirewall* recién creado y, en el editor, selecciona 1.4.0 como versión de iptables.



4. Definir reglas

Las reglas permiten que los servicios especificados puedan establecer conexiones con servicios ubicados en otros equipos. Por defecto, fwbuilder utiliza una política restrictiva, con lo que se corta todo el tráfico y solo permite el indicado explícitamente.

Para crear reglas, selecciona el menú *Rules* / *Insert Rule* y se creará una regla, que deberás editar.

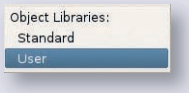
Los campos más importantes de la regla son:

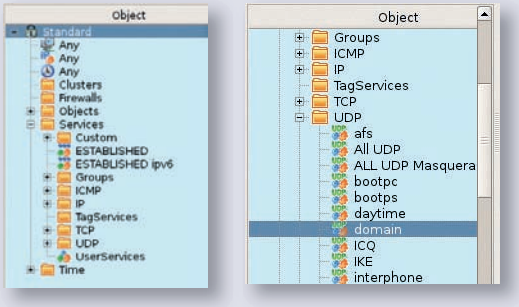
- *Source*: indica una dirección IP o una red desde la que se envían paquetes. Para interpretarlo correctamente hay que tener en cuenta el valor campo del campo *Direction*. Si el valor de *Direction* es *Inbound*, este campo hace referencia a los paquetes enviados desde otros equipos al nuestro y lo contrario, si el valor es *Outbound*.

1

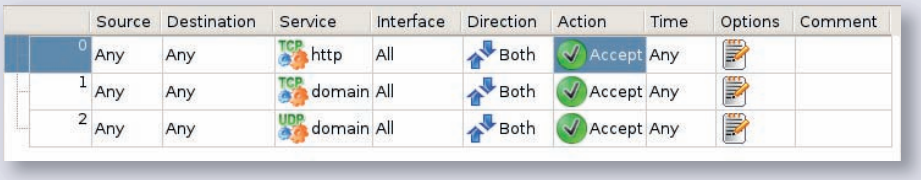
- *Destination*: especifica una dirección IP o una red a la que se envían peticiones. Su interpretación es similar a la del campo *Source*.
- *Service*: se puede restringir una regla a una aplicación o servicio concreto a partir del número de puerto que utiliza. Así, por ejemplo, si se desea navegar por Internet hay que indicar el puerto 80. Para ello, se crea un objeto servicio (*Service*) y se arrastra a este campo.
- *Direction*: indica si los paquetes entran a nuestro equipo (*Inbound*) salen de él (*Outbound*), o entran y salen (*Both*).
- *Action*: especifica si las peticiones que cumplan los criterios establecidos se aceptan (*Accept*), se rechazan (*Deny*) o se realiza alguna otra acción sobre ellas. Con el botón secundario se puede cambiar el valor de *Deny* a *Accept* y viceversa.
- Hay otros campos, como *Interface* y *Time*, que aunque no son básicos para cualquier regla sí añaden una mayor flexibilidad para crear las reglas.

Para rellenar el campo *Service* es conveniente que utices unas plantillas ya definidas por el programa que simplifican el trabajo. Por ejemplo, si lo que quieres es permitir que el navegador pueda acceder a Internet, tienes que permitir solo los servicios de DNS y de HTTP. Puedes acceder a estas plantillas haciendo clic en *User*, en la esquina superior izquierda y seleccionando *Standard*. En el panel izquierdo verás que aparecen objetos que no has creado. Si quieres permitir acceso al servicio DNS, abre la carpeta *UDP* y busca *domain*.





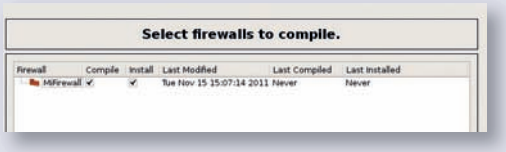
Finalmente, arrastra este servicio al campo *Service* de la regla deseada, con lo que al final esta debería presentar un aspecto similar al siguiente:



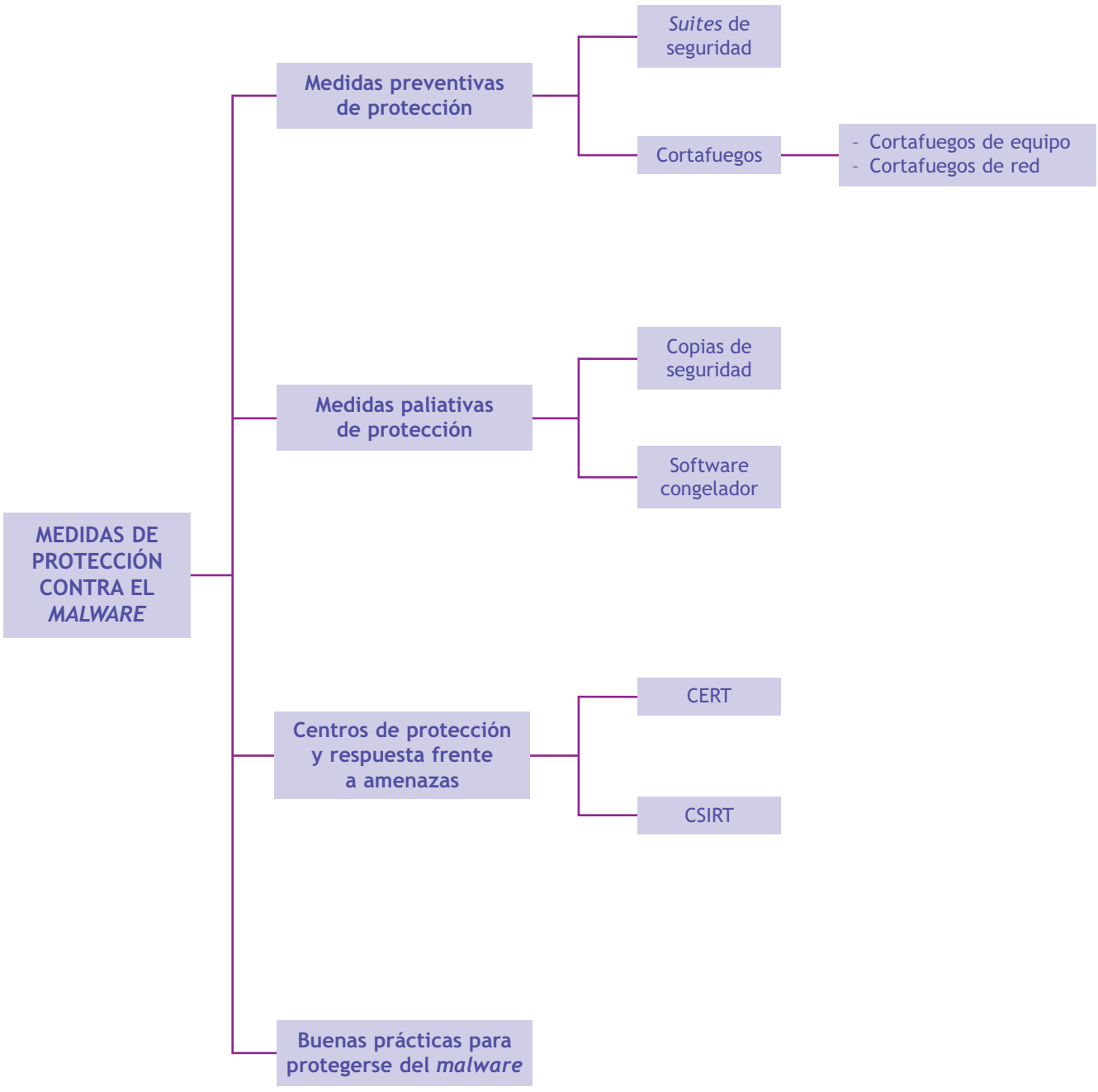
	Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
0	Any	Any	http	All	Both	Accept	Any		
1	Any	Any	domain	All	Both	Accept	Any		
2	Any	Any	domain	All	Both	Accept	Any		

5. Aplicar los cambios en el cortafuegos

Para poner en marcha el cortafuegos con las reglas que has creado, haz clic en *Rules* / *Install* / *Next* hasta llegar a la siguiente ventana, donde se indica el usuario que debes usar para instalar la configuración y que, lógicamente, debe ser root.



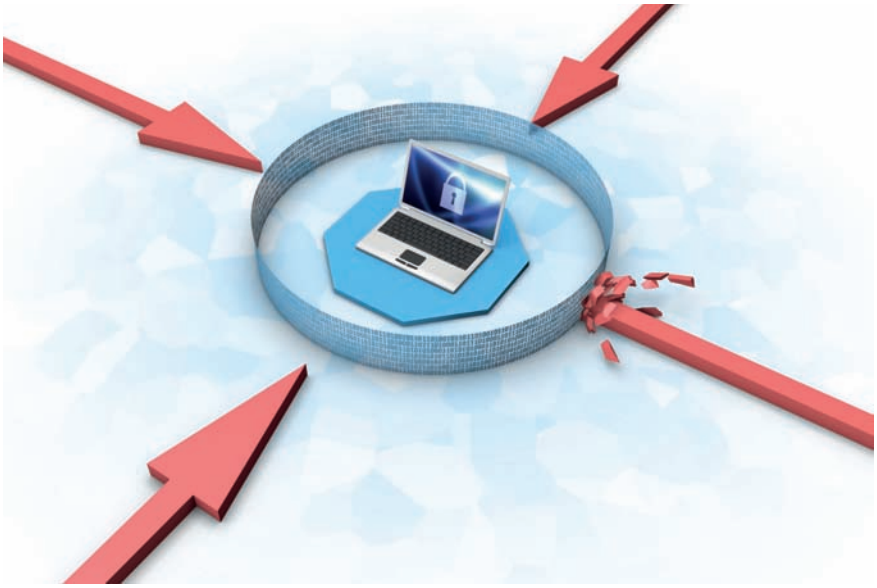
Ideas clave


MEDIDAS DE PROTECCIÓN CONTRA EL *MALWARE*
Medidas preventivas de protección
Suites de seguridad
Cortafuegos
- Cortafuegos de equipo
- Cortafuegos de red
Medidas paliativas de protección
Copias de seguridad
Software congelador
Centros de protección y respuesta frente a amenazas
CERT
CSIRT
Buenas prácticas para protegerse del *malware*

Cortafuegos personales y *malware*

El cortafuegos personal es una de las medidas "estrella" recomendada desde hace muchos años para luchar contra todo tipo de males. La inercia de la recomendación ha seguido hasta nuestros días, donde un cortafuegos entrante tradicional poco o nada puede hacer contra muchos de los ataques más sofisticados que se sufren hoy en día.

Instalar un cortafuegos personal era imprescindible hace diez años. Los sistemas operativos Windows 9X estaban conectados directamente a la red, con IP pública a través de módem. No contar con un *firewall* constituía un suicidio tecnológico. Después de Sasser y Blaster, XP SP2 se instauró con cortafuegos entrante integrado y activo. Las reglas del juego cambiaron por completo y los atacantes se adaptaron rápido, las víctimas... todavía no.



El cortafuegos entrante

Hoy en día un cortafuegos entrante no es útil contra el *malware*, han aprendido a sortearlo y es complicado encontrar troyanos "clásicos" que abran puertos en el sistema. Además, aunque lo consiguieran, no sería efectiva esta técnica: hoy también es mucho más habitual conectarse a la red de forma indirecta, anteponiendo un *router*. Estos *routers* suelen disponer de cortafuegos que protegen del exterior y, aunque no lo tuvieran, un atacante tendría que realizar una traducción a direcciones y puertos internos para llegar al sistema que quiere atacar. Por tanto, el cortafuegos entrante no está diseñado contra el *malware* de hoy.

El cortafuegos saliente

¿Qué es efectivo entonces? El cortafuegos saliente. Ese que introdujo Vista en 2006... desactivado por defecto y, por tanto, con nulo impacto real en la red. Su ventaja es que detendría a una buena parte de los troyanos actuales, que dependen de infraestructuras externas para salir a Internet e infectar el sistema.

Su problema es que, si bien no todas las aplicaciones legítimas reciben conexiones procedentes del exterior, sí que casi todas hoy en día se comunican con el exterior, y tendrían por tanto que estar contempladas como excepción en el cortafuegos saliente. Es una tarea compleja, pero teniendo en cuenta lo bien que se las ha apañado Windows con Vista y 7 para diseñar un cortafuegos entrante que no "estorba" y es efectivo, sospecho que en el futuro podría tenerlo activo por defecto si trabajan ciertos aspectos. Se podrían añadir ciertas funciones para hacer más cómodo un cortafuegos saliente, como:

- Que solo las aplicaciones firmadas pudieran salir sin problema a Internet. Las no firmadas, pedirían confirmación.
- Que solo las aplicaciones alojadas en ciertas rutas (en las que el usuario no tiene permiso de escritura como tal, solo como administrador) pudieran salir sin problemas.
- Función para bloquear aplicaciones por *hash*.
- Función para bloquear aplicaciones según el lugar de donde provienen.

Fuente: Extracto de artículo de Sergio de los Santos en www.hispasec.com

Actividades

1·· ¿Por qué era peligroso no utilizar *firewall* en sistemas operativos Windows 9X?

2·· Según el artículo, ¿por qué un cortafuegos entrante no es útil?

3·· ¿Por qué es un problema controlar las conexiones salientes?

unidad 8

Gestión del almacenamiento

SUMARIO

- Gestión y políticas de almacenamiento
- Dispositivos de almacenamiento
- El almacenamiento externo
- Tecnologías de almacenamiento redundante
- Copias de seguridad
- Imágenes del sistema
- Recuperación de datos

OBJETIVOS

- Conocer las características de la gestión del almacenamiento.
- Diseñar políticas de almacenamiento.
- Utilizar los medios de almacenamiento y saber cómo protegerlos.
- Reconocer las tecnologías de almacenamiento redundante más utilizadas.
- Realizar copias de seguridad e imágenes del sistema.
- Aprender a recuperar datos borrados.

1 >> Gestión y políticas de almacenamiento

A todos nos preocupa el almacenamiento de los archivos que contienen los dispositivos informáticos que utilizamos: fotografías, archivos ofimáticos, música, vídeo, etc. Pero, ¿sabemos realmente qué soportes de almacenamiento son los más fiables?

Los trabajos del instituto o los informes que se realizan en la oficina, suelen guardarse en una memoria USB o en un disco externo. Las fotografías digitales realizadas con cámaras y con dispositivos móviles las guardamos en el ordenador. ¿Son realmente seguros estos soportes? Para un usuario no avanzado puede parecer que sí, pero puede suceder que el disco duro donde estén almacenados se estropee.

Y si nos vamos a grandes volúmenes de datos, imaginemos la repercusión en una empresa de una pérdida de datos que afectara, por ejemplo, a las nóminas de los empleados, o en los registros bancarios que afectara a las transacciones realizadas.

Por todo ello, es fundamental tener un control sobre el almacenamiento de la información que garantice una seguridad física y lógica de la misma como ya se ha estudiado en anteriores unidades. Una correcta gestión permitirá mantener la integridad, autenticidad y disponibilidad de la información.

Además, no hay que olvidar que la Ley Orgánica de Protección de Datos de Carácter Personal obliga a toda organización a garantizar la seguridad de los datos de carácter personal que posea.

Una correcta gestión del almacenamiento implica, entre otras, la toma de decisiones como estas:

- ¿Qué información se debe almacenar?
- ¿Con qué frecuencia se va a usar y modificar?
- ¿Cuánta capacidad se va a necesitar?
- ¿Qué tecnología de almacenamiento será la más adecuada para una correcta disponibilidad de la información?
- ¿Cuál será el número de usuarios estimado en el acceso a la información almacenada?
- ¿Qué técnicas de seguridad van a ser necesarias?
  - Seguridad física: control de acceso al medio con sistemas biométricos, utilización de dispositivos NAS, utilización de una red de área de almacenamiento (SAN), etc.
  - Seguridad lógica: cifrado de datos, bloqueo de dispositivo, etc.

Por tanto, el concepto de seguridad en sistemas de almacenamiento engloba todas aquellas características y medidas que permiten mantener la información almacenada de forma segura frente a fallos físicos y lógicos, acceder a la información en todo momento y protegerla de accesos no autorizados

A lo largo de esta unidad veremos algunos de los aspectos anteriores, así como la forma de realizar un plan de copias de seguridad y recuperar información frente a posibles pérdidas.

Repercusión de la pérdida de datos

Según un estudio del Disaster Recovery Institute, el 90% de las empresas afectadas por una pérdida significativa de datos termina quebrando en un plazo de tres años.

Ley Orgánica de Protección de Datos Carácter Personal

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) tiene por objeto proteger el derecho a la intimidad personal y familiar de los ciudadanos y el adecuado tratamiento de la información referente a las personas físicas.

Políticas de almacenamiento

Para la adecuada gestión del almacenamiento de la información, las empresas deben definir unas políticas o normativas que definan con claridad las conductas que deben llevar a cabo los usuarios de la información para preservarla. Al menos, estas políticas deben recoger:

- Normas de almacenamiento en los equipos de trabajo.
- Normas de uso de dispositivos externos de memoria.
- Normas de almacenamiento en la red de la empresa.
- Normativa de realización de copias de seguridad.

Deberán estar redactadas de forma clara, indicando qué se puede hacer y qué no, qué información se debe almacenar y dónde, qué dispositivos se pueden utilizar y cómo, etc.

Ejemplos

Políticas de seguridad sobre el uso de dispositivos externos

La empresa PUBLIDISEÑO SL, dedicada al diseño y venta de publicidad, dispone una política de seguridad de almacenamiento de la información que recoge los siguientes puntos relativos al uso de dispositivos externos de memoria:

a) Indicación de si está o no permitido el uso de dispositivos externos ajenos a la empresa.
"Solo estará permitido el uso de los dispositivos externos siempre y cuando sean propiedad de la empresa. Todo usuario es responsable de conocer el buen uso del dispositivo".

b) Indicación de si está o no permitido el uso de dispositivos externos propiedad de la empresa y, si está permitido, qué tipo de información no podrá almacenarse en ellos.
"Podrá hacer uso de los dispositivos externos cualquier usuario que por sus funciones lo necesite, previa autorización por parte del administrador de sistemas conjuntamente con la dirección".

"No se permite el almacenamiento de cualquier tipo de software ilegal ni información de carácter externo a la empresa. También se considera como información no permitida aquella que sea de índole violenta, obscena, indecente u ofensiva".

c) Indicación de si el uso de este tipo de dispositivos fuera de la organización está o no permitida.
"El uso de los dispositivos externos fuera de la organización deberá ser autorizado previamente por escrito por el administrador de sistemas conjuntamente con la dirección".

d) Consecuencia del incumplimiento de las medidas.
"El incumplimiento por parte de los usuarios de las presentes políticas motivará las acciones oportunas que determine el director general o jefe del área junto con el administrador de sistemas".

Actividades propuestas

1·· ¿Qué medidas adoptas para almacenar tu información de manera segura? ¿Qué dispositivos de almacenamiento utilizas?

2·· Indica qué ventajas puede obtener una empresa al gestionar correctamente su almacenamiento.

3·· ¿Por qué deben las empresas elaborar una política de almacenamiento?

2 >> Dispositivos de almacenamiento

Los dispositivos de almacenamiento permiten guardar y manejar información temporal y permanente. Estos dispositivos se han convertido en un componente fundamental tanto a nivel personal como en las organizaciones. Un fallo en alguno de ellos puede ocasionar graves problemas si no se ha seguido una correcta política de seguridad.

2.1 > Clasificación

Pueden clasificarse de muchas formas en función del criterio utilizado.

Si atendemos al medio usado para el almacenamiento, tenemos:

- **Medios magnéticos:** discos duros, disquetes y cintas magnéticas.
- **Medios ópticos:** CD, DVD, HD-DVD o *Blu-ray.*
- **Electrónicos o memorias de estado sólido:** memorias *flash,* tarjetas de memoria y discos duros SSD.
- **Otros:** memorias híbridas magneto-ópticas, memoria holográfica, memoria molecular, *patterned media*, etc.

Otra clasificación que podemos encontrar es la siguiente:

- **Dispositivos locales.** Están conectados directamente al equipo y son gestionados por el mismo. Aquí incluiríamos los dispositivos extraíbles, que pueden ser extraídos de las unidades o puertos en los que están conectados sin necesidad de tener que apagar el equipo.
- **Dispositivos externos.** Gestionados por un sistema externo al equipo:
  - **Dispositivos remotos:** almacenan la información en dispositivos ubicados fuera de la organización. Posibilitan tener una copia de seguridad de la información (p. ej., granjas de servidores).
  - **Dispositivos de almacenamiento externo.**

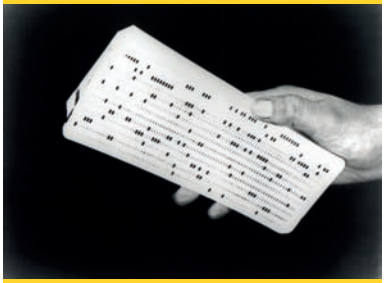
2.2 > Servicios de almacenamiento remoto

Existen empresas que ofrecen servicios de alojamiento remoto de la información. Estos servicios sustituyen la falta de espacio que muchas veces se produce en la organización si no se tiene una buena gestión del almacenamiento o si se tiene un gran volumen de información.

Los servicios de almacenamiento remoto pueden ser gratuitos o de pago. Los gratuitos tienen limitado el espacio además de una serie de restricciones. Los de pago ofrecen más servicios y espacio.

Algunos de los servicios gratuitos son los ofrecidos por empresas como Dropbox, SkyDrive, HiDrive, Box.net, etc. Uno de los requisitos necesarios para el uso de este tipo de dispositivos es, lógicamente, tener una buena conexión a Internet.

Este tipo de almacenamiento también es conocido como almacenamiento en la nube y se ofrece en las modalidades de *cloud* público y *cloud* privado. En el primero, el acceso al almacenamiento es a través de Internet, que es una red pública. En el segundo, de mayor coste, el proveedor ofrece una red privada virtual (VPN) para el acceso a los datos de forma segura.



Tarjetas perforadas

La tarjeta perforada fue uno de los primeros dispositivos de almacenamiento de información. Tenía el inconveniente de que no podía ser reutilizada. Las perforaciones son una representación de código binario.

Almacenamiento en la nube

El desarrollo de nuevas tecnologías basadas en Internet ha permitido la aparición de las llamadas aplicaciones en la nube. Muchas de estas aplicaciones están enfocadas al respaldo y sincronización de datos con los equipos físicos.

Granjas de servidores

Una granja de servidores es un grupo de servidores que trabajan de manera conjunta para obtener mayor capacidad de cálculo que trabajando de manera independiente. Los servicios que ofrecen son almacenamiento de datos, cómputo por demanda, comunicaciones, etc.

2.3 > Almacenamiento externo

En muchas ocasiones, la necesidad de espacio para el almacenamiento de datos lleva a que las organizaciones adopten soluciones como las de ampliar el número de discos duros o incluso la compra de nuevos servidores. Este tipo de medidas no siempre son la solución. Incluso a veces pueden llegar a empeorar el problema si no se lleva una buena gestión del almacenamiento.

Existen otro tipo de soluciones como pueden ser las ofrecidas por tecnologías como NAS o SAN, que veremos a continuación.

8.1. Sistema NAS QNAP TS 410.

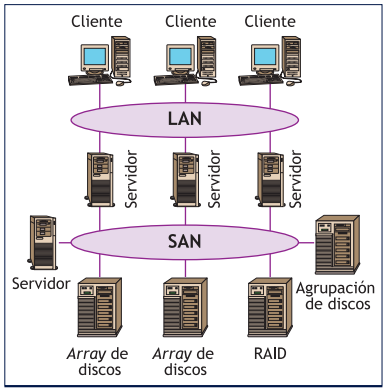
NAS *(Network Attached Storage)*

NAS es una tecnología de almacenamiento accesible desde la red. Permite ampliar la capacidad del sistema sin necesidad de añadir, modificar o cambiar los servidores de la organización.

Los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede a través de protocolos de red, como TCP/IP. Están diseñados para almacenar información y permitir que esté accesible desde los equipos de la red. Muchos de estos sistemas pueden tener más de un dispositivo para incrementar así su capacidad.

Existen distribuciones software específicas para crear sistemas NAS, como por ejemplo **FreeNAS** (basada en FreeBSD), que permite transformar un equipo en servidor NAS.

Los sistemas NAS ofrecen, entre otras funciones, realizar *backups*, tener tolerancia a fallos, balanceo de carga, compartir archivos y capacidad de expansión al poder agregar otros dispositivos.



8.2. Conexión entre red LAN y SAN.

SAN *(Storage Area Network)*

SAN es una alternativa a los sistemas NAS. Su traducción es red de área de almacenamiento.

Esta tecnología crea una red especializada y normalmente complementaria a la red de datos de la organización, para conectar los servidores, los discos de almacenamiento y demás elementos necesarios. Actualmente, algunos fabricantes como Cisco Systems ofrecen sistemas unificados que integran la red de datos y de almacenamiento en una sola infraestructura.

Generalmente utiliza la fibra óptica para poder garantizar una conexión rápida y fiable.

Actividades propuestas

4·· Busca información sobre dos proveedores de servicios de almacenamiento remotos e indica si ofrecen servicio gratuito y cuáles son las características de este. Si ofrecen servicio de pago, indica cuáles son las condiciones del mismo y qué ventajas ofrecen frente al gratuito.

5·· ¿Crees que la solución a la necesidad de espacio para el almacenamiento de información pasa por aumentar el número de discos duros en el servidor? Razona la respuesta.

6·· Busca fabricantes de sistemas NAS y realiza una comparativa entre sus productos.

3 >> Tecnologías de almacenamiento redundante y distribuido

Se conoce como **RAID (*Redundant Array of Independent Disks*)** a la utilización de varios discos sobre los cuales se distribuyen los datos y alguna información adicional. Esta tecnología tiene como finalidad mejorar la tolerancia a fallos y la integridad de los datos, aumentar la capacidad de almacenamiento de los discos e incrementar el rendimiento en las operaciones de lectura y/o escritura.

Para el sistema operativo, la configuración RAID es transparente, de hecho la ve como un único disco lógico. Sin embargo detrás se esconde una tecnología que utiliza la técnica de *stripping* o de división del espacio de cada disco en bandas: almacena los datos junto a información de control que permite que los fallos de disco pasen inadvertidos y que la recuperación de datos sea automática al reemplazar el disco averiado en el RAID.

En función del número de discos, número de bandas, tamaño de las mismas e información de redundancia almacenada en ellas, existen varios niveles de RAID, aunque los más utilizados son los siguientes.

3.1 > RAID 0

Para su implementación se precisa de, al menos, dos discos. La información se distribuye en *stripes* o bandas entre los dos discos con el objetivo de poder acceder más rápidamente a los datos.

Produce un incremento del rendimiento, ya que se puede acceder simultáneamente a los dos discos.

Frente a lo que ocurre con otros RAID, no se produce una pérdida de la cantidad de información que puede almacenarse.

En cambio, presenta el incoveniente de que no se realiza duplicación alguna de la información, por lo que no existe información de redundancia ni tolerancia a fallos (la pérdida de un disco supone pérdida de datos).

3.2 > RAID 1

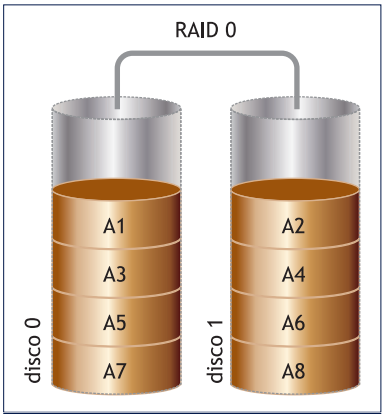
Al igual que RAID 0, necesita de dos discos para su implmentación, pero en este caso, en vez de repartir la información entre ambos, la información se duplica de un disco a otro, por lo que recibe el nombre de *disk mirroring* o discos en espejo.

Dado que cada disco es una copia del otro, se desperdicia la mitad de la capacidad de almacenamiento y no se optimiza esta capacidad, pues su límite vendrá dado por la capacidad del disco de menor tamaño de almacenamiento. A cambio, proporciona máxima seguridad con el menor número de discos.

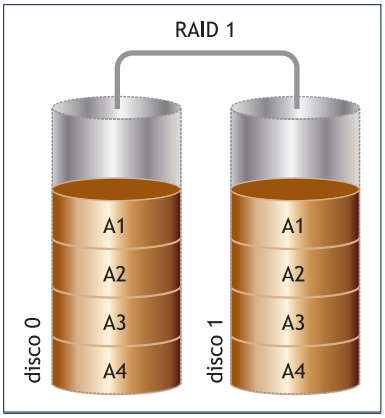
Es el sistema más lento en escritura, si bien las implementaciones más modernas de RAID 1 aprovechan que los datos están copiados en los dos discos para lanzar peticiones de lectura en paralelo a ambos, cada uno con una parte de la información, incrementando así el rendimiento en las lecturas.

Discos duros dinámicos

Windows introduce el concepto de disco dinámico para dar soporte a sistemas tolerantes a fallos mediante el uso de varios discos.



8.3. Diagrama de una configuración RAID 0.

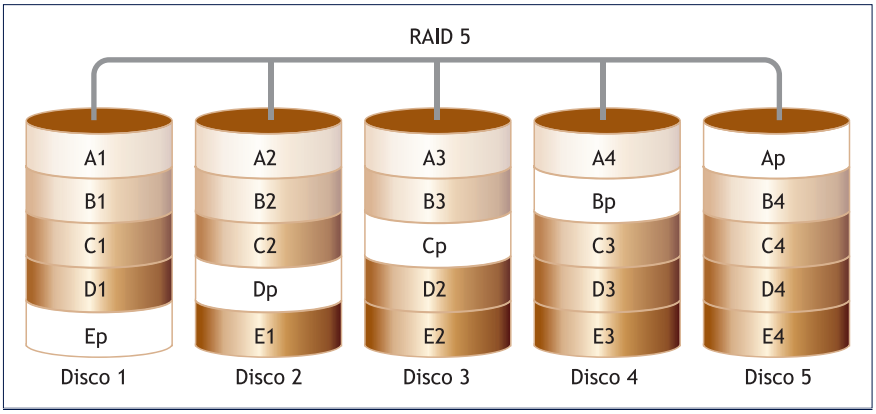


8.4. Diagrama de una configuración RAID 1.

3.3 > RAID 5

Aunque se puede montar con tres discos, lo óptimo es utilizar cinco. La información se reparte en bandas o *stripes*, igual que en el RAID 0, entre cuatro de los discos y, en la banda correspondiente del quinto, en vez de datos, hay información de paridad, de forma que en caso de que se pierda un disco la información es deducible a partir de los discos supervivientes y el disco de paridad. La paridad está repartida en bandas por los cinco discos (es decir, no hay un único disco dedicado a paridad, sino que cada banda dejará los datos de paridad en uno de los cinco discos).

Otras ventajas del RAID 5 son la mínima pérdida de capacidad de almacenamiento de los discos, su tolerancia a fallos y su buen rendimiento general.



8.5. Diagrama de una configuración RAID 5.

En cuanto a los inconvenientes del uso de los RAID, podemos indicar:

- El coste y la complejidad de su configuración pueden llegar a ser altos, dependiendo del tipo de configuración elegidos.
- Se produce una pérdida de capacidad de almacenamiento. Las técnicas de redundancia originan que se disponga de menos capacidad de almacenamiento de la que originalmente se tenía. Esto pasa en todos los casos, excepto en el RAID 0.
- Existe una penalización en el tiempo de escritura. Por ejemplo, en un RAID 5, cuando se graba un dato, al tiempo que se utiliza para su escritura hay que sumarle el tiempo necesario para calcular la paridad y el necesario para escribirla en la banda de paridad.

RAID permite recuperar los datos perdidos al estropearse un disco; no obstante, no es una tecnología de recuperación de datos, por lo que no sería apta para la pérdida de datos a causa de un virus, caso en el que lo idóneo sería el uso de una copia de seguridad.

Uso de los RAID

La mayor parte de los servidores actuales incorporan una controladora de hardware que establece un RAID entre los discos del servidor mediante hardware y, en el caso de las cabinas de almacenamiento SAN, cuando se configura un dispositivo para presentárselo a un servidor, el establecimiento de algún tipo de RAID para el dispositivo es obligatorio.

Actividades propuestas

7·· ¿Cuál es el nivel más alto de RAID que puede implementar un sistema operativo? Cita algunos ejemplos.

8·· ¿Qué quiere decir que RAID 0 no es tolerante a fallos?

4 >> Copias de seguridad

La realización de copias de seguridad de la información es para muchas empresas una tarea todavía pendiente. Muchas veces se toman las medidas adecuadas solo despúes de ocurrir algún accidente.

Una copia de seguridad (en inglés *backup*) es una copia de la información que se realiza como medida preventiva para el caso de que la información original se pierda o se dañe.

4.1 > Clases de copias de seguridad

En función de su contenido, las copias de seguridad pueden ser:

- **Normales o completas**: se copian todos los archivos que indiquemos.
- **Diferenciales:** se copian únicamente los archivos modificados después de la última copia completa.
- **Incrementales:** se copian únicamente los archivos que se hayan modificado después de la última copia completa o diferencial.

4.2 > Realización de copias de seguridad

La realización de las copias de seguridad no es una tarea sencilla, ni se puede hacer de cualquier forma, sino que precisa de una planificación adecuada, que debe tener en cuenta varios aspectos:

- **Datos a incluir en la copia de seguridad:** discos completos, directorios, ficheros, bases de datos, etc.
- **Frecuencia de modificación de los datos:** no es lo mismo hacer copia de ficheros que varían mensualmente que de aquellos que varían diariamente.
- **Frecuencia de la copia de seguridad:** cada cuánto tiempo se va a realizar un *backup* y de qué tipo. Hay que tener en cuenta que, para recuperar una copia de seguridad, necesitaremos la última copia completa y todas las incrementales o diferenciales a partir de esta. Por ello, para datos muy cambiantes no conviene retrasar la realización de la copia de seguridad completa más allá de una semana, ya que, además, si una de las incrementales estuviera en malas condiciones, no podríamos recuperar ninguno de los días posteriores.
- **Tipo de datos:** no es lo mismo hacer copia de registros de bases de datos o de bases de datos completas que de ficheros ordinarios.
- **Uso de los datos durante la realización de la copia:** hay sistemas que no pueden detenerse para poder realizar una copia de seguridad en frío, por lo que precisan de sistemas de copia de seguridad que permitan realizar respaldos de ficheros en uso, tablas abiertas, etc. Lo más habitual es la realización de copias se seguridad durante la noche, ya que disminuye la actividad de los servidores.
- **Tiempo requerido para la recuperación de los datos:** hay información crítica que, en caso de fallo, necesita ser accesible al instante.
- **Política de retención:** cuánto tiempo se va a conservar cada *backup*. La retención influye en las versiones que queremos conservar de los datos. Así, si se hace un *backup* diario con una retención de quince días, podríamos devolver un fichero al estado que tuvo hace quince días.

Copias de seguridad en frío y en caliente

- Copia "en frío": es la que se hace sobre ficheros y bases de datos sobre los que no hay accesos. Para garantizar que no se accede a la base de datos, no hay más remedio que apagar esta.
- Copias "en caliente": es aquella que se realiza sobre ficheros abiertos y bases de datos sobre las que se están realizando operaciones.

Backup remoto

Copias de seguridad en remoto u *online* es un servicio que permite crear copias de seguridad del equipo en un almacenamiento ubicado fuera de la organización, posiblemente en la nube. Un ejemplo de aplicación es Avast!BackUp.

Otro de los aspectos fundamentales para la realización de la copia de seguridad es el soporte o dispositivo en el que se va a llevar a cabo. Para una correcta elección del mismo, hay que tener en cuenta varios datos:

- Capacidad o cantidad de información que puede almacenar.
- Velocidad a la que se realizará la copia y el tiempo de acceso a los datos.
- Tiempo de vida. Estos soportes tienen un periodo de vida limitado, por lo que se debe controlar el tiempo que se quieren conservar los datos y comprobar que el periodo de vida del soporte es mayor.
- La relación de coste por byte, es decir, el precio.

Además, estos soportes deben tener una ubicación física distinta a la del almacenamiento de los datos originales y esta ubicación también debe tener garantizada su seguridad.

Por su parte, los sistemas de *backup* corporativos se apoyan en una infraestructura más compleja que las vistas, con un **servidor centralizado** desde el que se definen, se gestionan y se lanzan los *backups* a todos los servidores. Estos sistemas son capaces de manejar el *backup* con gran flexibilidad, gestionando la realización de copias a disco, la gestión de cintas de *backup*, etc.

Son herramientas complejas que precisan formación *ad hoc* para su administración. Ejemplos de algunos de estos productos son HP DataProtector, Tivoli Storage Manager y CommVault de Simpana Software.

Soluciones para realizar copias de seguridad en Linux

Existen numerosas soluciones específicas, como por ejemplo **tar y gzip, PartImage, Amanda, rsync,** etc.

Ejemplos

Realización de copia de seguridad completa y restauración de la misma con Windows 7

Para realizar una copia de seguridad, recuperar una copia previa ante un fallo o planificar la realización de copias utilizaremos la herramienta *Copias de seguridad y restauración* que lleva integrada Windows 7.

Para ello, en primer lugar, accedemos a la herramienta a través del *Panel de control* / *Sistemas y seguridad* / *Copias de seguridad y restauración*. Como vamos a crear una copia de seguridad, elegimos *Hacer una copia de seguridad del equipo* y luego seleccionamos la opción *Configurar copia de seguridad*.

En la siguiente ventana, elegimos dónde queremos almacenar la copia de seguridad. Vemos que el sistema nos da, incluso, la opción de poder guardarla en una unidad de red.

A continuación debemos elegir los archivos, carpetas, etc. sobre los que queremos hacer la copia. Windows nos da la opción de elegir los archivos o de que estos se seleccionen automáticamente. Seguidamente, se revisa la configuración realizada, pudiéndose realizar una programación automática de la misma. Para ello hay que seleccionar *Cambiar la programación* para elegir con qué frecuencia queremos hacer la copia de seguridad.

Finalmente hacemos clic en el botón *Guardar configuración* y ejecutamos la copia de seguridad.

Para recuperar una copia previa ante un fallo, procederemos del siguiente modo:

- Accedemos a la herramienta de copias, del mismo modo que la creamos, a través del *Panel de control* / *Sistemas y seguridad* / *Copias de seguridad*. Como ahora se trata de restaurar, elegimos la opción *Restaurar mis archivos* o bien *Restaurar todos los archivos de usuarios*.
- A continuación, buscamos los archivos a restaurar, indicamos la ubicación donde se van a restaurar y, finalmente, procedemos a restaurarlos.

Casos prácticos 1

Creación y administración de copias de seguridad con rsync

•• Dispones de un equipo con Linux y debes realizar las siguientes tareas:

a) Realiza, con rsync, una copia de seguridad del directorio *Documentos*, que a su vez contiene otros subdirectorios (*practicas*, *trabajos* y *otros)* y guárdala en un nuevo directorio denominado *copiaseg*, en un disco externo.
b) Modifica uno de los ficheros del subdirectorio *practicas* y vuelve a lanzar el mismo comando de copia.
c) Crea un nuevo fichero en el subdirectorio *practicas* y lanza de nuevo el comando copia.
d) Borra ficheros obsoletos de la copia de seguridad creada.

Solución •• El requisito fundamental para realizar este ejercicio es tener instalado rysnc en el equipo, por lo que, si no lo tienes, descárgalo e instálalo.

a) Para realizar una copia de seguridad rsync, las opciones más utilizadas son las siguientes: `-r` para que recorra toda la estructura de directorios que le indiquemos, `-l` para que copie enlaces simbólicos como enlaces simbólicos, `-p` para que mantenga los permisos, `-t` para que se mantenga la hora del fichero, `-g` para que se mantenga el grupo, `-o` para que se conserve el propietario, `-D` para que se conserven los ficheros de dispositivo (solo para root). No se mantienen los *hard links* (`-H`) ni las ACLs (`-A`) por defecto, `-z` comprime el bloque de datos antes de pasarlo.

Y finalmente, con la opción `-a` obtienes una copia exacta de la jerarquía de ficheros y directorios.

```
-a, —archive archive mode; same as -rlptgoD (no -H, -A)
```

Para llevar a cabo la copia de seguridad en el disco, tienes que escribir su nombre tal y como lo ve el sistema. En este caso, se llama TOSHIBA EXT (debes tener mucho cuidado con las mayúsculas y el espacio en blanco que hay en medio, para que no haya errores).

```
#rsync -av Documentos/ /media/TOSHIBA\ EXT/copiaseg

sending incremental file list
created directory /media/TOSHIBA EXT/copiaseg
./
otros/
otros/imagen1.jpeg
otros/imagen2.jpeg
practicas/
practicas/Practica_rsync.odt
practicas/practica1.txt
practicas/practica2.txt
trabajos/
trabajos/Trabajo1.odt
trabajos/Trabajo2.odt
trabajos/Trabajo3.odt
sent 50848 bytes received 179 bytes 102054.00 bytes/sec
total size is 50206 speedup is 0.98
```

En este caso, vemos que los subdirectorios tenían varios archivos dentro: *otros* (*imagen1* e *imagen2*), *practicas* (*Practica_rsync, practica1* y *practica2*) y *trabajos* (*Trabajo1, Trabajo2* y *Trabajo3*).

1

b) Al modificar un fichero, por ejemplo *practica2*, del subdirectorio *practicas* y volver a lanzar el comando, se observa que solo se ha copiado este fichero.

```
#rsync -av Documentos/ /media/TOSHIBA\ EXT/copiaseg
sending incremental file list
./
otros/
practicas/
practicas/practica2.txt
trabajos/
```

c) Si creas un nuevo fichero, por ejemplo, *practica3*, en el subdirectorio *practicas* y vuelves a lanzar el comando, puedes observar que, de nuevo, solo se ha copiado este fichero.

```
#rsync -av Documentos/ /media/TOSHIBA\ EXT/copiaseg
sending incremental file list
./
otros/
practicas/
practicas/practica3.txt
trabajos/
```

Recuerda que, al pasar directorios o los contenidos de estos, debes tener cuidado en situar o no la barra al final del directorio. Por ejemplo: `rsync /Documentos/trabajos /cpseg`, copia el directorio *trabajos* dentro del directorio *cpseg*, mientras que `rsync /Documentos/trabajos/ /cpseg`, únicamente copia el contenido del directorio *trabajos* en el directorio *cpseg*.

d) Para borrar ficheros obsoletos de la copia de seguridad debes usar la opción `—delete`

Ten mucho cuidado al utilizar esta opción, pues su objetivo es borrar en la copia destino los ficheros que ya no están en el origen. En este caso, borra en el origen el fichero *practica3.txt*. Este fichero sigue en la copia de seguridad; ejecutando el siguiente comando consigues que en el destino desaparezcan los ficheros que no están ya en el origen.

```
#rsync -av —delete Documentos/ /media/TOSHIBA\ EXT/copiaseg
sending incremental file list
./
otros/
practicas/
deleting practicas/practica3.txt
trabajos/

sent 322 bytes received 51 bytes 746.00 bytes/sec
total size is 50267 speedup is 134.76
```

Actividades propuestas

9·· ¿Cuándo recomendarías a una organización utilizar una copia de seguridad normal o completa, cuándo una incremental y cuándo una diferencial?

5 >> Gestión de imágenes del sistema

No hay que confundir la creación de imágenes del sistema con las copias de seguridad vistas en el punto anterior.

La creación de una imagen consiste en la clonación o realización de una copia exacta de un disco o partición. Es decir, una copia de la estructura y contenidos del disco en uno o varios archivos que, además, son comprimidos. En caso de fallo del sistema, para restaurar esa copia basta con transferir la estructura y el contenido del disco o partición donde se realizó la copia o a otro con la mismas características hardware.

Existen varios tipos de clonación:

- **Disco a disco:** se copia todo el contenido de un disco a otro compatible, que puede ser interno o externo.
- **Partición a partición:** se copia una partición en otra, creada anteriormente, que puede estar guardada en el mismo disco o en otro. Si se guarda en el mismo disco, con un gestor de arranque se puede arrancar cualquiera de los dos sistemas.
- **A archivo de imagen:** se copia el disco o una partición en un archivo. Este archivo puede guardarse en cualquier medio (CD, DVD, memorias USB, discos internos o externos).

Existen muchas herramientas, algunas son de pago (como Norton Ghost) y otras se encuentran bajo licencia GPL, como es por ejemplo Clonezilla.

Ejemplos

Clonación de una partición a otra partición utilizando Clonezilla

El primer requisito para llevar a cabo esta práctica es disponer en el equipo una partición libre, que nosotros denominaremos *Seguridad*.

Para crear una imagen de una partición, deberemos arrancar el sistema desde el *live* CD de Clonezilla. Al iniciar, nos dará a escoger entre diferentes modalidades de arranque. En nuestro caso, escogeremos *Clonezilla live (Default settings VGA 800x600)*. A continuación se nos da a escoger entre diferentes configuraciones de idioma. Elegimos *Es_ES.UTF8 Spanish | Español*. La siguiente pantalla se refiere a la configuración de teclado, así que seleccionamos *No tocar el mapa del teclado*.

Llegados a este punto, podemos iniciar el programa seleccionando *Start Clonezilla - Iniciar Clonezilla*. Como modo de trabajo de Clonezilla, elegimos *device-image - De disco o partición a imagen o viceversa*. La siguiente pantalla nos mostrará las opciones de destino para la imagen que vamos a crear. En nuestro caso, seleccionamos *Local Device - Usar dispositivo local (disco duro, USB, etc.)*. Al pulsar <Intro>, el sistema escaneará los dispositivos existentes. Si se va a utilizar un dispositivo USB y aún no se había conectado, ahora es el momento. En este caso, como vamos a utilizar una partición del mismo disco no haría falta esperar a que lo detecte.

En la siguiente ventana, Clonezilla nos mostrará los dispositivos de destino disponibles. Como en este caso vamos a clonar una partición del disco en otra del mismo, seleccionaremos la otra partición existente en el disco, que en nuestro caso, es reconocida por Clonezilla, como:

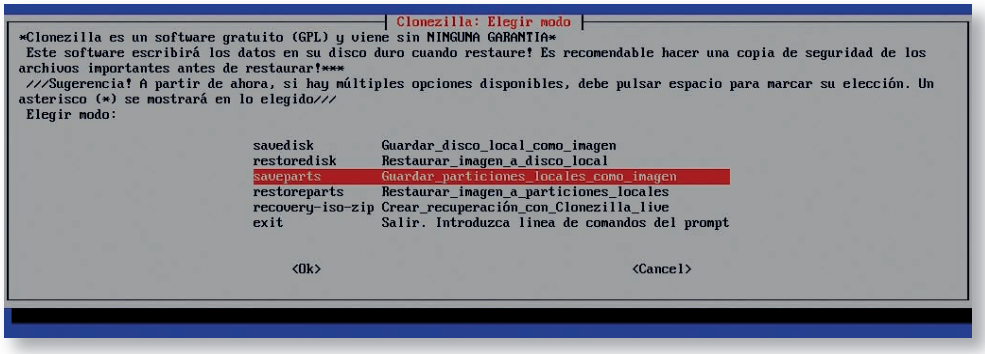
sda5 10.9GB_ntfs_Seg (IN_VOX_HARDDISK_)

A continuación, seleccionamos la carpeta donde almacenar la imagen que se va a crear. Dejaremos la opción que se muestra por defecto: / *Directorio_Superior_en_el_dispositivo_local*.

Dependiendo de la versión de Clonezilla utilizada, puede que se muestre información de todos los dispositivos o unidades actuales conectadas al equipo. Del mismo modo es posible que, en la pantalla siguiente, en función de la versión del programa que se esté usando, se muestren los modos de usuario en que se puede ejecutar Clonezilla.

Existen dos modos de operación con Clonezilla: uno predeterminado para usuarios inexpertos y otro para usuarios avanzados que permite un gran nivel de parametrización. En nuestro caso, elegimos *Beginner – Modo principiante*. Aceptamos las opciones por defecto.

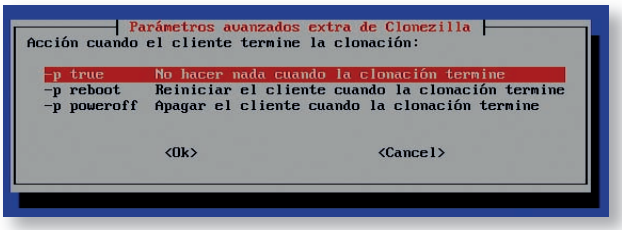
En la ventana *Elegir modo*, se valida lo que se quiere guardar. Si quisiéramos crear una imagen de todo el disco a otro disco del equipo o a un dispositivo externo, deberíamos seleccionar *savedisk – Guardar_disco local_como_imagen*. Sin embargo, como en este ejercicio estamos clonando una partición a otra del mismo disco, elegiremos la opción *saveparts – Guardar_particiones_locales_como_imagen*.



Se abre una ventana en la que se pide el nombre con el que se va a guardar la imagen. Una vez escrito hacemos clic en <*Ok*>. Seleccionamos el disco duro o partición que se quiere clonar y se hace clic en <*Ok*>.

A partir de este momento, el asistente pide que se elijan una serie de parámetros relacionados con la configuración. Si no estamos muy seguros de qué elegir, entonces lo mejor es dejar las opciones marcadas por defecto. Uno de los parámetros avanzados en la configuración que se solicita es el tamaño máximo en MB de los ficheros que se van a crear; si no sabemos qué poner, aceptaremos el valor por defecto (2000) que nos muestra.

Por último, el asistente preguntará qué acción se desea realizar una vez terminado el proceso de clonación. Si no se quiere hacer nada, se puede dejar como opción la que nos muestra por defecto. También se puede reiniciar el equipo o apagarlo. Tanto si marcamos reiniciar el cliente como si elegimos apagar, debemos tener en cuenta que, antes de que se reinicie el equipo la próxima sesión, deberemos extraer el CD de Clonezilla para que el equipo arranque nuevamente desde el disco duro.



Sea cual sea la opción elegida, se nos mostrará a título informativo cómo llevar a cabo las opciones utilizadas a lo largo del asistente mediante la línea de comandos, para que, en futuras ocasiones, resulte más rápido el proceso. Pulsamos <Intro>. A continuación, se nos solicitará confirmación pulsando la tecla <y>.

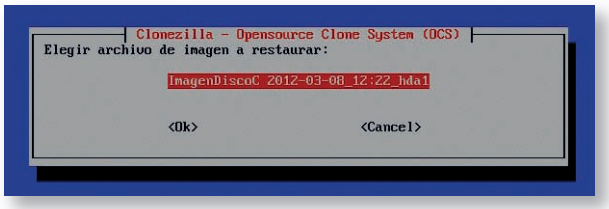
Ejemplos

Restauración de una partición desde otra utilizando Clonezilla

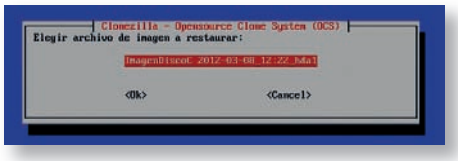
En el ejemplo anterior, clonamos una partición de un disco en otra del mismo disco. Imaginémonos que la partición original ha sido dañada y hemos perdido sus datos o su configuración y queremos restaurarla a partir de la imagen creada, que está guardada en la otra partición.

El primer paso será arrancar el sistema desde el *live* CD de Clonezilla e ir siguiendo los mismos pasos que eran necesarios para crear un archivo de imagen hasta llegar a la pantalla *Elegir modo*.

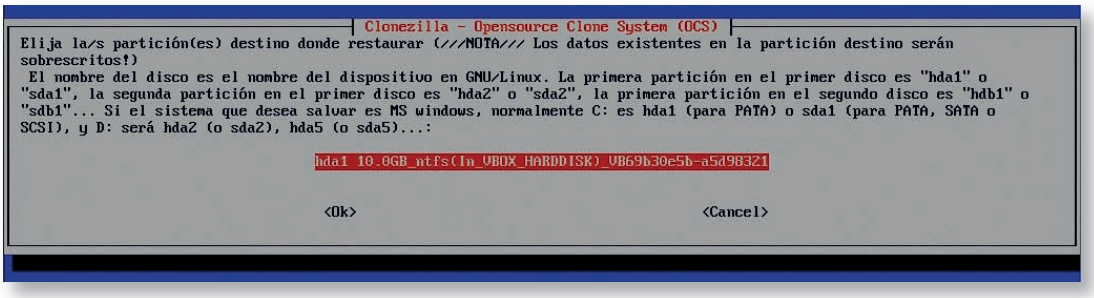
En este caso, como no queremos crear una imagen, sino restaurarla, debemos marcar la opción *restoreparts - Restaurar_imagen_a_particiones_locales*. Si en vez de una partición quisiéramos restaurar un disco completo, deberíamos marcar *restoredisk*.



A continuación, debemos indicar el nombre del fichero de imagen a partir del cual vamos a llevar a cabo la restauración.



Seguidamente, debemos seleccionar la partición en la que vamos a restaurar la imagen.



A partir de este punto, Clonezilla pedirá una serie de parámetros relacionados con la configuración. Si no se está seguro de qué elegir, lo mejor será dejar las opciones que aparecen por defecto.

Como en el caso de la realización de la clonación, se nos mostrará a título informativo cómo llevar a cabo las opciones utilizadas a lo largo del asistente mediante la línea de comandos. Pulsamos <Intro>. A continuación, se nos solicitará confirmación, advirtiendo de que los datos existentes serán sobrescritos y por tanto se perderán. Si estamos seguros, pulsamos la tecla <y>. Comienza el proceso de restauración de la imagen. Ahora ya no hay vuelta atrás.

Una vez finalizado el proceso, se nos mostrará una ventana con los detalles. Pulsamos <Intro>. Por último, se pedirá la acción que se desea que se realice una vez terminado el proceso de restauración (no hacer nada, reiniciar el equipo o apagarlo).

Actividades propuestas

10·· Indica en qué situaciones es interesante utilizar este sistema de recuperación.

11·· Haz una comparativa de Clonezilla con otras herramientas para la creación de imágenes.

6 >> Recuperación de datos eliminados

En apartados anteriores, hemos visto cómo se pueden recuperar los datos a partir de una copia de seguridad creada o cómo, a partir de una imagen, se puede restaurar la configuración del equipo para llevarlo a un estado anterior.

Pero existen otras circunstancias que pueden llevarnos a no poder recurrir a los anteriores mecanismos para recuperar datos perdidos. Por ejemplo, puede ocurrir que tras actualizar o instalar un nuevo controlador de dispositivo o un nuevo programa, el equipo empiece a comportarse de manera extraña.

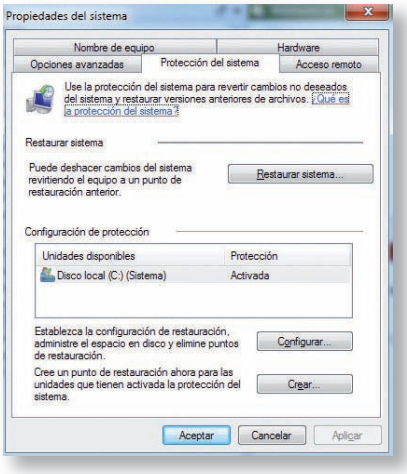
En estos caso, en lugar de clonar el equipo o restaurar el sistema a partir de una copia de seguridad, se puede recurrir a pasar a un estado anterior del sistema mediante lo que se conoce como **punto de restauración**.

Ejemplos

Utilización de los puntos de restauración en Windows 7

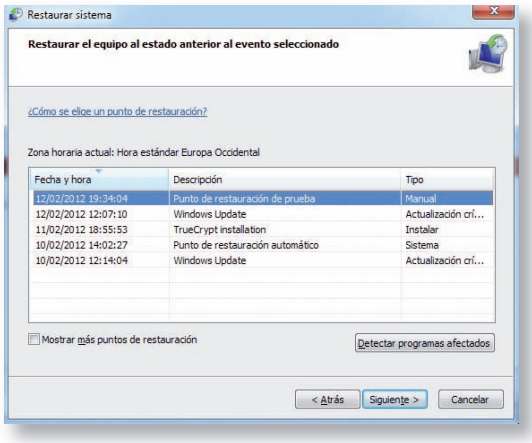
En esta práctica vamos a crear un punto de restauración en Windows 7 y, posteriormente, vamos a restaurar el sistema a partir de un punto de restauración creado con anterioridad.

El primer paso, por tanto, será ver cómo se crea un punto de restauración. Para ello, accedemos a la herramienta desde *Panel de control* / *Sistema y seguridad* / *Sistema*.



Al hacer clic sobre el enlace *Protección del sistema* del margen izquierdo, se abre la ventana *Propiedades del sistema*, donde hay que activar la pestaña *Protección del sistema*.

Hacemos clic en el botón *Crear* y se nos pedirá una descripción para ayudar a identificar posteriormente el punto de restauración creado. Conviene ser lo más descriptivo posible para luego encontrarlo fácilmente. Por ejemplo, *Instalación Adobe Acrobat 9* puede indicar que hemos creado el punto de restauración justo antes de la instalación de ese programa; si esa instalación ocasiona un problema, podemos volver al momento inmediatamente anterior a realizarla.



Para restaurar el sistema a partir de un punto creado, accedemos a la herramienta desde la misma ventana y pestaña que utilizamos para crear el punto de restauración, pero ahora hacemos clic en el botón *Restaurar sistema*. Eso iniciará el asistente para la restauración de archivos y configuración del sistema, que nos permitirá elegir uno de los puntos de restauración creados.

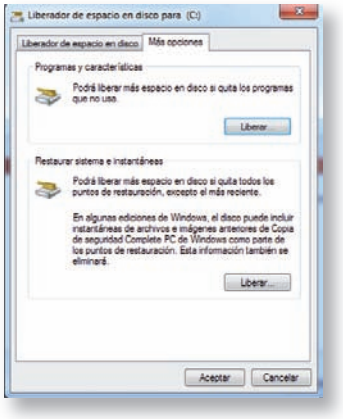
Finalmente, se muestra un resumen del punto elegido y se nos pide la confirmación para continuar con el proceso.

El sistema se reiniciará para poder aplicar los cambios y restaurar el sistema desde el punto elegido.

Dada la utilidad que proporcionan los puntos de restauración, el único problema que pueden ocasionar es su uso inmoderado, debido al espacio que ocupan en el disco. No obstante, eso no supone mayor problema si vamos borrando periódicamente los puntos más antiguos.

Ejemplos

Liberación de espacio en disco mediante el borrado de puntos de restauración en Windows 7



En Windows 7 accedemos al menú de Inicio / *Todos los programas* / *Accesorios* / *Herramientas del sistema* / *Liberador de espacio*.

Seleccionamos la pestaña *Más opciones*. En la sección de *Restaurar sistema e instantáneas* hacemos clic en el botón *Liberar*.

A continuación, nos pregunta si se quieren borrar todos los puntos de restauración creados excepto el último.

Si hacemos clic en el botón *Aceptar*, podremos comprobar que efectivamente se ha liberado espacio en disco.

Estos sistemas de restauración son muy útiles, pero hay ocasiones en que el equipo ni siquiera es capaz de arrancar el sistema operativo. En este caso, no puede utilizarse la opción anterior.

Una posible solución, antes de recurrir a la restauración del sistema mediante una imagen, sería intentar iniciar el sistema utilizando la última configuración que funcionó correctamente; es lo que se conoce como **"modo a prueba de fallos"**. Se puede acceder a esta opción mediante el menú que aparece al pulsar la tecla **<F8>** antes de iniciar el sistema operativo.

Ahora imaginemos otra situación. Podría ser posible que, voluntaria o accidentalmente (virus, corte de corriente, etc.), se formateara o borrara un medio de almacenamiento de datos (disco, memoria USB, etc.) y que no tuviéramos ninguna copia de seguridad o fueran muy antiguas. En este caso habría dos posibles opciones:

- Posiblemente, la mejor solución, pero con un elevado coste económico, sería acudir a empresas especializadas en extraer información de soportes dañados.
- La otra solución, más económica pero que no siempre tiene garantías de éxito, sería la utilización de alguna aplicación que nos permitiera recuperar la máxima información posible.

Hay numerosas aplicaciones, tanto de pago como gratuitas, disponibles para cualquier sistema de ficheros. En esta unidad vamos a ver la aplicación **GetDataBack.** Se trata de una herramienta bastante potente que cuenta con una versión para recuperar ficheros sobre sistemas de archivos NTFS y otra para hacerlo sobre FAT. Es una aplicación comercial pero existe una versión de prueba que, al menos, muestra los archivos a recuperar.

Ejemplos

Recuperación de datos utilizando GetDataBack

Antes de comenzar a utilizar el programa GetDataBack hay que tener en cuenta las siguientes normas:

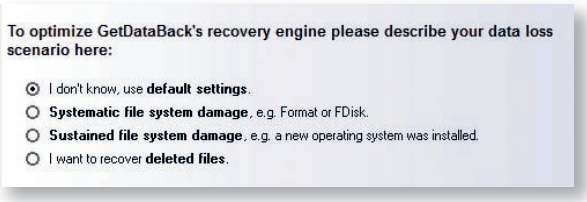
- En primer lugar, a la hora de instalar la aplicación, hay que tener en cuenta que nunca debe realizarse esta instalación sobre el disco o unidad de la que se quieren recuperar los datos. Por ejemplo, si se quieren recuperar los datos del disco D:, entonces la aplicación se instalará en C.
- En segundo lugar, es conveniente crear una carpeta en una unidad, partición o disco diferente del que se van a recuperar los datos, porque es posible que el programa no dé la opción de crearla luego.
- Finalmente, los datos recuperados nunca se deben guardar en el mismo disco, unidad o partición de la que se están recuperando.

Si la unidad que queremos recuperar es el disco del sistema, es recomendable conectarlo a otro equipo como disco secundario.

Instalamos el programa en la unidad C. Una vez instalado, accedemos a él a través del menú de Inicio / *Todos los programas* / *Runtime Software-Getdataback*. En todo caso, hay que ejecutar el programa como Administrador.

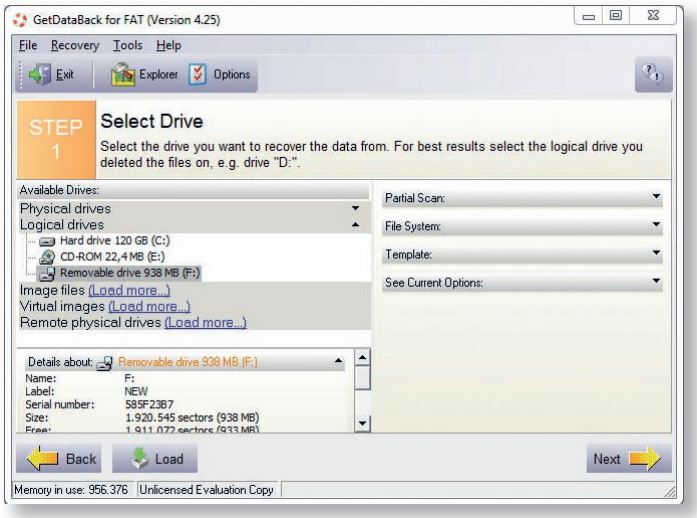
En la ventana de *Inicio* nos pide, entre otras cosas, que se elija el mejor escenario de pérdida de datos en el que nos encontramos. Las opciones son:

- Utilizar la configuración por defecto (si no estamos seguros).
- Daño sistemático en el sistema de archivos, por ejemplo, tras usar format o fdisk.
- Daño sostenido del sistema, por ejemplo tras la instalación de un nuevo sistema operativo.
- Recuperación de ficheros borrados.



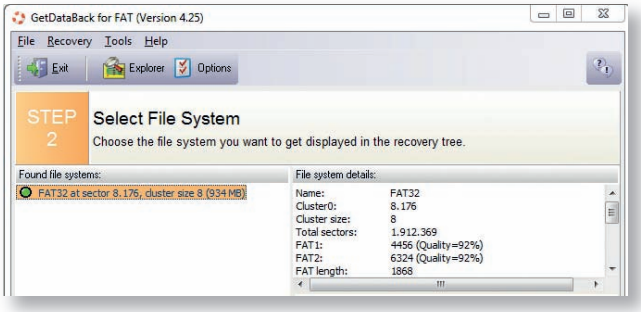
En este caso práctico, vamos a ver cómo recuperar ficheros borrados, por lo que seleccionamos la última casilla de verificación.

En la siguiente ventana se puede escoger la unidad desde la que se quieren recuperar los datos. A la izquierda, se muestran todas las unidades detectadas. En nuestro caso, elegimos recuperarlos desde el dispositivo USB, que es donde los tenemos copiados, por eso seleccionamos la unidad (F:).



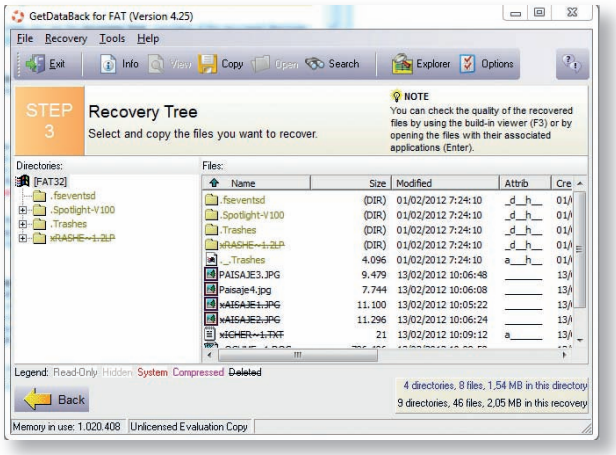
En el siguiente paso, comienza el proceso de escaneo en la unidad elegida (en nuestro caso F:) en busca de ficheros para recuperar.

Una vez finalizado el escaneo, se muestra en la parte izquierda los sistemas de ficheros que ha encontrado. En este caso FAT32.



Se elegirá el sistema de ficheros del cual queremos recuperar y continuaremos el proceso haciendo clic en el botón *Next*. En este caso solo se ha detectado un sistema, con lo cual no hay dudas sobre cuál elegir.

A continuación, se muestran los archivos a recuperar.



Situándonos sobre cualquiera de los archivos recuperados, con el botón secundario del ratón y seleccionando *Show information*, se pueden observar más detalles del fichero a recuperar.

Para recuperar los ficheros, habrá que seleccionarlos, elegir la opción *Copy* y dar la ruta donde queremos copiarlos. En la versión de prueba del software no podremos hacerlo, ya que para ello habría que utilizar la versión de pago.

Actividades propuestas

12·· Busca en Internet otras herramientas para la recuperación de información, además de la explicada en este epígrafe, sean o no gratuitas, y realiza una comparativa entre ellas.

13·· Busca en Internet empresas que se dediquen a la recuperación de datos.

Actividades finales

.: CONSOLIDACIÓN :.

1·· Indica errores humanos típicos que ponen en peligro la seguridad de nuestros datos.

2·· ¿En qué consisten las políticas de almacenamiento?

3·· ¿Qué ventajas ofrecen los servicios de alojamiento de datos remotos? ¿Utilizas alguno? ¿Cuál?

4·· ¿Qué diferencia encuentras entre un dispositivo NAS y un disco duro en red?

5·· ¿En qué consiste un RAID y qué ventajas ofrece? ¿Si tuvieras que instalarte un sistema RAID en tu casa, qué nivel elegirías? ¿Por qué?

6·· ¿Cuál crees que sería el RAID óptimo para un sistema de base de datos donde hubiera pocas modificaciones y muchas consultas? ¿Y para un sistema donde interesara tener un rendimiento muy alto pero no importaran demasiado las pérdidas de datos?

7·· Realiza un cuadro comparativo indicando las ventajas e inconvenientes de los siguientes tipos de copias: total o completa, diferencial e incremental.

8·· ¿Qué ventajas e inconvenientes proporciona un servicio de copias de seguridad remotas en lugar de uno tradicional?

9·· ¿Qué diferencias hay entre realizar una copia de seguridad y crear una imagen del sistema? Indica situaciones en las que es más recomendable utilizar una u otra.

10·· Haz un resumen de los métodos para recuperar datos vistos a lo largo de la unidad, poniendo para cada uno de ellos un ejemplo de uso.

11·· Indica si las siguientes afirmaciones son verdaderas o falsas. En caso de ser falsas indica por qué.

a) En una configuración RAID 5, cada disco guarda una quinta parte de la información.
b) Una buena política de gestión de imágenes del sistema consistiría en realizar semanalmente una imagen de todo el sistema y diariamente una incremental.
c) Las copias de seguridad consisten en la clonación o realización de una copia exacta de un disco o partición.

.: APLICACIÓN :.

1·· Programa una copia de seguridad incremental de tu ordenador para que se lleve a cabo una vez a la semana. Realiza un manual que muestre el proceso que has seguido.

2·· Una empresa de reciente creación está buscando asesoramiento sobre el tema de las copias de seguridad.

a) ¿Qué medios de almacenamiento le recomendarías?
b) ¿Qué recomendaciones sobre la política de copias de seguridad le harías?

3·· ¿Qué recomendaciones darías a una organización para garantizar la integridad de las copias de seguridad realizadas?

4·· Busca herramientas gratuitas para realizar copias de seguridad. Selecciona una de ellas, instálatela y utilízala. Realiza un pequeño manual de su uso.

5·· Busca herramientas comerciales para la realización de copias de seguridad y haz una comparativa.

6·· Elige una de las herramientas para recuperar datos del listado que hiciste en la actividad propuesta 12 de esta unidad, instálala y utilízala. Crea un pequeño manual de uso.

Caso final 2

Copias de seguridad

•• La empresa PIXMOVIE, SL está muy preocupada por el tema de la seguridad de sus datos. Por ello, está buscando a un experto que elabore un proyecto para mejorar su política de seguridad de datos.

Elabora un proyecto donde se incluya una politica de seguridad, una programación de copias de seguridad, los medios de almacenamiento más recomendables, etc.

Solución •• La solución está abierta a múltiples opciones. A continuación mostramos una de ellas.

a) Elaboración de una política de almacenamiento de la empresa, que incluya, entre otros aspectos:
- El uso de los dispositivos de almacenamiento fuera de la empresa.
- ¿Qué está permitido almacenar en los dispositivos de la empresa y qué no lo está?
- ¿Quiénes son los responsables del uso de los dispositivos?

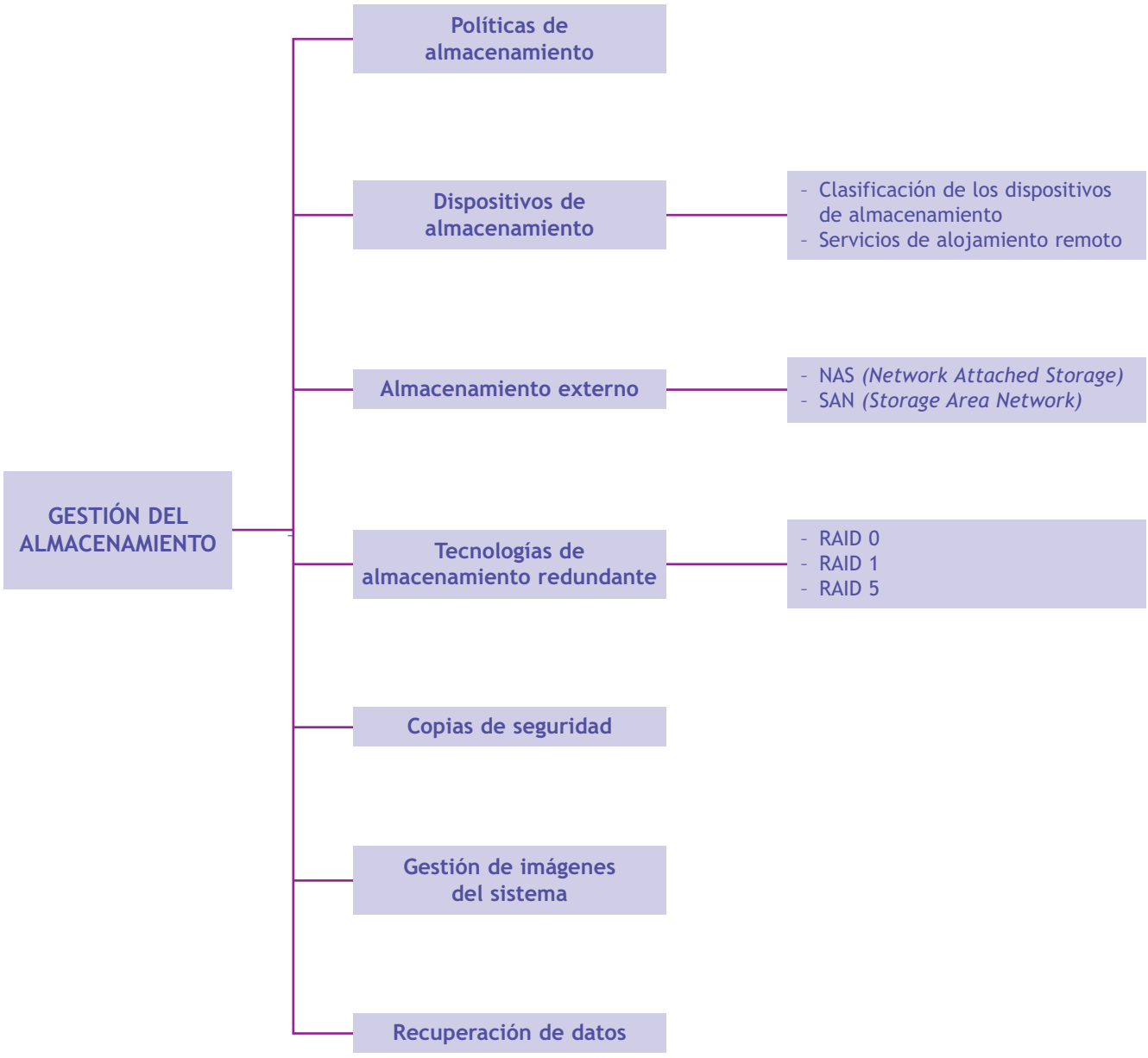
b) Propuesta de la compra de una aplicación comercial para la realización y gestión de copias de seguridad que incluya el servicio de mantenimiento. Se debe justificar por qué se ha elegido esa aplicación frente a otras posibles alternativas.

c) Realización de una propuesta de programación de las copias de seguridad.
- **Copias totales:** se creará una copia total al inicio del proyecto y el primer día de cada mes. Las copias se realizarán cuando menos actividad tenga la empresa, por ejemplo a las 23:00 h.
- **Copias incrementales:** cada día se creará una copia incremental excepto el día que se haga la copia total. Estas ocupan menos tiempo y espacio.
- **Copia diferencial:** se realizarán cada viernes y todos los últimos días de cada mes, excepto cuando estos días coincidan con una copia total. Para ahorrar espacio de almacenamiento, estas copias se irán sobrescribiendo cada dos semanas, exceptuando la del final de mes, que se guardará para poder llevar un registro de todo lo almacenado durante el mes. Estas copias también deberán ser realizadas cuando menos actividad tenga la empresa, por ejemplo a las 23:00 h.

d) Almacenamiento de las copias de seguridad. Una vez reunidos con los responsables de la empresa, se constata que el volumen de datos a almacenar va a ser elevado, por lo que se propone el siguiente plan de almacenamiento de las copias de seguridad de la organización:
- Situar un servidor de almacenamiento por departamento.
- A través de la red local y con una configuración de subredes, cada departamento almacenará las copias de seguridad en el servidor.
- Para garantizar la integridad de los datos, el servidor dispondrá de una serie de discos de gran tamaño configurados en RAID 1.
- Los administradores tendrán acceso a todos los servidores de almacenamiento.

e) Medios de almacenamiento. Se realiza una propuesta de presupuesto de los servidores y medios de almacenamiento necesarios:
- Propuesta de un servidor de almacenamiento, con prestaciones similares al QNAP TS-410 NAS por departamento.
- Dos discos duros extraíbles preparados para servidores.
- Presupuesto total no superior a 800 €.
- Contratación de un alojamiento remoto para almacenar la copia de seguridad mensual en ella con una previsión de un año vista en copias de seguridad.

Ideas clave


GESTIÓN DEL ALMACENAMIENTO
Políticas de almacenamiento
Dispositivos de almacenamiento
- Clasificación de los dispositivos de almacenamiento
- Servicios de alojamiento remoto
Almacenamiento externo
- NAS (Network Attached Storage)
- SAN (Storage Area Network)
Tecnologías de almacenamiento redundante
- RAID 0
- RAID 1
- RAID 5
Copias de seguridad
Gestión de imágenes del sistema
Recuperación de datos

Solo un tercio de las organizaciones que usan la nube protegen adecuadamente sus datos

Un 62% de las organizaciones utiliza la nube o la virtualización, pero solo un tercio reconoce comprobar de forma regular sus planes de recuperación de datos para asegurarse de que cuentan con los protocolos correctos para proteger sus datos.

Estos datos se extraen de un estudio realizado por Kroll Ontrack entre 367 empresas y proveedores de servicios. El mismo estudio pone de manifiesto que un 49% de las organizaciones sufrió algún tipo de pérdida de datos el pasado año, aunque no en todos los casos tuvo lugar necesariamente desde la nube. En un 55% de los casos, la pérdida de datos provenía de un soporte tradicional de almacenamiento, mientras que un 26% se daba en un entorno virtual, un 3% en la nube y un 16% perdió los datos en ambos formatos, virtual y en la nube.

"Está claro que la nube está ganando terreno rápidamente entre las organizaciones que buscan racionalizar sus infraestructuras tecnológicas y reducir costes en tecnologías de la información (TI). Entre los encuestados, un 26% afirma utilizar la infraestructura como servicio (IaaS); un 16% el software como servicio (SaaS); y un 13% utiliza ambos", declara Nicholas Green, director general de Kroll Ontrack Iberia. "Sin embargo, si hay algo que la tecnología nos ha enseñado es que la pérdida de datos puede ocurrir en cualquier entorno, sin importar la tecnología utilizada. La clave para minimizar el riesgo de la pérdida de datos y recuperarlos con éxito está en hacerse las preguntas adecuadas antes de adoptar un nuevo método de almacenamiento, y modificar de manera acorde tus políticas y procedimientos", afirma Green.

Algunas preguntas que hay que considerar antes de incorporar la nube en la arquitectura de almacenamiento son:

- ¿Tiene la empresa un sistema de *backup* y protocolos de actuación previstos? ¿Están alineados estos sistemas de *backup* y protocolos con las políticas internas de tu empresa?
- ¿Tiene tu proveedor de la nube identificado un proveedor de recuperación de datos en su plan de continuidad/recuperación de desastres?
- ¿Cuáles son los niveles de acuerdo del servicio en lo que respecta a la recuperación de datos, fiabilidad en la pérdida, reparación y consecuencias en el negocio?
- ¿Puedes compartir datos entre distintos servicios en la nube? En el caso de finalizar el contrato con un servicio en la nube, ¿puedes recuperar los datos? Si es así, ¿en qué formato? ¿Cómo puedes asegurarte de que se destruyen todas las copias?

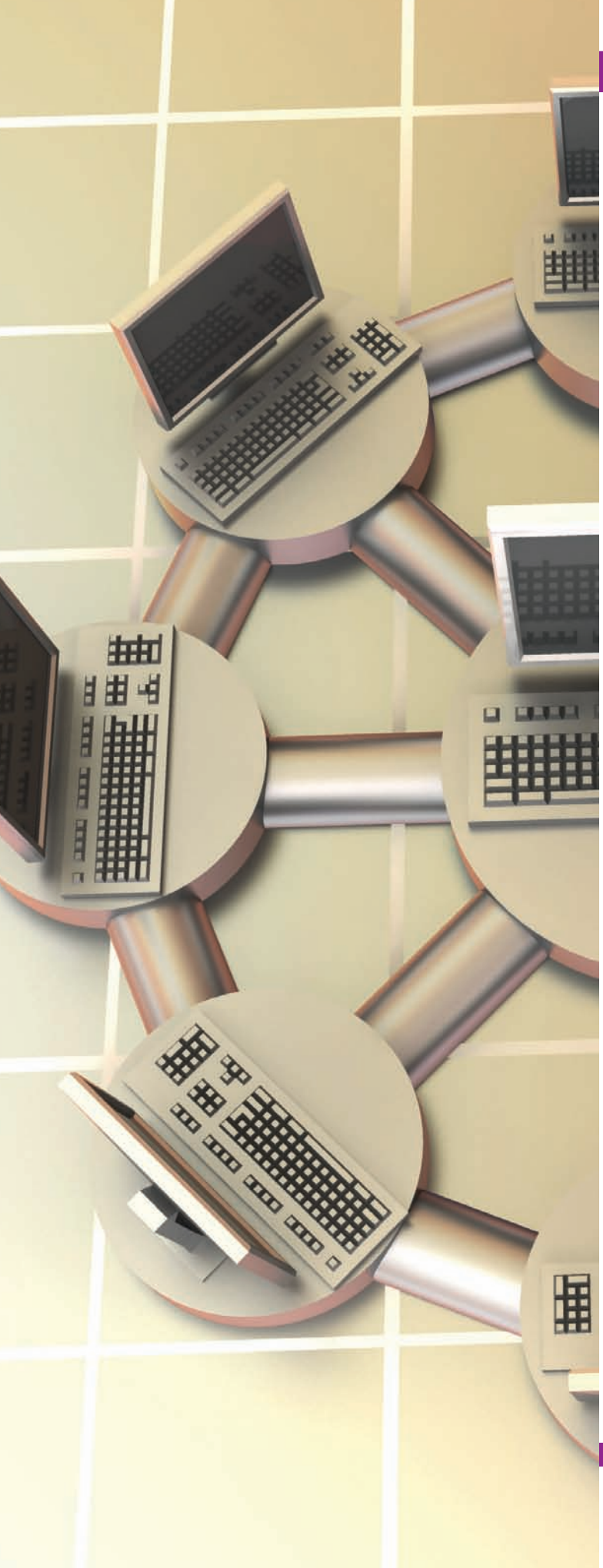
Ante la pregunta sobre la capacidad de los proveedores de la nube para gestionar un incidente de pérdida de datos de forma correcta, solo un 29% reconoció tener falta de confianza, frente al 55% obtenido en el mismo estudio realizado en 2011. Sin embargo, solo un 17% de los encuestados afirmó comprobar regularmente su plan de recuperación de datos para validar la disposición tanto técnica como personal ante una recuperación de datos, ya sea en la nube o virtual, y un 13% reconoció no tener un plan de recuperación de datos.

"La virtualización es el motor de la tecnología en la nube. Si la virtualización falla, la nube falla", añade Green.

Fuente: www.haycanal.com. Extracto del artículo publicado el 09/10/2012.

Actividades

1·· Debate con tus compañeros sobre las ventajas e inconvenientes del uso de la nube para el almacenamiento y la gestión de los datos de las empresas.



unidad 9

Seguridad en redes

SUMARIO

- Vulnerabilidades de los servicios en red
- Monitorización
- Técnicas de protección
- Seguridad en los protocolos para redes inalámbricas
- Auditorías de seguridad informática

OBJETIVOS

- Estudiar las vulnerabilidades existentes en la comunicación entre equipos.
- Conocer qué es una herramienta de monitorización y cómo nos puede ayudar a mejorar la seguridad de una red.
- Aprender cómo funcionan y cómo nos pueden ayudar algunas herramientas de protección de redes como cortafuegos, *proxies* o detectores de intrusos.
- Conocer los mecanismos de seguridad en redes inalámbricas y sus vulnerabilidades.
- Aprender qué es una auditoría de seguridad informática y para qué se utiliza.

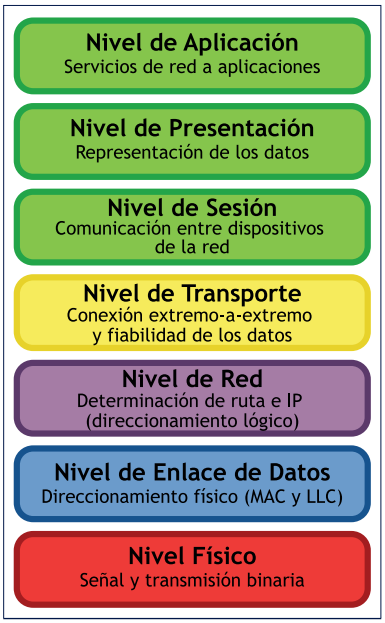
1 >> Vulnerabilidades de los servicios de red

Hoy en día, el uso de las telecomunicaciones permite que una persona pueda jugar en red con otra que se encuentra al otro lado del mundo, utilizar su teléfono móvil para navegar por Internet o incluso gestionar su vivienda desde el trabajo mediante aplicaciones domóticas. Todo esto es posible gracias a las comunicaciones en red.

No obstante, estas comunicaciones entre equipos a través de la red no están exentas de riesgos que debemos conocer. Para entender estos riesgos, conviene conocer cómo funcionan las redes de telecomunicación y estudiar sus vulnerabilidades.

Las redes de telecomunicación basan su funcionamiento en el **modelo OSI** de interconexión de equipos informáticos, que define **siete capas** o niveles, de manera que cada nivel tiene una funcionalidad bien definida y se comunica mediante una interfaz que oculta los detalles de implementación al resto de niveles facilitando su uso por los niveles inmediatamente inferior o superior, que son los únicos que podrán acceder a él. Por ejemplo, el nivel 4 (nivel de transporte) solo puede enviar y recibir información de los niveles 3 (nivel de red) y 5 (nivel de sesión).

Cada nivel del modelo OSI presenta vulnerabilidades que pueden ser explotadas por un atacante, por lo que en los próximos apartados estudiaremos las vulnerabilidades de los niveles de este modelo.



9.1. Pila del modelo OSI.

1.1 > Nivel físico

Este nivel es responsable de la conexión del equipo informático a la red y se encarga de la transmisión de información a través de ella. Las vulnerabilidades de este nivel están relacionadas con el acceso físico no autorizado a los dispositivos de red.

Algunos ejemplos de ataques sobre este nivel son: corte o desconexión de un cable de red o interferencias electromagnéticas ocasionadas por algún dispositivo que impidan el funcionamiento normal de la red.

Estos ataques pueden tener un gran impacto sobre el funcionamiento de los equipos informáticos, independientemente de si se han producido de forma accidental o intencionada, por lo que deberemos tenerlos en cuenta y controlar el acceso físico a los dispositivos de red.

1.2 > Nivel de enlace de datos

Se encarga del direccionamiento físico, acceso al medio, la detección de errores, la distribución ordenada de tramas y del control de flujo. Aquí se dan vulnerabilidades asociadas al medio sobre el que se realiza la conexión, como el control de acceso y la confidencialidad. Algunos ataques son:

- **Escuchas de red**, tanto intrusivas en medios cableados (pinchar un cable), como no intrusivas en medios inalámbricos (ataques WEP).
- **Falsificación de direcciones MAC** para evitar restricciones de acceso basadas en el filtrado MAC.
- **Envenenamiento ARP**.

Envenenamiento ARP

El envenenamiento ARP o *ARP poison*, también conocido como ataque *man in the middle (MITM)*, es un tipo de ataque donde el intruso intercepta el tráfico enviado a otra estación o al *router*, atendiendo a peticiones dirigidas a otras estaciones y suplantándolas.

1.3 > Nivel de red

Este nivel proporciona conectividad entre equipos, permitiendo que la información llegue desde el origen al destino aunque se encuentren en redes diferentes. Esto es posible gracias a la información de cabecera que contienen todos los paquetes IP y a la utilización de elementos que permiten la interconexión de redes como *routers*. Este nivel presenta vulnerabilidades asociadas a la integridad y confidencialidad de la información. Se pueden dar los siguientes ataques:

- **Suplantación de mensajes** (*IP spoofing,* en inglés). El atacante envía paquetes utilizando una dirección origen diferente, modificándola por una dirección IP falsa o de otro equipo legítimo de la red.
- **Denegación de servicio** (*Denial of Service*, en inglés o **DoS**). Los atacantes realizan ataques de inundación de la red (*IP flooding* o *net flood,* en inglés), que consisten en generar un elevado tráfico de red hacia una víctima con el objetivo de saturar su línea de comunicación. Existe una gran variedad de ataques de denegación de servicio y en la mayoría se trata de manipular los paquetes alterando algún campo o lanzando una gran cantidad de peticiones al resto de estaciones.

Smurfing

Es una técnica de DoS muy utilizada que consiste en envíar una gran cantidad de paquetes ICMP *(ping)* a la dirección de *broadcast*, falsificando la dirección de origen por la de la víctima, que recibirá la respuesta de todas las estaciones de la red.

1.4 > Nivel de transporte

Este nivel proporciona un servicio de transporte desde la máquina origen a la de destino, independizándolo del hardware de red utilizado. Los protocolos más conocidos son TCP y UDP, que transmiten información sobre paquetes IP. Las vulnerabilidades de este nivel se asocian a la autenticación, integridad y confidencialidad de la información.

Algunos ataques sobre este nivel son:

- **Denegación de servicio**, que como se ha comentado utiliza técnicas de IP *flooding* sobre datagramas UDP, TCP o ICMP. Una variante muy interesante es la inundación SYN (*SYN flooding,* en inglés), donde el atacante no completa el establecimiento de conexión TCP a propósito. Esto provoca que el servidor desperdicie recursos manteniendo conexiones que no serán utilizadas, por lo que se podría provocar el colapso en la máquina. Esta debilidad se debe a una pobre implementación del protocolo TCP, que fue aprovechada en las primeras implementaciones de la pila TCP. En la actualidad, los servidores suelen liberar las conexiones no utilizadas con rapidez, por lo que el problema debería estar solucionado.
- **Ataques contra el establecimiento de sesiones TCP**, que consisten en la interceptación de sesiones TCP establecidas para redirigirlas a otros equipos. Este tipo de ataques se aprovechan de la simplicidad del proceso de autenticación entre equipos, lo que puede ser aprovechado por un atacante a la escucha de los intercambios de información realizados en el inicio de la sesión.
- **Ataques de reconocimiento**, que consisten en realizar barridos de puertos TCP/UDP contra un equipo y de esta forma averiguar qué aplicaciones y puertos tiene en escucha para poder realizar un ataque posterior a un determinado servicio.

Denegación de servicio en televisores

Los ataques de denegación de servicio pueden atacar a cualquier dispositivo que utilice la red para enviar y recibir información, por lo que los teléfonos móviles, lectores de *Blu-ray* que se actualizan a través de la red o televisores que acceden a Internet pueden verse afectados.

El pasado mes de abril de 2012 se detectó una vulnerabilidad en una conocida marca de televisores que podía ocasionar una denegación de servicio al enviarle un paquete de red manipulado.

1.5 > Niveles de sesión, presentación y aplicación

Los niveles superiores son los más cercanos al usuario y se suelen agrupar para facilitar su estudio. Estos niveles desconocen la forma en la que se comunican los equipos y la ruta establecida y se encargan de definir los protocolos de aplicación que utilizan las aplicaciones finales para intercambiar datos. No obstante, estos niveles presentan muchas vulnerabilidades que afectan a la confidencialidad, integridad, disponibilidad, no repudio o autenticación, que pueden ser aprovechadas por atacantes.

Existe una gran variedad de ataques que aprovechan las vulnerabilidades de estos niveles:

- **Ataques sobre la confidencialidad.** Algunas aplicaciones presentan fallos importantes de seguridad y envían toda la información de la sesión sin cifrar (como telnet o FTP), por lo que un atacante podría obtener las claves de sesión usando programas de escucha de la red.
- **Suplantación del servicio de nombres de dominio** (*pharming*, en inglés). Cuando se solicita una petición sobre un servicio en un equipo remoto se debe conocer la dirección IP de ese equipo. Para ello se realiza una consulta sobre el servidor DNS enviándole un paquete UDP al servidor DNS que proporciona la dirección IP del destino. En este tipo de ataque se suplanta al servidor DNS, suministrando una dirección IP falsa que será utilizada por la víctima sin saberlo, accediendo a una página web falsa que imitará la página web legítima con la finalidad de obtener información importante de la víctima, como sus contraseñas.
- **Agotamiento de direcciones IP** (*DHCP starvation*, en inglés), que consiste en enviar una gran cantidad de peticiones al servidor DHCP con distintas direcciones físicas de origen para obtener una dirección IP diferente cada vez, con lo que se podría agotar las direcciones IP disponibles para el resto de equipos legítimos.
- **Inyección SQL** (*SQL injection*, en inglés), que aprovecha vulnerabilidades en el diseño de una aplicación web para ejecutar código SQL no esperado sobre una base de datos. Mediante este tipo de ataques se altera el funcionamiento normal de la consulta original y se consigue ejecutar operaciones de actualización o consultas no esperadas. Así, por ejemplo, una operación de consulta sobre una tabla modificada convenientemente puede dar como resultado la visualización de información de tablas para las que no se tiene acceso o a borrar su contenido.
- **Escalada de directorios,** que consiste en acceder a directorios para los que no se debería tener acceso. Existen muchas aplicaciones que permiten a usuarios acceder a directorios de un equipo remoto, lo que presenta problemas de seguridad si facilita el acceso a todos los directorios del equipo. Estas aplicaciones suelen proporcionar herramientas que permiten el "enjaulamiento" de los usuarios remotos para limitar el acceso solo a los directorios autorizados.
- **XSS** (*Cross Site Scripting*, en inglés), que consiste básicamente en inyectar código malicioso en las páginas web visitadas.
- **Desbordamiento de búfer,** que consiste en aprovechar algún fallo de diseño de una aplicación con el objetivo de ejecutar código malicioso en el ordenador de la víctima.

Defensa contra el agotamiento de direcciones IP

Una posible defensa sobre este tipo de ataque sería limitar la cantidad de peticiones DHCP que se puede realizar por cada puerto del *switch* o configurar la seguridad por puerto para que solo permita que determinadas direcciones físicas estén conectadas a un puerto y deniegue el resto.

1.6 > Ataques de denegación de servicio en redes

Los ataques de denegación de servicio o DoS (*Denial of Service*, en inglés) en redes son tal vez el ejemplo más conocido de ataque sobre los niveles de red y transporte, también conocidos como ataques TCP/IP.

Existe una gran variedad de ataques de denegación de servicio: inundación IP, falsificación IP origen, inundación TCP/SYN, *teardrop*, *snork*, *ping* de la muerte, etc.

A continuación describiremos los ataques de denegación de servicio más representativos, aunque algunos de ellos ya se han citado anteriormente:

- **Inundación IP** (*IP flooding* en inglés). Consiste en el envío de tráfico masivo para conseguir la degradación de los servicios de la red. El atacante consume un gran ancho de banda ralentizando las comunicaciones existentes en la red. Este ataque es efectivo en redes en las que no se realiza ningún control de acceso al medio y cualquier equipo puede enviar y recibir paquetes sin ningún tipo de limitación del ancho de banda consumido.
- **Falsificación IP origen** (*IP spoofing* en inglés). Distinguimos dos tipos de ataque: *broadcast y smurf.*
  - ***Broadcast.*** Variante del anterior ataque de denegación de servicio en el que se falsea la dirección IP origen del atacante, indicando la dirección de difusión (*broadcast*) de la red. En este caso, cada equipo responde a la dirección IP origen, que al resultar la dirección de difusión, realiza un envío masivo al resto de equipos de la red.
  - ***Smurf.*** Variante del ataque de inundación IP en la que el atacante falsea su dirección IP origen, enviando paquetes de difusión haciéndose pasar por la dirección IP de la víctima, quien recibirá las respuestas de todas las estaciones de la red.

Aunque en algunas ocasiones estos ataques pueden tener un único origen, es muy frecuente que el ataque se realice desde varias máquinas coordinadas, dando lugar a **ataques DDoS** (*Distributed Denial of Service,* Denegación de Servicio Distribuida) consiguiendo un mayor impacto sobre la víctima. En estos casos los atacantes pueden llegar a controlar centenares o miles de equipos formando una red de ordenadores "*zombies*" o *botnet.*

Actividades propuestas

1·· Enumera las vulnerabilidades que presentan los niveles de red y transporte.

2·· Explica en qué consiste la escalada de directorios y por qué representa una amenaza.

3·· ¿Qué diferencias existen entre un ataque de denegación de servicio *smurf* y uno de tipo *broadcast*?

4·· Busca información sobre herramientas MITM (*man in the middle*) como Cain & Abel, arpspoof, ettercap, etc. y contesta a las siguientes preguntas:

a) ¿Qué son? ¿En qué consisten?
b) ¿Qué daño o impacto pueden producir sobre una red de datos?
c) ¿Cómo se pueden detectar y evitar?

2 >> Monitorización

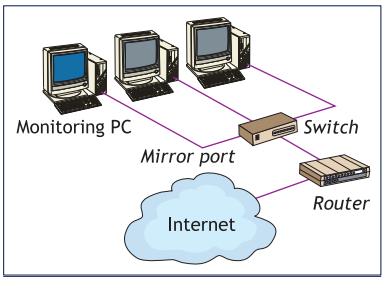
Las redes informáticas constituyen un entorno dinámico con cambios continuos en el que los usuarios están continuamente navegando por Internet, descargando ficheros de otros equipos, enviando mensajes de correo electrónico, accediendo a otros equipos, etc.

Aunque una red funcione correctamente al principio, con el paso del tiempo su rendimiento puede ser menor y presentar riesgos de seguridad para los equipos. En ocasiones esta disminución del rendimiento puede ser debida a algún *malware* que genera tráfico en la red, a un aumento en el tráfico por el número de usuarios o la utilización de nuevas aplicaciones, a interferencias electromagnéticas o incluso al desgaste por la utilización de los dispositivos de la red como tarjetas estropeadas o cableado defectuoso.

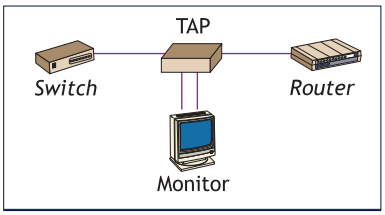
Por lo tanto, no basta con diseñar e implantar una red informática en una organización, es necesario monitorizar y evaluar el rendimiento de la misma a lo largo de su vida mediante herramientas que permitan conocer cómo se comporta y si se está haciendo un uso indebido que ocasione un consumo excesivo del ancho de banda.

Para analizar el tráfico que circula por la red se suele enviar una copia de todo el tráfico que circula por la misma a una herramienta de monitorización. Existen dos sistemas para enviar la copia del tráfico al analizador de redes:

– ***Port mirroring.*** Este sistema de monitorización se basa en configurar un dispositivo por el que pasa todo el tráfico de la red, como puede ser un *switch*, para que reenvíe una copia del tráfico que recibe a la herramienta de monitorización. El puerto que conecta el analizador de la red con el *switch* recibe el nombre de *mirror port* o *monitor port.* El funcionamiento de este sistema es simple: como todos los paquetes llegan al *switch*, se aprovecha esta circunstancia para reenviar una copia por el *monitor port* al equipo que analiza la red.
– ***Network tap.*** En esta forma de monitorización se utiliza un dispositivo hardware que permite acceder al tráfico de datos en un punto de la red donde no es posible usar *port mirroring*. El analizador de paquetes recibe todo el tráfico que le llega al dispositivo.



9.2. *Port mirroring.*



9.3. *Network tap.*

Herramientas de monitorización

Existen en el mercado muchas herramientas diseñadas para analizar y monitorizar una red, tanto comerciales como *open source.* Sus funciones son similares: generación de mapas de red automáticos, elaboración de informes con estadísticas, envío de alertas por *email* y/o sms, etc.

Estas son algunas herramientas muy utilizadas en el ámbito de la monitorización de redes: Wireshark, Ettercap, Ntop, HP Openview, MRTG, Cacti, Nagios, PandoraFMS, Ganglia, Zabbix.

Actividades propuestas

5·· ¿Por qué no se puede utilizar siempre *port mirroring* para monitorizar el tráfico?

3 >> Técnicas de protección

En unidades anteriores hemos estudiado la importancia de proteger los equipos contra atacantes y *malware*. En una red de ordenadores en la que varios equipos comparten información, se comunican entre sí y acceden a otras redes o a Internet, el impacto producido por un ataque sobre la red es más grave que el producido sobre un equipo, por lo que conviene establecer medidas específicas que protejan a los usuarios de la red.

Entre las técnicas de protección más utilizadas en redes destacamos los cortafuegos, sistemas de detección de intrusos, *proxies*, sistemas de gestión unificada de amenazas, VPN, sistemas centralizados de autenticación y zonas desmilitarizadas. Algunas ya se han estudiado en unidades anteriores, como los *firewall*, por lo que nos centraremos en cómo utilizarlas en redes, mientras que otras técnicas son nuevas y conviene conocerlas.

3.1 > Cortafuegos

Si en los equipos personales, el uso del *firewall* era una medida muy recomendable, en las redes de ordenadores es una técnica básica para evitar accesos no autorizados a equipos o servicios de la red.

En una red de ordenadores, el cortafuegos se ubica en el límite de la red para poder analizar todo el tráfico que entra o sale de la misma. En algunas redes, algunos dispositivos de red (*routers*) hacen las funciones de *firewall*, mientras que en otras existe un equipo que dispone de dos tarjetas de red y analiza todo el tráfico.

Un cortafuegos permite o deniega el tráfico en función de parámetros definidos en **reglas**. Si se cumplen las condiciones establecidas en una regla se aplicará la misma, aceptando o rechazando el paquete, y dejará de comprobarse el resto. Cuando no existe ninguna regla que coincida con las características del paquete recibido se aplicará la política por defecto para el paquete que entra al sistema o sale de él. Distinguimos dos tipos de políticas por defecto:

- **Política restrictiva**, donde se rechaza todo el tráfico por defecto y solo se permite el paso de los paquetes aceptados de forma explícita.
- **Política permisiva**, en la que se acepta todo el tráfico, excepto aquellos paquetes especificados en las reglas, que serán rechazados.

Ejemplos

Aplicación de políticas en un cortafuegos

Imaginemos que configuramos un cortafuegos con la siguiente política de entrada: REGLA 1 (permitir la entrada a aplicaciones que utilizan FTP) y REGLA 2 (permitir la entrada a aplicaciones que utilizan telnet). Política de entrada (RECHAZAR).

Este *firewall* solo permite que otros equipos accedan a nuestro equipo o red mediante FTP y telnet. Si algún equipo intenta establecer una conexión por SSH, el *firewall* rechazará la petición.

Como se ha visto en unidades anteriores, existen diferentes tipos de *firewall* (cortafuegos de equipo, cortafuegos de red, cortafuegos de filtrado de paquetes, cortafuegos de aplicación y cortafuegos de estado).

A continuación vamos a estudiar **iptables**, el cortafuegos de Linux, que es un cortafuegos de estado que puede funcionar como cortafuegos de equipo o perimetral.

Iptables

Iptables es el cortafuegos por defecto de los sistemas Linux y permite filtrar paquetes, realizar tareas de encaminamiento, redirigir tráfico a equipos concretos, realizar traducción entre direcciones de red (NAT/PAT) y mantener registros de log.

Todas estas configuraciones se pueden realizar mediante la línea de comandos o, de una forma más práctica, mediante *scripts*. Es muy habitual definir las reglas del cortafuegos en un *script* de inicio que se cargue automáticamente al iniciarse el sistema. Los *scripts* de inicio se suelen guardar en el directorio ***/etc/init.d/***

Este cortafuegos se organiza en tablas y cada tabla contiene cadenas. Existe una tabla para filtrar paquetes (tabla *FILTER*), para traducir direcciones privadas y públicas (tabla *NAT*), etc.

Iptables se configura mediante reglas que definen criterios que deben cumplir los paquetes para ser aceptados y rechazados, alterados, redirigidos, etc. Si se cumple el criterio o regla, entonces se ejecuta la acción que indica la regla y finaliza el proceso, es decir, no se siguen procesando el resto de reglas. Si no se cumple ninguno de los criterios especificados, se aplica la política por defecto para ese tipo de reglas.

La tabla *FILTER* se utiliza para indicar qué paquetes se aceptan o se rechazan en el sistema. Cuando llega un paquete al cortafuegos, se analizan sus campos (origen, destino, puerto, etc.) para determinar si se acepta o se rechaza. Esta tabla está compuesta por tres cadenas:

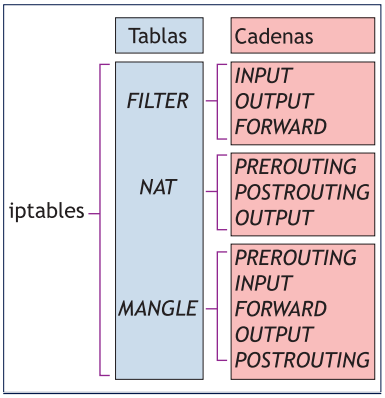
- ***INPUT.*** Esta cadena analiza los paquetes que van dirigidos al equipo donde se ejecuta el cortafuegos, que decide si los acepta o rechaza, en base a la política por defecto *INPUT* y a la información de las reglas *INPUT*. Si otro equipo se conecta al nuestro por ssh o nos hacen un *ping*, ese tráfico pasa por esta cadena.
- ***OUTPUT.*** Esta cadena analiza los paquetes que se han generado en el equipo que ejecuta el cortafuegos, que decidirá si se permite o no el envío del paquete en función de la política por defecto *OUTPUT* y las reglas *OUTPUT* definidas. Si intentamos enviar un correo electrónico o navegar por Internet estamos estaremos generando tráfico que se analizará por esta cadena.
- ***FORWARD.*** Esta cadena se utiliza cuando el equipo que utiliza iptables hace las funciones de *router* y redirige el tráfico. Los paquetes son enviados al cortafuegos que decide qué equipo debe recibir un tipo de tráfico en función de la información introducida en las reglas de este tipo. Se puede, por tanto, hacer que todos los paquetes que van a un servidor FTP lleguen a un solo equipo, que es el que hace las funciones de servidor FTP.

Script

Un *script* es un fichero de texto que contiene órdenes para que el sistema operativo las ejecute.

En Linux este fichero debe tener permisos de ejecución y suele empezar con una línea que indica el lenguaje de *script* que se ha utilizado para programarlo. Así, en el caso de *scripts* para bash:

```
#!/bin/bash
```



9.4. Esquema de iptables.

La sintaxis utilizada para definir reglas mediante la tabla *FILTER* es:

```
iptables –A CADENA [–p tcp|udp|icmp] [OPCIONES] –j ACCION
```

CADENA puede tener cualquiera los valores: *INPUT* (afecta a los paquetes que llegan al equipo donde se ejecuta iptables) y *OUTPUT* (afecta a los paquetes que salen del equipo).

ACCION puede tener estos tres valores:

- *ACCEPT*. El paquete se acepta. Si se utiliza en una regla *INPUT* se permite la entrada del paquete en el sistema, mientras que si se utiliza en una regla *OUTPUT* se permite el envío de ese paquete.
- *DROP*. El paquete se rechaza sin informar al emisor de este rechazo. Si se utiliza en una regla *INPUT*, se descarta ese paquete que ha llegado al sistema, mientras que si se utiliza en una regla *OUTPUT* se rechaza el envío de ese paquete.
- *REJECT*. El paquete se rechaza pero se informa al emisor de que se rechazó el paquete. Su funcionamiento es análogo al de la directiva *DROP*.

Como ya hemos dicho, iptables es un *firewall* de estado y eso significa que mantiene registros de todas las conexiones que pasan por él. Permite diferenciar entre paquetes nuevos que inician una conexión, paquetes enviados entre dos equipos que han establecido una conexión y paquetes que finalizan una conexión establecida.

Tipos de paquetes de estado	Definición de la regla
Paquetes que inician una nueva conexión.	`-m state –state NEW`
Paquetes que forman parte de una conexión existente.	`-m state –state ESTABLISHED`
Paquetes que finalizan una nueva conexión, pero que están relacionados con una existente.	`-m state –state RELATED`
Cuando se navega por un servidor web, la página HTML que devuelve el servidor en la conexión HTTP generada, pasa por la cadena *INPUT*.	`-m state –state RELATED, ESTABLISHED`

Ejemplos

Creación de reglas en iptables

Algunas de las reglas que se pueden crear en iptables son las siguientes:

- Para permitir que nuestro equipo pueda comunicarse por telnet (puerto TCP 23) con otro equipo:

```
iptables –A OUTPUT –p tcp –dport 23 –j ACCEPT
```

- Para rechazar todas las peticiones dirigidas al servidor de correo (puerto TCP 25) de nuestro equipo, informando al emisor de que la conexión fue rechazada:

```
iptables –A INPUT –p tcp –dport 25 –j REJECT
```

Casos prácticos 1

Utilización de iptables

•• Genera un *script* de comandos que se ejecute cuando arranque el servidor y que aplique las siguientes reglas:

a) Política restrictiva de entrada y salida (no puede entrar ni salir ningún paquete a tu servidor excepto los permitidos explícitamente).
b) Permitir que el servidor pueda enviar y recibir *ping*, hacer consultas DNS y permitir que se puedan conectar al equipo por FTP, ssh, HTTP y HTTPS.
c) Permitir los paquetes relacionados con otras conexiones, tanto de entrada como salida.

Solución ••

a) En primer lugar, guarda el *script* en */etc/init.d/firewall*.

Dale permisos de ejecución con el comando `chmod +x /etc/init.d/firewall` y habilita que se ejecute en el arranque dependiendo de la distribución Linux:

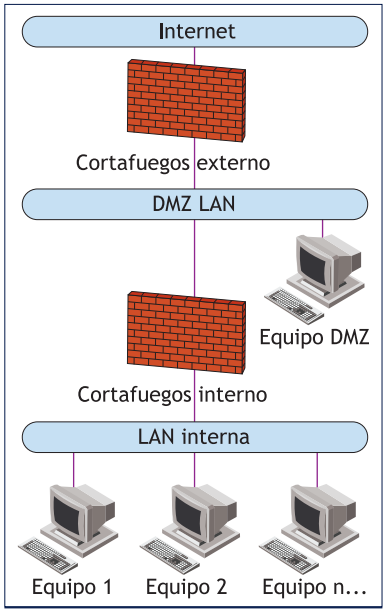
- Distribuciones Debian/Ubuntu: `update-rc.d firewall defaults`
- Distribuciones Red Hat/Fedora/Suse/CentOS: `chkconfig firewall on`

b) Antes de empezar es necesario cargar el módulo *nf_conntrack_ftp* para que funcione el modo de seguimiento de conexiones (*firewall* con estado) para la aplicación FTP, y el cortafuegos pueda abrir dinámicamente los puertos que se necesiten para FTP. Esto se hace como root con el comando:

```
$ modprobe nf_conntrack_ftp
```

c) El contenido del *script* */etc/init.d/firewall* será similar a este:

```
#!/bin/bash
iptables -F
iptables -t nat -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
# Permitimos la entrada de paquetes relacionados con conexiones iniciadas
iptables -A INPUT -m state —state RELATED,ESTABLISHED -j ACCEPT
# Permitimos la salida de paquetes relacionados con conexiones iniciadas
iptables -A OUTPUT -m state —state RELATED,ESTABLISHED -j ACCEPT
# Permitimos la SALIDA de paquetes icmp (PING)
iptables -A OUTPUT -p icmp -j ACCEPT
# Permitimos la ENTRADA de paquetes icmp (PING)
iptables -A INPUT -p icmp -j ACCEPT
# El servidor permite la entrada de paquetes al puerto 53: DNS
iptables -A OUTPUT -p udp —dport 53 -j ACCEPT
# El servidor permite la entrada de paquetes al puerto 22: SSH
iptables -A INPUT -p tcp —dport 22 -j ACCEPT
# El servidor permite la entrada de paquetes al puerto 80: HTTP
iptables -A INPUT -p tcp —dport 80 -j ACCEPT
# El servidor permite la entrada de paquetes al puerto 443: HTTPS
iptables -A INPUT -p tcp —dport 443 -j ACCEPT
```



9.5. Esquema de DMZ.

Snort

Snort es un IDS/IPS desarrollado bajo licencia GPL por Sourcefire que se ha convertido en estándar en la industria.

Las firmas de este sistema han sido desarrolladas por muchos colaboradores y es capaz de detectar todo tipo de ataques.

Colocación del IDS

- **Antes del cortafuegos:** pueden producir falsos positivos.
- **Después del cortafuegos:** permiten detectar ataques reales.
- **Antes y después del cortafuegos:** además de detectar si se producen ataques reales, permiten conocer si el cortafuegos está mal configurado. Si el IDS indica que se están produciendo muchos ataques reales significa que el cortafuegos no corta los ataques de forma eficiente, por lo que habrá que modificarlo.

3.2 › Zonas desmilitarizadas

Una zona desmilitarizada o DMZ (*DeMilitarized Zone*, en inglés) es una red que suele albergar servidores que ofrecen algún servicio en Internet y que, generalmente, actúa como intermediaria entre la red interna de una empresa y la red externa, incrementando la seguridad de las redes internas. La red interna y la externa pueden establecer conexiones con la DMZ, pero desde la DMZ solo se permite establecer conexiones con la red externa, denegando conexiones de entrada a la red interna.

De esta forma, los equipos de la DMZ pueden iniciar conexiones con equipos externos de forma legítima como, por ejemplo, el servidor de antivirus corporativo que se descarga regularmente las firmas y actualizaciones de los virus.

Es importante remarcar que no se permiten conexiones desde la DMZ a la red interna porque se trata de una red con un nivel de seguridad relativamente bajo, con lo que podría darse el caso de que un atacante controlase alguno de los servidores que hay dentro de la DMZ y tratase de establecer conexiones con los equipos de la red interna.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

3.3 › Detectores de intrusos

Este tipo de sistemas está formado por un dispositivo o software que monitoriza, alerta y/o elimina ataques a la red o a los equipos informáticos. Dentro de este tipo de técnicas distinguimos entre sistemas detectores de intrusos y sistemas de prevención de intrusos:

– **Sistemas detectores de intrusos,** o IDS (*Intrusion Detection System*, en inglés), son un elemento pasivo que detecta ataques pero no los elimina. Distinguimos tres tipos de IDS:
  - HIDS (*Host* IDS), que monitoriza y protege un equipo.
  - NIDS (*Network* IDS), que monitoriza y protege una red.
  - DIDS (*Distributed* IDS), donde se dispone de NIDS distribuidos y gestionados por una consola.
– **Sistemas de prevención de intrusos** o IPS (*Intrusion Prevention System,* en inglés), son un elemento activo que trata de neutralizar el ataque, adaptándose a él. Suelen estar formados por un IDS y un cortafuegos que modifica sus reglas dinámicamente para evitar accesos no autorizados a la red.

El proceso utilizado para detectar ataques suele ser el estudio de la red en condiciones normales para elaborar estadísticas sobre el rendimiento y detectar anomalías.

Otra técnica utilizada para detectar ataques es similar a la utilizada por los antivirus para detectar infecciones de *malware* no recogido en su base de datos: se trata de "adivinar" si se produce un ataque mediante la comparación de patrones de ataques (firmas) con el tráfico que circula por la red en tiempo real.

3.4 > *Proxies*

Un *proxy* o intermediario de red es un servicio, normalmente instalado en un servidor o dispositivo dedicado, que realiza la función de intermediario entre él y los clientes que solicitan un determinado servicio, como por ejemplo HTTP. Un *proxy* web por tanto es un dispositivo que trabaja en el nivel de aplicación de OSI.

El uso más habitual de un servidor *proxy* es permitir el acceso a Internet a los equipos de una organización cuando solo se puede disponer de un único equipo conectado, que es el propio *proxy*. Este permite a los clientes conectarse a una red (generalmente Internet) de forma indirecta a través de él, proporcionando de esta forma una capa adicional de seguridad.

Cuando un equipo de la red desea acceder a una información o recurso, es realmente el *proxy* quien realiza la comunicación y a continuación traslada el resultado de la petición al cliente.

Algunas de las ventajas de usar un *proxy* son las siguientes:

- La navegación puede ser más rápida si se usa la caché y esta es suficientemente grande.
- Proporciona seguridad al proteger a los equipos cliente de la red externa.
- Posibilita definir filtros de contenidos y listas de control de acceso para permitir a las organizaciones realizar un control del servicio que se está usando.

Proxy Squid

Squid es una de las aplicaciones *proxy* más utilizadas en Internet y funciona como *proxy* HTTP, HTTPS y FTP.

3.5 > Gestión unificada de amenazas

Los dispositivos conocidos como **UTM** (*Unified Threat Management*, en inglés) o gestión unificada de amenazas, combinan distintas técnicas de protección de redes como cortafuegos, antivirus, *antispam*, filtro de contenidos, detección y prevención de intrusos redes privadas virtuales y servidor *proxy*, todo ello en un único aparato.

Son la tendencia actual, sobre todo en pequeñas empresas, donde el ahorro de costes es crítico y no es posible invertir mucho dinero en soluciones de seguridad de varios fabricantes.

No obstante, hay que tener en cuenta que el hecho de que todos los sistemas de protección estén integrados en un solo dispositivo puede presentar problemas de rendimiento, escalabilidad y disponibilidad. Por ejemplo, un fallo completo en el dispositivo implica un fallo en todos los sistemas de protección de la red.

9.6. UTM Netgear.

Actividades propuestas

6·· Busca información en Internet sobre productos UTM de diferentes fabricantes. Realiza una tabla comparativa de precios, características así como los servicios de seguridad que ofrecen.

7·· Realiza un esquema resumen de los medios de protección expuestos en este epígrafe, indicando las ventajas e inconvenientes de implantar cada uno de ellos.

4 >> Protección en redes inalámbricas

Millones de personas utilizan el estándar 802.11 a diario, o lo que es lo mismo las redes inalámbricas o redes WiFi, que presentan muchas ventajas sobre las redes cableadas tradicionales, como la flexibilidad, movilidad y facilidad de conexión. Así, por ejemplo, para poder comprobar el correo electrónico desde la calle, únicamente necesitamos que nuestro dispositivo inalámbrico (por ejemplo, una *tablet* o un *smartphone*) se encuentre dentro del alcance de la señal que proporciona un punto de acceso a Internet y que se establezca una conexión entre ellos.

Si bien es cierto que las redes inalámbricas presentan muchas ventajas para los usuarios, este tipo de redes no están exentas de vulnerabilidades que amenazan la disponibilidad, confidencialidad e integridad de la información, que debemos tener en cuenta y de las que deberemos protegernos adecuadamente.

Es un error muy común es pensar que solo los vecinos pueden acceder a una red inalámbrica, pues un intruso solo precisaría de estar dentro del alcance de la red, para lo cual puede utilizar equipos especiales que le permitan acceder a una red ubicada a cientos de metros de distancia, donde la señal original de la red no llegaría de forma normal.

Entre los tipos de ataques más comunes, distinguimos:

- **Ataques de denegación de servicio (DoS)** ocasionados por una fuente emisora de ondas que trabaja en la misma banda de frecuencias que la red inalámbrica, lo que provocaría que ningún equipo de la red pudiera comunicarse con el punto de acceso. Nos encontramos ante un ataque contra la disponibilidad de la red.
- **Escuchas del tráfico de la red (*sniffing*),** donde cualquier equipo podría interceptar el intercambio de información enviada en la red, afectando a la confidencialidad de la comunicación.
- **Inyección de tráfico en la red,** donde un usuario no legítimo trata de inyectar paquetes sobre la red para generar tráfico entre las estaciones y obtener las claves de sesión si se está utilizando un protocolo de seguridad inseguro como WEP.
- **Conexiones no autorizadas a la red,** que podrían darle al atacante acceso sin restricciones a la red.
- **Ataques de acceso,** como la desautenticación y la falsa autenticación. La **desautenticación** es un ataque diseñado para obtener un ESSID oculto de una red y capturar mensajes intercambiados para establecer una conexión, obligando a los clientes a reautenticarse. También se utiliza para hacer denegación de servicio. La **falsa autenticación** (*fake auth*), se utiliza para registrar una dirección MAC de cliente falsa en un punto de acceso inalámbrico.

Por lo tanto, debemos utilizar mecanismos que permitan establecer comunicaciones seguras en redes inalámbricas. Para ello debemos proteger tanto las redes inalámbricas, garantizando que solo equipos legítimos acceden a la red y que la información se encuentra protegida de forma conveniente, como a los clientes de la red inalámbrica frente a posibles ataques que puedan sufrir de otros equipos de la red.

Acceso al tráfico en una red inalámbrica

En una red inalámbrica cualquier equipo que se encuentre dentro de su alcance puede acceder a la información transmitida en esa red, lo que puede ser aprovechado por usuarios ilegítimos para realizar ataques sobre ella.

Mecanismos de seguridad

En una red inalámbrica solo deberían poder acceder a la red los equipos autorizados. Además, la información que circula por ella no debería ser comprensible para los equipos no legítimos. Por ello, las redes inalámbricas deben cifrar las comunicaciones y controlar la forma en que los equipos se autentican en la red. Estos son los principales mecanismos de seguridad utilizados en redes inalámbricas:

- **WEP (*Wired Equivalent Privacy*).** Es el mecanismo de seguridad utilizado por defecto por muchos puntos de acceso y *routers* inalámbricos en la actualidad. Presenta graves fallos de seguridad en el mecanismo de cifrado (RC4), con lo que un atacante podría obtener la contraseña muy rápidamente, por lo que se desaconseja su uso.
- **WPA (*Wireless Protected Access*).** Se le considera como un estadio intermedio en el camino desde el WEP hacia la implementación completa del estándar 802.11i (WPA2). Ofrece una mayor protección que WEP, ya que proporciona una versión mejorada de RC4 e incorpora mecanismos de seguridad adicionales, como TKIP, pero se recomienda utilizar WPA2.
- **WPA2.** Se considera el mecanismo de seguridad más adecuado para redes inalámbricas y ofrece mecanismos de cifrado robustos (AES, *Advanced Encryption Standard*). Existen dos tipos de WPA2 (*Personal* y *Enterprise*) que se diferencian en los mecanismos de autenticación:
  - **WPA2 *Personal* o PSK**. Su mecanismo de autenticación es PSK (*Pre-Shared Key*), en el que la contraseña se comparte entre el punto de acceso y los clientes de la red. Es la opción recomendada para redes domésticas.
  - **WPA2 *Enterprise*.** Proporciona una mayor flexibilidad para gestionar los mecanismos de autenticación, pudiendo utilizarse un servidor de contraseñas aleatorias (servidor RADIUS) o diferentes tipos de protocolos EAP como usuario y contraseña, certificados digitales, tarjetas inteligentes *(smartcards),* etc. Es la opción recomendada para empresas.

Existen otras medidas que, en algunos casos, complican la gestión de la red o disminuyen el nivel de seguridad, por lo que pueden ser consideradas como falsas medidas de seguridad y se desaconseja su uso:

- **Filtrado de direcciones MAC.** Esta medida crea una falsa sensación de seguridad, ya que puede ser fácilmente burlada mediante programas que cambien la dirección MAC del atacante.
- **Ocultación del SSID.** El problema de esta medida es que en este tipo de redes si los puntos de acceso no difunden el SSID, son las estaciones cliente quienes continuamente envían peticiones preguntando si esa red se encuentra dentro de su alcance. Un atacante podría aprovechar esta situación para suplantar la red y establecer conexiones.

Rogue ap

En este tipo de ataque, un equipo se hace pasar por un falso punto de acceso al que se conecta el cliente, interceptando sus claves y toda la información que transmite por la red.

Para evitarlo es importante mantener actualizados el sistema operativo, las aplicaciones que hacen uso de Internet y los *drivers* del dispositivo, no conectarse a redes inseguras y mantener la lista de redes preferidas actualizada, eliminando redes no utilizadas y redes que no difunden su SSID de esta lista.

Actividades propuestas

8·· ¿Qué mecanismo de seguridad, de los expuestos en este apartado, consideras más seguro para proteger la red inalámbrica de tu casa? ¿Y para tu *smartphone*?

5 >> Auditorías de seguridad en redes

Amenazas internas

Las empresas especializadas en consultoría y auditorías de seguridad informática aseguran que la mayoría de amenazas y ataques reales provienen del interior de las organizaciones.

La seguridad informática es un proceso dinámico que no finaliza cuando se han implantado distintas medidas de seguridad informática en una empresa u organización. Es necesario evaluar si el sistema de seguridad informática que se ha adoptado está cumpliendo con su función correctamente y mejorarlo si fuera necesario.

Cada día surgen nuevas amenazas ante las que un sistema informático puede ser vulnerable y, por tanto, es necesario adaptarlo a las nuevas circunstancias. Un sistema que un día era seguro, con el paso del tiempo, si no se va actualizando en materia de seguridad, puede presentar fallos de seguridad. Con este fin se realizan auditorías de seguridad informática en las organizaciones.

Una auditoría es el proceso realizado por una persona o equipo de personas, denominados auditores, que pueden ser personal de la propia empresa o de una empresa externa, con el objetivo de revisar el funcionamiento de una determinada área en la organización. Así, podemos tener auditorías financieras y contables, auditorías de calidad o, como en el caso que nos ocupa, auditorías de seguridad informática.

Los principales objetivos de una auditoría de seguridad informática son los siguientes:

- Verificar si el sistema de seguridad implantado en la organización cumple correctamente con la finalidad de proteger el sistema informático.
- Detectar posibles vulnerabilidades y amenazas en el sistema informático.
- Realizar un informe detallado con los resultados obtenidos y, si fuera necesario, un plan de acciones para mejorar el actual sistema de seguridad.

En una auditoría de seguridad es fundamental realizar un correcto **análisis de riesgos** para identificar todos los elementos que componen el sistema informático y valorar el impacto y riesgo de las posibles amenazas.

El proceso del análisis de riesgos pasa por las siguientes fases:

- Inventario y valoración de los activos de la organización.
- Identificación y valoración de las amenazas y vulnerabilidades en el sistema informático.
- Definición de sistemas de medición de riesgos.
- Determinación del impacto y riesgo de un ataque o amenaza.
- Identificación y evaluación de las medidas de seguridad existentes.

Exploit

Los *exploit* son códigos maliciosos diseñados para aprovechar una vulnerabilidad informática. Se emplean en las herramientas de test de intrusión.

Un concepto relacionado es el de ***pentest* o test de penetración o intrusión**, que consiste en la aplicación de técnicas para intentar romper los sistemas de seguridad de una organización y obtener acceso no autorizado al sistema informático. Es realizado por los auditores de seguridad autorizados por la empresa después del análisis de vulnerabilidades para determinar la vulnerabilidad del sistema informático de una organización.

En este punto, nos centraremos en las auditorías de seguridad en redes informáticas.

5.1 > Tipos de auditorías de red

Las auditorías de seguridad informática se pueden clasificar en distintos tipos, atendiendo a criterios como el lugar desde el que se realiza la auditoría o cuáles son los objetivos en los que se centra la auditoría. De esta forma, se puede realizar la siguiente clasificación:

Auditoría de red interna

En esta auditoría se realiza un análisis de riesgos, amenazas, vulnerabilidades e impactos desde dentro de la organización sin tener en cuenta los riesgos y amenazas desde Internet. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.

Auditoría perimetral y de DMZ

Esta es la auditoría que se realiza desde Internet, fuera del perímetro de seguridad de la empresa, con el objetivo de evaluar el grado de protección de la empresa frente a ataques externos.

Se evalúa tanto la protección de la red interna, como de la DMZ (zona desmilitarizada), que es donde se ubican los servidores de la empresa que ofrecen servicios a Internet (DNS, web, correo, FTP, etc). Se utilizan distintos tipos de ataques contra la red comprobando si esta es vulnerable, con previo aviso a la organización del momento en que se va a llevar a cabo la auditoría.

Test de intrusión

Consiste en un método de auditoría mediante el cual se intenta acceder a los sistemas para comprobar el nivel de resistencia a una intrusión no deseada. Se utiliza una base de datos de vulnerabilidades conocidas para automatizar el análisis y generar un informe con las vulnerabilidades encontradas. Es un complemento fundamental para la auditoría perimetral.

Auditoría de aplicaciones

En este tipo de auditoría solo se testean y evalúan las aplicaciones de la empresa, sin tener en cuenta los servidores, dispositivos de red o sistemas operativos. Se hacen pruebas como el desbordamiento de búfer, la inyección SQL, el XSS, la escalada de directorios, etc.

Análisis forense

Es una auditoría que se realiza cuando los sistemas ya han sido atacados y comprometidos. En este caso, se separa la máquina atacada de la red y se analiza en detalle para ver qué es lo que ha ocurrido y poder evitar ataques similares en el futuro.

El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la vez que se valoran los daños ocasionados.

Si los daños han provocado la inoperatividad del sistema, el análisis se denomina **análisis post mórtem**.

Shellcode

Son *exploits* cuyo objetivo es conseguir una consola o línea de comandos remota en el equipo que se ataca. Suelen aprovechar fallos de programación como los conocidos desbordamientos de búfer.

0-day exploits

Los *0-day exploits* o *exploits* de día cero son herramientas que explotan vulnerabilidades no conocidas por el desarrollador o fabricante del software y que por tanto no han sido aún solucionadas.

5.2 > Herramientas para auditorías

A continuación, se comentan algunas de las herramientas y técnicas que utilizan los auditores de seguridad informática para realizar auditorías de seguridad a una organización.

– **Enumeración de redes.** Su objetivo es identificar las redes IP asociadas a una organización y descubrir sus servidores. Esta información se puede obtener públicamente con herramientas como whois o el propio servicio DNS. La enumeración de redes sirve de base para el rastreo masivo de la red.
– **Rastreo de redes.** Su objetivo es obtener información más detallada a partir de la conseguida en la enumeración. Sirve de base para el análisis de vulnerabilidades. Una de las herramientas más utilizadas para realizarlo es nmap, del que existen versiones para varios sistemas operativos como GNU/Linux o Windows. Sus técnicas son:
  - Barrido de direcciones IP con ICMP.
  - Barrido de puertos TCP y UDP.
  - Identificación de sistema operativo y aplicaciones.
– **Barrido de puertos.** Un barrido de puertos trata de identificar qué puertos TCP y UDP están abiertos en un ordenador para poder aprovechar ciertos servicios que dependen de ellos para entrar en el sistema. Existe una gran variedad de herramientas de barrido de puertos accesibles en la red y esta será una de las cosas que primero compruebe un atacante. Una de las herramientas más conocidas para hacer barridos de puertos es nmap.
– ***Fingerprinting:*** son técnicas que sirven para identificar el sistema operativo y las versiones de las aplicaciones que se están usando en los servidores. Además de las utilidades ya expuestas, nmap también es una excelente herramienta para realizar esta técnica. Con un analizador de protocolos como Wireshark, también se puede identificar la versión de una aplicación como, por ejemplo, la versión de un servidor web cuando se le hace una petición web.
– **Análisis de vulnerabilidades.** El objetivo de esta técnica es detectar debilidades en el sistema informático de la empresa y corregirlas. Las debilidades se contrastan contra enormes bases de datos de vulnerabilidades donde se encuentran todas perfectamente definidas y catalogadas. Para el análisis de vulnerabilidades se pueden utilizar herramientas muy diversas, como por ejemplo, Nessus, OpenVAS, SAINT, GFI LanGuard, Core Impact, Retina, ISS, etc.
– **Tests de penetración.** Los tests de penetración, tests de intrusión o *pentests* son un método para evaluar la seguridad de un sistema informático simulando un ataque de un usuario malicioso, como un *black hacker* o *cracker.* Ejemplos de herramientas son: SAINTexploit, Metasploit Framework, NeXpose.

Si se trabaja en entorno Linux, existen además algunas distribuciones especializadas en auditorías de seguridad en redes que incluyen muchas de las herramientas comentadas en este apartado y además permiten auditar la seguridad de una red inalámbrica. Algunas de estas distribuciones son: Backtrack, Wifiway, WifiSlax o nUbuntu.

Whois

Whois es una herramienta que permite consultar una gran base de datos mundial con información relacionada de todos los dominios y rangos de direcciones IP de Internet y sus redes.

Web

Bases de datos de vulnerabilidades

- MITRE CVE: http://cve.mitre.org
- OSVDB: http://www.osvdb.org
- ISS X-Force: http://xforce.iss.net/
- Bugtraq: http://www.securityfocus.com
- CERT: http://www.kb.cert.org/vuls/
- Secunia: http://www.secunia.com

Casos prácticos 2

Utilización de la herramienta de auditoría de redes nmap

•• Para realizar esta práctica necesitamos un sistema operativo (Windows, GNU/Linux o Mac OS X) con la aplicación nmap instalada (disponible para distintas plataformas en http://nmap.org).

Utilizando la interfaz gráfica de nmap, mediante el barrido de puertos y *fingerprinting*, realiza las siguientes tareas:

a) Realiza un barrido intenso al ordenador de un compañero y observa la información que presenta.
b) ¿Cómo realizarías un barrido intenso de todos los puertos TCP? ¿Qué diferencia hay con el anterior?
c) ¿Cómo realizarías un barrido intenso de todos los ordenadores del aula?
d) ¿Cómo podrías realizar un barrido para descubrir los ordenadores que hay en una red, sin necesidad de descubrir los puertos abiertos?

Solución ••

Para realizar esta práctica necesitas un sistema operativo (Windows, GNU/Linux o MacOS X) con la aplicación nmap instalada (disponible para distintas plataformas en http://nmap.org). Si aún no la tienes instalada, descárgatela e instálala.

a) Barrido intenso. Selecciona *Intense Scan* en el desplegable *Profile*, escribe la dirección IP o el nombre del ordenador de tu compañero en el campo de texto *Target* y haz clic en el botón *Scan*. Como resultado, se muestra el sistema operativo que nmap ha descubierto, así como un listado de los puertos abiertos como se ve en el siguiente ejemplo:

```
Starting Nmap 5.51 (http://nmap.org ) at 2012-05-18 01:43 CEST
Nmap scan report for windowspc (192.168.1.20)
Host is up (0.00045s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
3389/tcp open microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:4C:0A:BF (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop
Service Info: OS: Windows
```

b) Barrido intenso de todos los puertos TCP. Selecciona *Intense Scan, all TCP ports* en el desplegable *Profile* y haz clic en el botón *Scan*. La diferencia es que ahora nmap, en vez de realizar un barrido de los puertos más comunes, realiza un barrido de todos los puertos TCP, desde el 1 al 65535.

c) Barrido de todos los ordenadores de un aula. Indica la red y la máscara de la subred en el campo *Target*. Por ejemplo, al indicar el *target* 192.168.1.0/24, se realiza el barrido de las 254 direcciones IP de la red 192.168.1.0/24. nmap permite además indicar rangos, como por ejemplo: 192.168.1.1 192.168.1.5 192.168.10-20

d) Descubrir ordenadores de una red sin barrido de puertos. Puedes hacer un barrido de *ping* (*ping scan*), aunque en ocasiones puede no funcionar correctamente debido a la existencia de cortafuegos personales.

Actividades finales

.: CONSOLIDACIÓN :.

1·· Describe los ataques de denegación de servicio vistos en esta unidad.

2·· ¿En qué consisten los ataques DDoS?

3·· Enumera dos tipos de ataques a los que son vulnerables cada uno de los niveles del modelo de redes ISO/OSI.

4·· Explica cómo funcionan las dos técnicas de monitorización estudiadas en esta unidad y en qué situación son convenientes.

5·· ¿Por qué es importante filtrar el tráfico de una red? ¿Cómo se llama este tipo de herramientas?

6·· Explica qué es un IDS y enumera los tipos de IDS estudiados en esta unidad.

7·· ¿Qué ventajas plantea la utilización de una zona desmilitarizada en una red?

8·· Explica por qué técnicas como el filtrado MAC o la ocultación del SSID son consideradas como "falsas técnicas de seguridad" en redes WiFi.

9·· Enumera y describe los tipos de auditoría descritos en esta unidad.

.: APLICACIÓN :.

1·· Un amigo nos comenta que quiere proteger su punto de acceso inalámbrico para evitar que personas no autorizadas puedan acceder a su red y a la información que circula por ella. ¿Qué recomendaciones le darías?

2·· ¿Qué podemos hacer para evitar que usuarios maliciosos accedan a nuestro dispositivo móvil o portátil en una red pública?

3·· ¿Cómo configurarías iptables para que desde nuestro equipo solo se pueda navegar por Internet? ¿Y para que nuestro equipo haga de servidor web?

4·· ¿Qué tipo de cortafuegos podemos utilizar para evitar ataques sobre nuestro servidor web?

5·· ¿Cómo podríamos conocer los puertos abiertos de los equipos de nuestra red local (192.168.0.0/24)?

6·· ¿Qué tipo de herramientas le recomendarías a un cliente que busca proteger la red contra accesos no autorizados, *malware* y *spam*, así como evitar que sus hijos accedan a páginas con contenido no apropiado?

7·· Un cliente ha configurado un equipo para que realice tareas de servidor web y servidor web seguro, pero quiere protegerlo frente a accesos no autorizados. Este servidor utiliza una distribución Linux Fedora con iptables como cortafuegos predeterminado. ¿Cómo configurarías iptables para que solo atienda las peticiones HTTP y HTTPS de los clientes?

8·· Si en escenario expuesto en la actividad número 7, el cliente desease navegar con ese equipo por Internet utilizando un navegador web, ¿qué cambios deberías realizar sobre iptables?

9·· En una empresa, tienen el servidor web y el servidor FTP conectado a la misma red que el resto de equipos. La red de dicha empresa está protegida por un cortafuegos configurado para permitir conexiones a los puertos necesarios por estos servicios.

a) ¿Qué fallos de seguridad detectas? ¿Cómo se podrían solucionar?
b) Enumera alguna herramienta que recomendarías utilizar a la empresa para mejorar la seguridad de este tipo de redes.

Caso final 3

Estudio de la seguridad de una empresa

•• El propietario de una empresa te ha contratado para realizar un estudio de la seguridad informática. La empresa dispone de un servidor web que contiene su página web, un servidor DNS que atiende peticiones de los distintos equipos y un total de 300 equipos que acceden a la red.

¿Qué consejos podrías darle al propietario de la empresa para mejorar la seguridad de esta empresa?

Solución •• Esa configuración plantea serios problemas de seguridad por las siguientes razones:

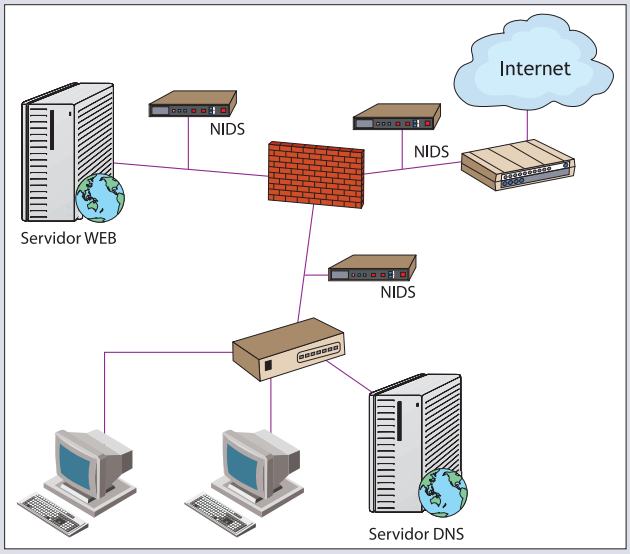
- No se filtra el tráfico.
- En la misma red interna se encuentran servicios que solo deben ser accedidos desde la propia red interna (servidor DNS) y servicios que pueden ser accedidos desde el exterior (servidor web).
- No se realiza monitorización del tráfico.
- Los equipos no están protegidos frente al software malicioso y *spam*.

Para solucionar estos problemas de seguridad podrían realizarse las siguientes acciones:

1. Utilizar un cortafuegos para filtrar el tráfico. Si el *router* que suministra acceso a la red de la empresa dispone de cortafuegos, podrías configurarlo. En el caso de que el *router* no realice tareas de filtrado de paquetes, se podría utilizar un equipo para realizar esta tarea. Se recomienda utilizar una política restrictiva de entrada y salida rechazando el tráfico entrante y saliente por defecto, así como permitir el acceso de aquellas aplicaciones autorizadas de forma explícita mediante la declaración de reglas. Una posibilidad sería utilizar un sistema operativo basado en Linux y configurar iptables.

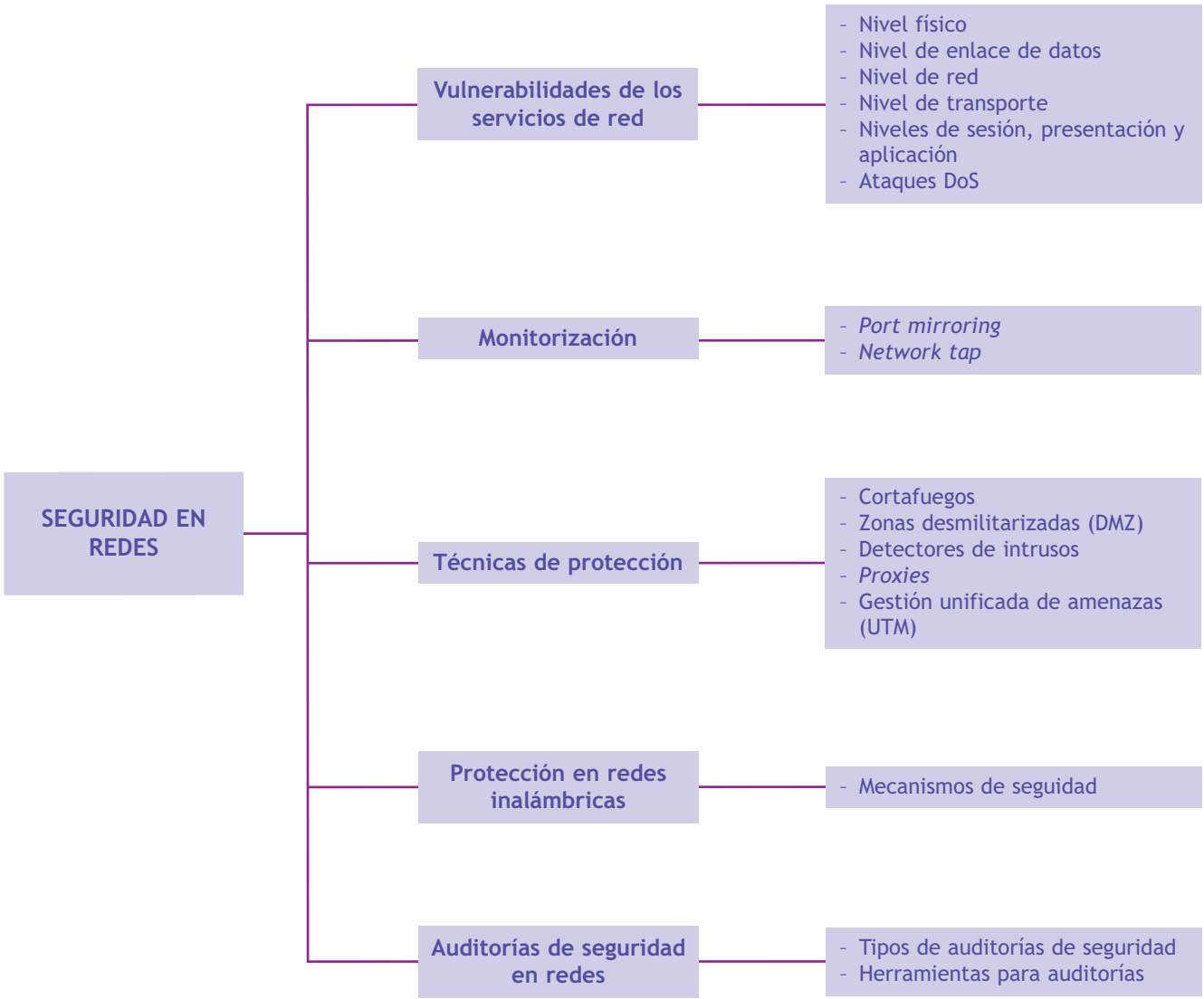
2. Configurar una zona desmilitarizada (DMZ) que contenga los servidores accesibles desde el exterior (servidor web). Los servicios que se ofrecen a Internet suelen sufrir muchos ataques, con lo que al separar estos servicios del resto de la red un atacante que consiga acceso a uno de ellos no tendrá acceso a la red de la empresa. La DMZ puede configurarse en el cortafuegos.

3. Instalar un sistema de monitorización y de detección de intrusos. Se podrían instalar sistemas de identificación de intrusos en red (NIDS) en cada interfaz de la empresa, es decir, uno en la red interna, otro en la DMZ y otro en la interfaz que conecta con el exterior (Internet). Otra técnica de protección que se podría adoptar es la utilización de un sistema de monitorización que permita estudiar si se producen situaciones anómalas que afectan al tráfico que circula por la red. Para ello se podrían utilizar técnicas estudiadas como *port mirroring* (si el *switch* lo soporta) o *network taps*.



4. Instalar antivirus en los equipos. La utilización de este tipo de herramientas puede evitar que contenido dañino como *malware* o *spam* acceda a los equipos. En una empresa se recomienda utilizar un antivirus corporativo, con lo que se mejora el ancho de banda en operaciones como actualizaciones. Tras la adopción de estas medidas, el esquema de la red de la empresa quedará como se muestra en la imagen.

Ideas clave


SEGURIDAD EN REDES
Vulnerabilidades de los servicios de red
- Nivel físico
- Nivel de enlace de datos
- Nivel de red
- Nivel de transporte
- Niveles de sesión, presentación y aplicación
- Ataques DoS
Monitorización
- *Port mirroring*
- *Network tap*
Técnicas de protección
- Cortafuegos
- Zonas desmilitarizadas (DMZ)
- Detectores de intrusos
- *Proxies*
- Gestión unificada de amenazas (UTM)
Protección en redes inalámbricas
- Mecanismos de seguidad
Auditorías de seguridad en redes
- Tipos de auditorías de seguridad
- Herramientas para auditorías

Las claves por defecto de algunos *routers* inalámbricos al descubierto

Se ha hecho público el algoritmo que genera las contraseñas de los routers Comtrend. Estos son los que ofrecen Movistar (Telefónica) y Jazztel a sus clientes para dar acceso a Internet. A efectos prácticos, significa que si los clientes de Telefónica o Jazztel no han cambiado su contraseña WiFi desde que recibieron el *router,* su cifrado es inútil. Actualmente, esto es más sencillo incluso que romper una clave WEP.

Hace algunos años, los *routers* que ofrecían los proveedores venían con cifrado WEP. WEP siempre ha sido un estándar sencillo de romper, por tanto, "colarse" en este tipo de redes WiFi resultaba relativamente sencillo si su dueño no saltaba a WPA. No hace mucho, los *routers* comenzaron a ofrecerse con el estándar de cifrado WPA y una contraseña por defecto (escrita en el propio *router*). Esto supuso un gran avance porque, por el momento, al estándar WPA no se le conocen graves problemas de seguridad. El punto débil se encontraba pues en la generación de la clave por defecto. Se trata de un proceso automático, así que si se descubría este proceso de generación se podrían conocer las contraseñas de todos los usuarios que utilizaran estos *routers* y no hubieran cambiado su contraseña.

Se ha descubierto el mecanismo de generación de claves, basado en el BSSID y el ESSID del *router* (habitualmente WLAN_XXX en routers de Movistar) y la dirección MAC del *router* (escrita normalmente en su base). Estos dos datos son públicos cuando se usa WiFi, por tanto, cualquiera puede calcular la clave.

El algoritmo combina estos dos valores, les concatena la cadena "bcgbghgg" al comienzo, calcula el *hash* MD5 y se queda con los 30 primeros caracteres. Incluso existen ya aplicaciones para Android que calculan la clave.

Por tanto, a partir de ahora el escenario es el siguiente: un atacante esnifa una red WiFi de un usuario cualquiera, cifrada con el estándar WPA. Obtiene el BSSID y ESSID y, con este sencillo algoritmo, descubre la clave que se ha calculado por defecto. Se conecta a esa red y una vez dentro podrá utilizar esa red como plataforma de ataques o intentar ataques internos a los equipos que estén conectados a ella. También podrá esnifar su tráfico y ver los datos que no se transmitan por SSL o cifrados, como pueden ser contraseñas, conversaciones de chat...

Lo recomendado es entrar en el *router* y cambiar la contraseña. Habitualmente, hay que introducir en el navegador la dirección 192.168.1.1, introducir la contraseña del *router,* buscar la configuración de seguridad de la red inalámbrica (WLAN) y modificar la contraseña WPA introduciendo una nueva de más de 16 caracteres que contenga números, letras y símbolos. O mejor aún, si el *router* los soporta, cambiar al estándar WPA2. El problema es que esto puede resultar una operación compleja para el usuario medio, que no quiere arriesgarse a modificar aspectos técnicos que no termina de asimilar. Será de ellos de los que se aprovechen los atacantes.

Fuente: Sergio de los Santos. Una al día. 5/2/2011 www.hispasec.com

Actividades

1·· ¿Qué tipo de acciones puede realizar un atacante sobre una red para la que tiene acceso?

2·· ¿Qué recomendaciones pueden seguir los usuarios que tienen este tipo de redes según el texto?

unidad 10

Normativa sobre seguridad y protección de datos

SUMARIO

- Legislación sobre protección de datos
- Agencia Española de Protección de Datos
- Legislación sobre los servicios de la sociedad de la información y el comercio electrónico
- Normas ISO sobre gestión de seguridad de la información

OBJETIVOS

- Tomar conciencia de la importancia de la protección de datos.
- Describir la legislación existente sobre protección de datos.
- Identificar las figuras legales que intervienen en el tratamiento de datos.
- Conocer la legislación existente sobre los servicios de la sociedad de la información y el comercio electrónico.
- Contrastar las normas ISO sobre gestión de la seguridad de información.

1 >> Protección de datos de carácter personal

Seguramente todos estamos familiarizados con la expresión "protección de datos". Cuando vamos a alguna consulta médica privada por primera vez probablemente tengamos que rellenar un formulario con datos personales y relacionados con nuestra salud. Si estudiamos el documento con un poco de detenimiento veremos cómo al pie del formulario o en algún anexo se indica que nuestros datos van a formar parte de un fichero de datos protegido por la Ley Orgánica de Protección de Datos (LOPD). De la misma forma, cuando realizamos un trámite de forma telefónica, es frecuente que nos informen que la conversación puede estar siendo grabada.

Toda la información relativa a nuestra persona como: domicilio, fecha de nacimiento, estado civil, nivel de estudios, número de teléfono, DNI, grupos sociales, organizaciones a las que pertenecemos, religión, salud, aficiones, ideología política, imagen, etc., son datos personales que nos pertenecen y que nos pueden hacer vulnerables si caen en manos de personas no autorizadas.

Estos datos, además, son constantemente incorporados a bases de datos gestionadas por empresas privadas y organismos públicos: si te compras un teléfono, pasas a formar parte de la base de datos de la compañía telefónica; cuando te matriculas en un centro educativo, tus datos se incorporan a la base de datos de dicho centro, etc.

La **Constitución Española**, en su **artículo 18.4**, dice que "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".

Este mandato constitucional, unido a disposiciones de la Unión Europea como 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, han obligado a la autoridades españolas a regular legalmente la materia de la protección de datos.

La normativa básica al respecto es la siguiente:

- **Ley Orgánica 15/1999, de 13 de diciembre**, de Protección de Datos de Carácter Personal, en adelante LOPD.
- **Real Decreto 1720/2007, de 21 de diciembre**, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Esta normativa, con el ánimo de proteger a las personas físicas, detalla cómo se tienen que obtener los datos de carácter personal, cómo se tienen que conservar, si pueden cederse o no y si las empresas pueden remitir a las personas físicas correspondencia no solicitada (generalmente de carácter comercial).

Determina también los derechos que tienen las personas respecto a sus datos: cómo pueden acceder a ellos, cómo y cuándo pueden modificarlos o cancelarlos, etc. Para asegurar el cumplimiento de sus disposiciones, identifica las infracciones y les impone unas sanciones bastante severas.

Fichero

Es un conjunto organizado de datos de carácter personal que permite el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Ahora bien, **¿qué debe entenderse por datos de carácter personal?**

> **Según la LOPD, los datos de carácter personal son cualquier información concerniente a personas físicas identificadas o identificables.**

Por tanto, no todos los datos están protegidos por esta normativa, sino únicamente los relativos a las personas físicas, por lo que los relativos a las personas jurídicas (sociedades, organismos públicos, etc.) están excluidos. Los datos protegidos son de diverso tipo, como por ejemplo:

- Datos de identificación (nombre, apellidos, DNI, fotos, etc.).
- Circunstancias sociales y personales (estado civil, raza, religión).
- Datos sanitarios (expediente médico, enfermedades).
- Datos profesionales o académicos (expediente laboral, titulación).
- Datos comerciales (por ejemplo, solvencia).

1.1 > Tratamiento de los datos

El objeto de la normativa de protección de datos es vigilar que el tratamiento de los mismos sea adecuado. Pero, **¿qué es el tratamiento de los datos?**

> **El tratamiento engloba todas las operaciones y procedimientos mediante los que se recogen, almacenan, modifican y cancelan los datos, así como las cesiones que se llevan a cabo de los mismos.**

Es decir englobaría todas las operaciones que se llevan a cabo con los datos. No obstante, la propia LOPD excluye algunos tipos de tratamiento que no estarán sujetos a la misma:

- Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (por ejemplo, los datos recogidos en una agenda telefónica personal, siempre que no se tengan con finalidades comerciales).
- Los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

Las personas cuyos datos estén sometidos a tratamiento tienen los siguientes derechos:

- El tratamiento de los datos de carácter personal requerirá el **consentimiento** inequívoco del afectado, salvo que la ley disponga otra cosa. Este consentimiento podrá ser revocado.
- Consulta gratuita al Registro General de Protección de Datos sobre la existencia de tratamientos de datos de carácter personal.
- Acceso a sus datos sometidos a tratamiento.
- Rectificación y cancelación de sus datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la ley.
- Derecho a indemnización cuando sufran daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la ley por el responsable o el encargado del tratamiento.

Consentimiento del afectado

Para proceder al tratamiento de los datos de los mayores de catorce años será necesario su consentimiento, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela.

En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

Veamos cómo regula la normativa los distintos aspectos del tratamiento.

Recogida de los datos

Los datos se pueden obtener por tres vías:

- A través del propio interesado o sus representantes legales.
- A través de terceras personas que hayan cedido los datos obtenidos con anterioridad a sus titulares.
- De fuentes accesibles al público.

Cuando las empresas solicitan datos a una persona en un cuestionario o formulario en papel o formato informático, **deben informar previamente:**

- De la existencia del fichero o tratamiento y su finalidad.
- De la identidad y dirección del responsable del fichero.
- De los derechos que tiene el afectado (acceso, rectificación, cancelación y oposición al uso de sus datos).
- De las consecuencias que tendría la negativa a facilitar los datos.

Además de estas obligaciones básicas, hay determinados datos a los que, a causa de su contenido, la normativa otorga una protección especial:

- Los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias solo podrán ser tratados con el consentimiento expreso y por escrito del afectado.
- Los datos de carácter personal que hagan referencia al origen racial, la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
- Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas solo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Fuentes accesibles al público

Son aquellos ficheros que pueden ser consultados por cualquier persona. Por ejemplo, el censo promocional, los listados telefónicos, los diarios y boletines oficiales, los medios de comunicación, etc.

10.1. Logotipo anunciando que se está en una zona videovigilada.

Ejemplos

Cláusula informativa a los afectados del tratamiento de sus datos

En cumplimiento con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que sus datos personales serán tratados y quedarán incorporados en ficheros responsabilidad de JPAC, SL, registrados en la Agencia Española de Protección de Datos, con la finalidad de gestionar adecuadamente sus pedidos.

Los datos que se le solicitan resultan necesarios, de manera que de no facilitarlos no será posible la prestación del servicio requerido: en este sentido, usted consiente expresamente la recogida y el tratamiento de los mismos para la citada finalidad.

En todo caso, puede ejercitar los derechos de acceso, rectificación, cancelación y oposición dirigiéndose a la sede social, sita en calle Mayor, 6 de Logroño.

Conservación de los datos

En cuanto a la conservación de los datos, el responsable de los ficheros en los que consten deberá adoptar las medidas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Los datos no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos y deben ponerse al día de forma que respondan con veracidad a la situación actual del afectado.

Las empresas, dentro del deber de conservar la documentación que elaboran, deben archivar esta durante los plazos marcados por la ley. Cuando los ficheros de la empresa contengan datos personales, esta tiene las siguientes obligaciones:

- Inscribirlos en el Registro de Protección de Datos, existente en la Agencia Española de Protección de datos.
- Informar a los afectados de que sus datos figuran en un archivo, indicando dónde está ese archivo y cuál es su finalidad y solicitarles el consentimiento para poder tratar sus datos.
- No ceder los datos sin el expreso consentimiento de sus titulares.
- Guardar secreto y mantener la confidencialidad de los datos recogidos. Esta obligación incumbe tanto la empresa como a sus trabajadores respecto de los datos que conocieran por su trabajo.
- Adoptar, en la conservación de los datos, las medidas de seguridad exigidas por la legislación.
- Permitir a los titulares de los datos el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición.

Cuando en un archivo figuren datos personales, las empresas deben tomar las medidas necesarias que garanticen la seguridad de los mismos y eviten su alteración, pérdida o el acceso no autorizado.

En función del tipo de datos de que se trate, la legislación establece tres niveles de seguridad: básico, medio y alto.

Nivel de protección básico

Es el que se aplicará a los archivos, salvo que estén en uno de los otros niveles. En este nivel se aplicarán las siguientes medidas de seguridad:

- Deberá redactarse el **documento de seguridad**.
- Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal, las cuales deberán anotarse en un registro especial.
- Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
- La creación y salida de soportes (CD, DVD…) que contengan datos de carácter personal deberá ser previamente autorizada.
- Los usuarios deberán estar perfectamente identificados (por ejemplo, con el uso de contraseñas) para el acceso a los datos.
- Deberán realizarse, al menos con una frecuencia semanal, copias de seguridad, salvo que en ese periodo no se produjera ninguna actualización de los datos.

Confidencialidad

La obligación de confidencialidad persiste aún después de la cancelación o destrucción de los documentos con datos personales.

Por esto muchas empresas hacen firmar a sus trabajadores las denominadas "cláusulas de confidencialidad".

Cesión de los datos

Es la revelación de datos realizada a una persona distinta del interesado. Puede llevarse a cabo mostrando los datos o transmitiéndolos a otra persona o empresa.

Documento de seguridad

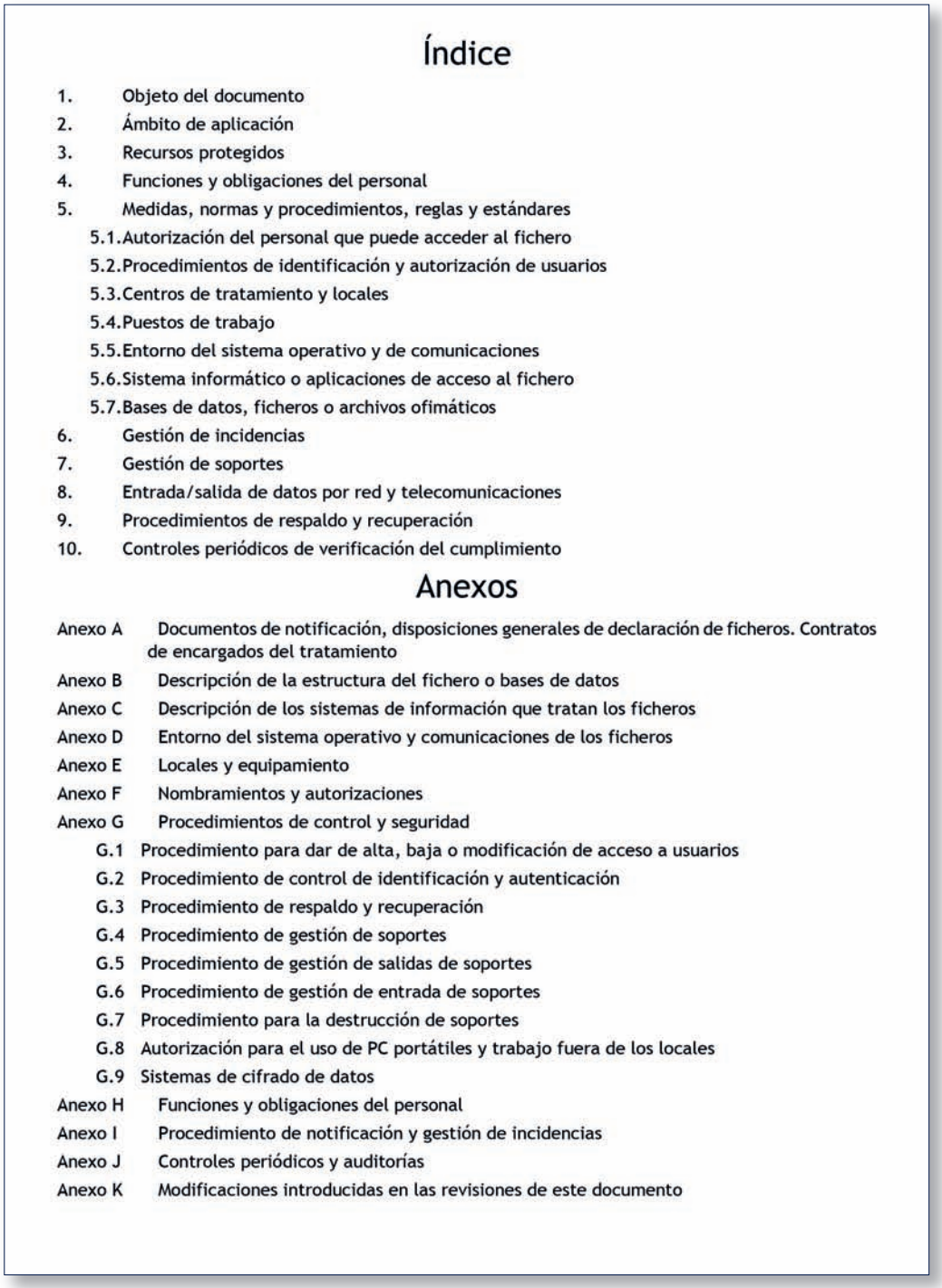
Es un documento formal que recoge la normativa de seguridad de la empresa. En él deben figurar todas las medidas de seguridad y confidencialidad para la protección de datos personales.

En la página web de la Agencia Española de Protección de Datos, www.agpd.es, puede descargarse un modelo de este documento.

Ejemplos

Documento de seguridad

La siguiente imagen muestra un ejemplo de los contenidos que incluye un documento de seguridad. Como se ve, regula detalladamente todos los procesos y medidas que se aplican en la empresa en materia de protección de datos personales.



Índice

Anexos

Nivel de protección medio

Se aplicará a los archivos que contengan:

– Datos sobre la comisión de infracciones administrativas o penales (por ejemplo, aquellos en que consten las multas de tráfico de una persona o donde figuren sus antecedentes penales).
– Información de la Hacienda Pública (por ejemplo, los datos que reflejan lo que se ha declarado a Hacienda).
– Información de servicios financieros (por ejemplo, datos que poseen las entidades bancarias acerca de los movimientos de las cuentas de una persona o de las deudas de la misma).

En este nivel se aplicarán las medidas establecidas para el nivel básico y además:

– Deberán designarse uno o varios **responsables de seguridad.**
– Los ficheros se someterán, al menos cada dos años, a una auditoría que verifique el cumplimiento de las medidas de seguridad.
– Se establecerán registros de entrada y salida de soportes que permitan conocer todas las circunstancias relativas a los mismos (cuándo entran y salen y quién los lleva).
– Se establecerán mecanismos para limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.
– Solo podrá tener acceso a los lugares físicos donde se encuentren los soportes de los sistemas de información el personal autorizado.
– Deberán registrarse los procesos de recuperación de datos.

Nivel de protección alto

Se aplicará a los archivos que contengan: datos de ideología, afiliación sindical, religión, creencias, raza, salud o vida sexual (por ejemplo, datos de afiliación a un partido político o sindicato, historiales médicos, etc.), así como los relativos a violencia de género.

En este nivel se aplicarán las medidas propias del nivel medio y además:

– Las copias de seguridad deberán guardarse en lugar diferente de aquel en el que están los equipos informáticos que contienen los datos copiados. No tiene sentido hacer copias de datos y guardarlas en el mismo equipo, puesto que cualquier incidente (robo, incendio, etc.) afectaría tanto al original como a la copia.
– Se creará un registro de accesos para tener constancia de quién y cuándo ha accedido a los datos.
– Cuando se extraigan o transporten datos de carácter personal (por ejemplo, en un ordenador portátil o un soporte externo, como un *pendrive* o DVD), dichos datos deberán estar cifrados, para que, en caso de que el soporte caiga en manos indebidas, nadie pueda acceder a ellos.
– La transmisión de los datos a través de redes de comunicaciones electrónicas se hará igualmente cifrando dichos datos, de forma que aunque caigan en manos indebidas su contenido no pueda ser conocido (por ejemplo, si se adjuntan a un mensaje de correo electrónico y hay un error en la dirección de entrega, o si un pirata informático intercepta la comunicación).

Responsable de seguridad

Persona a la que el responsable del fichero ha asignado la función de coordinar y controlar las medidas de seguridad aplicables.

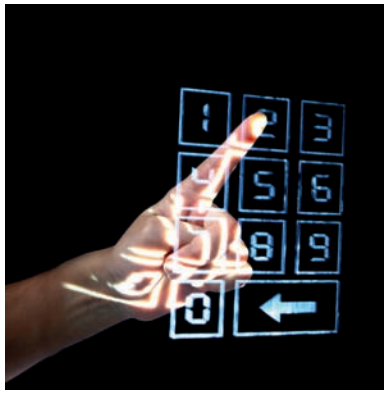
Casos prácticos 1

Aplicación de medidas de seguridad en ficheros automatizados

•• El departamento de personal de una empresa tiene una base de datos en la que figuran todas las circunstancias necesarias para la administración de la relación con sus empleados y el abono de sus nóminas. En dicha base figuran el nombre y apellidos de los empleados, su dirección, correo electrónico y número de teléfono; también se incluyen el historial de enfermedades de dichos empleados, así como sus datos de afiliación sindical.

¿Según la legislación de protección de datos, qué medidas de seguridad debe tomar esa empresa respecto a la base de datos indicada?

Solución •• La base de datos expuesta en el enunciado es un fichero de carácter automatizado, por lo que se deberán tomar las medidas referidas a este tipo de ficheros.



En cuanto al nivel de protección, habrá que observar los datos recogidos en el fichero. Los datos de filiación (nombre, apellidos, etc.) requerirían protección de nivel básico, pero junto a ellos existen otros datos que requieren un nivel de protección alto, pues hacen referencia a la afiliación sindical y a la salud. Cuando en un fichero hay varios tipos de datos, siempre hay que aplicar el nivel de protección correspondiente a los datos más sensibles, en este caso, por tanto, se aplicará el correspondiente al nivel alto.

Como consecuencia de ello, habrá que implementar conjuntamente las medidas de nivel básico, las de nivel medio y las de nivel alto. Por tanto, deberán aplicarse estas medidas:

- Deberá redactarse el documento de seguridad.
- Deberán designarse uno o varios responsables de seguridad.
- El fichero deberá someterse, al menos cada dos años, a una auditoría de seguridad.
- Será necesario establecer un procedimiento de notificación y gestión de las incidencias referentes a los datos, las cuales deberán anotarse en un registro.
- Los usuarios únicamente podrán acceder a los datos identificándose con un nombre y contraseña. Además cada usuario solo podrá hacerlo a los datos que necesite para ejercer sus funciones (por ejemplo, solo se podrá acceder a los datos médicos para computar las bajas médicas) y todos los accesos a datos quedarán registrados para saber quién ha accedido a ellos y cuándo lo ha hecho.
- En caso de que un usuario no autorizado intentara reiteradamente acceder a los datos, se bloqueará su acceso.
- Solo se podrán grabar los datos en un soporte externo con previa autorización del responsable de seguridad. Además, si ese soporte va a salir de la empresa, deberá anotarse en un registro especial quién es el portador del mismo y cuándo se produce la salida. Cuando el soporte vuelva a entrar, se volverá a anotar la entrada. Además, como el nivel de protección es alto, debe establecerse un sistema de cifrado para el soporte que impida a un usuario no autorizado acceder a los datos.
- Deberán realizarse, al menos semanalmente, copias de seguridad (salvo que los datos no varíen). Estas copias deberán guardarse en un lugar diferente a aquel en que se encuentran almacenados los datos originales.
- Únicamente el personal debidamente autorizado podrá acceder a los lugares físicos donde están almacenados los datos.
- En caso de que los datos se transmitan a través de redes de telecomunicaciones, se deberán tomar medidas para asegurar la confidencialidad y, además, la transmisión deberá estar cifrada.

1.2 > Elementos personales que intervienen en el tratamiento de los datos

La normativa en materia de protección de datos reconoce varias figuras que intervienen en el tratamiento y mantenimiento de los ficheros de datos:

- **Afectado:** es la persona física titular de los datos objeto del tratamiento. Como luego veremos, tiene diversos derechos, como el acceso a sus datos, la rectificación de datos erróneos y su cancelación, entre otros.
- **Responsable del fichero o tratamiento:** es la persona física, jurídica o entidad sin personalidad (por ejemplo, una comunidad de vecinos), que decide sobre la finalidad, contenido y uso del tratamiento de los datos, aunque no lo realice materialmente.
- **Encargado del tratamiento:** es la persona física o jurídica, pública o privada, u órgano administrativo, que lleva a cabo el tratamiento de datos personales por cuenta del responsable del tratamiento o del responsable del fichero. Es decir, trata los datos, pero no tiene capacidad para decidir el por qué del tratamiento ni la finalidad del mismo.
- **Cesionario:** la persona física o jurídica, distinta del afectado, a la que se cedan los datos, por parte del responsable.
- **Tercero:** cualquier persona física o jurídica distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Tratamientos por cuenta del responsable

La realización de tratamientos por cuenta del responsable deberá estar regulada en un contrato.

En él se deberá determinar que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los utilizará con fin distinto al que figure en dicho contrato, ni los comunicará a otras personas.

Casos prácticos 2

Elementos personales del tratamiento de datos

•• La empresa GESTOSA, SL dispone de un fichero con los datos personales de sus trabajadores con la finalidad de gestionar la relación laboral existente con ellos. Para gestionar el pago de las nóminas y los seguros sociales, ha cedido este fichero a la asesoría laboral NOMINASA. Además, con consentimiento de los trabajadores, ha cedido algunos de sus datos (nombre y correo electrónico) a DESCONTISA una empresa de gestión de cupones de descuento por Internet, para que les remitan ofertas personalizadas por su pertenencia a GESTOSA.

Identifica los elementos personales de este tratamiento de datos.

Solución •• Los elementos personales que figuran en este tratamiento son los siguientes:

- **Afectados:** serían cada uno de los trabajadores de la empresa GESTOSA, cuyos datos personales son objeto del tratamiento.
- **Responsable del tratamiento:** sería GESTOSA, que es la titular de los datos y la que decide sobre la finalidad y el uso del tratamiento de esos datos.
- **Encargado del tratamiento:** sería la asesoría laboral NOMINASA, quien, mediante un contrato suscrito con GESTOSA, recibe los datos y procede a su tratamiento, exclusivamente con la finalidad encomendada, sin que pueda ceder esos datos a terceros.
- **Cesionario:** DESCONTISA, quien recibe los datos de los trabajadores, en virtud del consentimiento prestado por ellos, para la gestión de los vales de descuento.

1.3 > Derechos de los afectados

Los afectados por el tratamiento tienen los siguientes derechos:

- **Derecho de consulta** al Registro General de Protección de Datos para conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.
- **Derecho de acceso.** El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
- **Derecho de oposición.** Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo, cuando no sea necesario su consentimiento para el tratamiento.
- **Derecho de rectificación y cancelación.** El afectado tiene derecho a rectificar o cancelar sus datos cuando su tratamiento no se ajuste a lo dispuesto en la ley y, en particular, cuando tales datos resulten inexactos o incompletos.
- **Derecho a indemnización** por los daños o lesiones ocasionados en sus bienes o derechos.

El interesado al que se deniegue el ejercicio de sus derechos podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o del organismo competente de cada Comunidad Autónoma, que, en su caso, impondrá la correspondiente sanción.

Ejercicio de los derechos

Los derechos de oposición, acceso, rectificación o cancelación se ejercitarán mediante solicitud del interesado al responsable del tratamiento, que deberá conceder lo solicitado, si se cumplen los requisitos establecidos, en un plazo de diez días. A la solicitud se acompañará, cuando sea necesaria, la documentación justificativa de la misma. Este ejercicio será gratuito para los interesados.

Ejemplos

Ejercicio del derecho de cancelación

D. Antonio Torres Vega, mayor de edad, con domicilio en la Plaza Bronce, nº. 12, de Almazán, provincia de Soria, C.P. 42212, comunidad autónoma de Castilla y León, con DNI: 16202404C, del que acompaño copia, por medio de la presente solicitud manifiesto el deseo de ejercer mi DERECHO DE CANCELACIÓN respecto a mis datos de carácter personal.

De conformidad con el artículo 16 de la Ley Orgánica 15/1999, y 25, 31 y 32 del Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, solicito que se proceda a la efectiva cancelación de cualesquiera de los datos relativos a mi persona que se encuentren en los ficheros que a continuación se mencionan y me sea comunicada la misma de forma escrita a la dirección arriba indicada en el plazo máximo de diez días desde la recepción de esta solicitud.

En el caso de que los datos objeto de esta cancelación hubieran sido comunicados previamente, solicito de la misma forma que el responsable del tratamiento notifique de esta cancelación a quienes hubieran sido comunicados, para que proceda de igual manera a la cancelación de los mismos.

En Almazán a 22 de Noviembre de 2014

Firmado: Antonio Torres Vega

DATOS DEL RESPONSABLE DEL FICHERO: JPAC SL, Plaza Mayor nº 6, C. Postal 42214, Soria, Castilla y León, CIF: A-789456

1.4 > Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica y plena capacidad, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Está regulada en el Título VI de la Ley Orgánica 15/1999 y un estatuto propio que, a la fecha de publicación de este libro, es el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Podemos agrupar sus funciones del siguiente modo:

Tipo de función	Funciones
General	Vigila el cumplimiento de la legislación sobre protección de datos y controla que se aplique, especialmente, en lo referente a derechos de información, acceso, rectificación, oposición y cancelación de datos.
En relación con los afectados	Se encarga de atender sus peticiones y reclamaciones, así como de informar de sus derechos reconocidos en la ley a través de diversas campañas de difusión.
En relación con quienes tratan los datos	Emite las autorizaciones pertinentes previstas en la ley, así como autoriza transferencias internacionales de datos. Puede requerir medidas de corrección y ordenar, en caso de que no se cumpla la ley, el cese en el tratamiento y la cancelación de los datos. Ejerce la potestad sancionadora.
En la elaboración de normas	Informa los proyectos de normas de desarrollo de la LOPD y de normas en materias de protección de datos. Dicta instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD y en materia de seguridad y control de acceso a los ficheros.
En materia de telecomunicaciones	Vela por los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas.
Otras funciones	Coopera con otros países, representa a España en los foros internacionales en la materia de protección de datos, imparte formación específica en la materia, etc.

Web

www.agpd.es: página web del la Agencia Española de Protección de Datos.

Actividades propuestas

1·· Busca en algunas revistas o en Internet hechos que aparentemente vulneren el derecho a la intimidad de las personas relacionados con la utilización de las nuevas tecnologías.

2·· Busca información sobre las infracciones y sanciones aplicables en materia de protección de datos.

3·· ¿Existe en tu Comunidad Autónoma algún organismo específico en materia de protección de datos?

4·· ¿Cuál es la función principal de la Agencia Española de Protección de Datos?

5·· Describe las acciones que debe realizar la persona responsable de un fichero de datos para cumplir la ley.

6·· Consulta la Carta de Servicios de la AEPD. ¿Qué información contiene? Esquematiza su contenido.

2 >> Legislación sobre los servicios de la sociedad de la información y comercio electrónico

Actualmente se habla muy a menudo de la sociedad de la información, pero ¿realmente sabemos lo que significa?

Desde sus comienzos, Internet ha sido y es un filón interminable para la comunicación. Las empresas han visto en la Red una forma económica de expandir sus negocios. Pero la generalización en el uso de la web lleva aparejados nuevos riesgos, pues actualmente todo está conectado y la información fluye como nunca antes lo había hecho. Además, Internet supone la aparición de nuevas formas de negocio que se escapan a la legislación pre-Internet y se mueven en áreas donde existe un vacío legal.

En todo este contexto, surge la **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE)**, con la intención de establecer las nuevas reglas del juego que indiquen los derechos y deberes de empresas y particulares en el mundo de las transacciones de productos y prestaciones de servicios realizadas a través de Internet.

Esta ley tiene por objeto determinar el régimen jurídico aplicable a los **servicios de la sociedad de la información**, entendiéndose por tales:

> **Aquellos servicios que se prestan telemáticamente o que se apoyan en plataformas de telecomunicaciones para su difusión y que suponen una actividad económica para la empresa, entidad o individuo que los presta.**

Como supuestos de sociedad de la información, la propia ley cita los siguientes:

- La contratación de bienes y servicios por vía electrónica.
- El suministro de información por dicho medio (como el que efectúan los periódicos o revistas que pueden encontrarse en la red).
- Las actividades de intermediación relativas a la provisión de acceso a la red.
- La transmisión de datos por redes de telecomunicaciones.
- La realización de copia temporal de las páginas de Internet solicitadas por los usuarios.
- El alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la 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.

Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

INTECO

El Instituto Nacional de Tecnologías de la Comunicación SA (INTECO) nace con varios objetivos, entre los cuales está el de servir como instrumento para desarrollar la sociedad de la información basándose la investigación aplicada, la prestación de servicios y la formación. Su web es www.inteco.es

Información que se debe facilitar a los usuarios de los servicios de la sociedad de la información

En España, hasta la llegada de la LSSICE, cualquiera se podía abrir una web sin necesidad de añadir información sobre la persona física o jurídica que estaba detrás de la misma. El usuario podía encontrarse con el caso de utilizar los servicios de una web y, en caso de tener que reclamar, no encontrar dónde ni a quién reclamar.

En este sentido, la LSSICE obliga a informar a los usuarios de diversos aspectos relacionados con los servicios que se les están prestando por vía electrónica. Esta información se adapta al servicio que se preste.

Información general

Toda web que suponga una actividad económica (porque está asociada a un negocio físico, porque ofrece algún servicio de pago en Internet o porque obtiene ganancias a partir de la publicidad) debe incluir, claramente visible, la siguiente información:

- El nombre o denominación social del prestador de los servicios, su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
- El número de identificación fiscal que corresponda.
- Los datos de inscripción del prestador en el Registro Mercantil o en otro registro en el que debiera estar inscrito.
- Los códigos de conducta a los que, en su caso, esté adherido el prestador y la forma de consultarlos electrónicamente.
- Si la actividad estuviera sujeta a autorización administrativa, los datos referentes a la misma.
- Si la actividad hiciera referencia a una profesión regulada (por ejemplo, un abogado o un médico), datos del colegio profesional, título oficial con el que cuente el prestador, país en el que se expidió ese título, etc.
- Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

Ejemplos

Cláusula de aviso legal en página web comunicando los datos exigidos por la LSSI

A continuación incluimos un ejemplo de cláusula que debería ir incluida dentro del apartado *Aviso legal* de una página web, para dar cumplimiento a las obligaciones que exige la LSSI:

"En cumplimiento del artículo 10 de la Ley 34/2002, del 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE), se exponen a continuación los datos identificativos de la empresa: la empresa titular de www.jpac.es es JPAC, SL, con domicilio en calle Mayor, 6 de Soria, CP 42424 y NIF A-789456. Esta sociedad está inscrita en el Registro Mercantil de Soria, en el libro 145, tomo 452, página 256. E-mail para comunicaciones: info@jpac.es".

Información previa a la contratación

Si el prestador de servicios realiza actividades de contratación electrónica, además de la información general, tiene la obligación de poner a disposición del destinatario, antes de iniciar el procedimiento de contratación, de forma permanente, fácil y gratuita, información clara y comprensible sobre los siguientes extremos:

- Los distintos trámites que deben seguirse para celebrar el contrato.
- Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si este va a ser accesible.
- Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos.
- La lengua o lenguas en que podrá formalizarse el contrato.

Información sobre seguridad y privacidad

Las empresas que presten servicios de acceso a Internet deberán informar a sus clientes sobre:

- Los medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados (*spam*).
- Las medidas de seguridad que apliquen en la provisión de los mencionados servicios.
- Las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.

Información sobre comunicaciones comerciales

Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y el anunciante deberá también identificarse claramente. Si tienen lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente, incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi".

En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y en los concursos o juegos promocionales, además de los requisitos anteriores, se deberá obtener la autorización previa del destinatario y las condiciones de acceso y participación deben ser fácilmente accesibles y expresarse de forma clara e inequívoca.

Información sobre privacidad

Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales *(cookies)*, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Actividades propuestas

7·· ¿Cuál es el objetivo de la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico?

8·· Busca en Internet el texto de la LSSICE y lee el artículo 21. ¿A qué se refiere dicho artículo?

9·· ¿Por qué crees que los prestadores de servicios deben informar sobre el uso de *cookies*?

10·· Pon ejemplos de los distintos supuestos que, según la LSSICE, se pueden considerar un servicio de la sociedad de la información.

3 >> Sistemas de gestión de seguridad de la información

Uno de los principales activos que poseen las empresas es la información que manejan. Un correcto tratamiento de la información requiere la adopción de las medidas que sean necesarias para proteger los tres aspectos básicos de la misma: integridad, confidencialidad y disponibilidad.

Un Sistema de Gestión de la Seguridad de la Información o SGSI sería, por tanto, un conjunto de medidas destinadas a preservar estos tres elementos de la información que maneja una empresa, independientemente del soporte, tipo, etc., de la misma.

Para que estas medidas sean efectivas, deben llevarse a cabo a través de procesos estandarizados, documentados, conocidos y aplicados por toda la empresa. Para sistematizar estos procesos, existe un conjunto de normas conocidas como **ISO 27000**, encaminadas a la gestión de la seguridad. Una empresa puede elegir implementar estas normas o bien establecer su propia política de gestión de la seguridad, aunque el uso de estándares normalizados le permite acceder a certificaciones independientes.

En el cuadro siguiente se especifican algunas normas y guías relacionadas con esta normativa. Constantemente se van revisando y se crean otras nuevas respondiendo a las distintas necesidades.

Norma	Contenido
ISO/IEC 27000	Ofrece una visión general de las normas de toda la serie 27000, una introducción a los SGSI, terminología utilizada, etc.
ISO/IEC 27001	Es la norma principal y contiene los requisitos del sistema de gestión de seguridad de la información. Es la norma utilizada por los auditores externos para certificar los SGSI de las empresas.
ISO/IEC 27002	Guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables relativos a la seguridad de la información. No es certificable.
ISO/IEC 27003	Se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. No es certificable.
ISO/IEC 27004	Guía para medir eficacia de un SGSI. No es certificable.
ISO/IEC 27005	Proporciona las directrices para la gestión del riesgo en la seguridad de la información. No es certificable.
ISO/IEC 27006	Especifica los requerimientos para la acreditación de entidades de auditoría y certificación de SGSI.
ISO/IEC 27007 ISO/IEC TR 27008	Guías de auditoría.
ISO/IEC 27011	Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

Elementos de la información

- **Integridad:** implica el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Confidencialidad:** implica que únicamente pueden acceder a la información quienes estén autorizados para ello.
- **Disponibilidad:** supone la posibilidad de que los usuarios autorizados puedan acceder a la información cuando deseen.

3.1 > Contenido de un SGSI

Las medidas que integran el SGSI deben estar recogidas en una serie de documentos que, según ISO 27001, están estructurados en los siguientes niveles:

- **Nivel 1:** este determina las normas fundamentales del sistema, que están recogidas en el **manual de seguridad**. Este documento expone los objetivos, políticas, directrices, etc., del SGSI.
- **Nivel 2:** en este nivel se encuentran los documentos de **procedimientos**. Son los documentos de carácter operativo, que definen la planificación, realización y control de los procesos que integran el sistema.
- **Nivel 3:** los documentos de este nivel son las **instrucciones**, ***checklists*** **y formularios**. En ellos se describe la forma de realizar las tareas y las actividades relacionadas con la seguridad de la información.
- **Nivel 4:** está integrado por los **registros**, que son documentos que demuestran que se ha cumplido lo indicado en los otros tres niveles.

3.2 > Implantación de un SGSI

Uno de los aspectos más destacados del ISO 27000 es la descripción del proceso de implantación de un SGSI. Básicamente se resume en un proceso cíclico continuo que pasa por las fases ***Plan-Do-Check-Act*** y vuelta a empezar.

- **Arranque o inicio del proyecto:** en esta fase es necesario un compromiso por parte de la dirección de la empresa u organización, la realización de una buena planificación, así como la asignación de los responsables del proyecto.
- **Planificación (*Plan*).** En esta fase se deberían concretar aspectos como: la definición del alcance del SGSI, la política y los objetivos en materia de seguridad, la metodología y enfoque a utilizar para la evaluación de riesgos, el inventario de activos, la identificación de puntos débiles, la identificación de impactos, etc.
- **Realización (*Do*).** En esta fase se definiría e implantaría el plan de tratamiento de riesgos, se implementarían elementos de control, tareas de formación y concienciación al personal y se operaría ya con el SGSI.
- **Revisión (*Check*).** Posteriormente a la fase de realización, se hace necesario revisar el proceso con el fin de medir la eficacia de los controles y revisar otros riesgos. Se realizan auditorías internas del SGSI, así como un registro de las distintas acciones y eventos.
- **Actuación (*Act*).** En esta fase se implantarían mejoras y se adoptarían medidas correctoras y preventivas, con el fin de comprobar la eficacia de las acciones realizadas.

Web

www.iso27000.es: portal de información, en español, sobre las normas ISO 27000.

Actividades propuestas

11·· ¿Es lo mismo seguridad informática que seguridad de la información? Matiza tu respuesta.

12·· ¿Qué necesita una empresa, que tiene implantado un SGSI, para obtener una certificación ISO 27000?

13·· Realiza un esquema que recoja las fases de un SGSI y las principales actividades que se llevan a cabo en cada una de ellas.

Actividades finales

.: CONSOLIDACIÓN :.

1·· ¿En qué consiste la protección de datos?

2·· ¿Qué tipo de datos protege la Ley Orgánica de Protección de Datos?

3·· ¿Qué diferencias hay entre el responsable del fichero y el responsable del tratamiento del mismo?

4·· Indica qué tipos de medidas de seguridad se aplicarían a los ficheros que contienen la siguiente información sobre tu persona:

a) Datos fiscales.
b) Estado de salud.
c) Afiliación a un partido político.
d) Color de pelo.
e) Número de teléfono.
f) Multas de tráfico.

5·· ¿Qué es una auditoría de protección de datos?

6·· ¿Qué es un documento de seguridad?

7·· ¿Qué es INTECO? ¿Existen más organismos del mismo tipo?

8·· ¿Qué es un SGSI?

9·· ¿Cómo podrías saber qué ficheros de titularidad pública o privada contienen tus datos de carácter personal? ¿Qué deberías hacer si quisieras que tus datos fueran eliminados de los mismos?

.: APLICACIÓN :.

1·· Cumplimenta a través de Internet algún tipo de cuestionario. Verifica que se te informa de que tus datos van a registrarse en cumplimiento de la LOPD. Copia en un documento de texto la URL de dicha web, así como el texto informativo en materia de protección de datos.

2·· Una empresa tiene una base de datos de clientes en la que únicamente figuran sus nombres y apellidos, dirección, correo electrónico y número de teléfono. ¿Qué medidas de seguridad debe de tomar esa empresa según la legislación de protección de datos?

3·· Imagina que habéis creado una página web para la clase. En ella hay páginas relativas a los estudios, las prácticas, apuntes, fotos de actividades, etc.

a) ¿Puedes colocar en ella fotos con tus compañeros de clase, algunos de los cuales son menores de edad? ¿Por qué?
b) ¿Qué tendrías que hacer para cumplir con las obligaciones de la LOPD?
c) ¿Puedes ser sancionado?
d) ¿Pueden publicarse en la web las notas de los alumnos? Justifica tu respuesta.

4·· Suscríbete a algún foro o servicio de Internet en el que se pida como dato de registro tu dirección de correo electrónico. ¿Puedes modificar tus datos fácilmente? ¿Cuándo te das de alta, te facilitan algún enlace para poder darte de baja de dicho servicio si ya no quieres pertenecer a él?

5·· ¿Existen medidas que protejan los distintos tipos de datos o información personal que publicas en una red social (Tuenti, Facebook, Twitter, etc.)? Cita ejemplos.

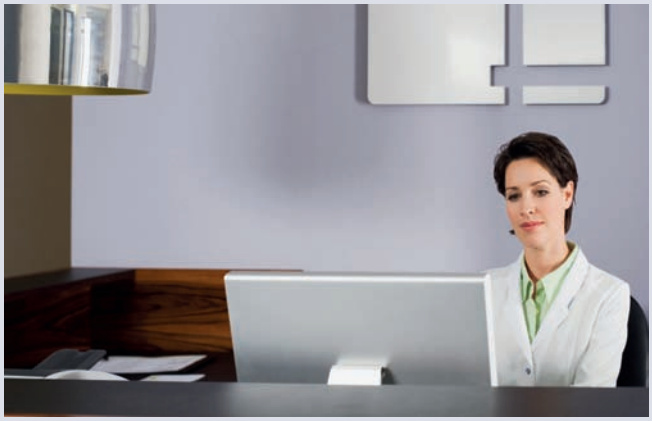
6·· Investiga la forma de darse de baja de las principales redes sociales. ¿Conservan estas redes sociales los datos de sus antiguos usuarios?

Caso final 3

Adecuación de una empresa a la normativa de protección de datos

•• Mario acaba de ser contratado como técnico informático por la empresa TUSALUD, SL, que gestiona una clínica dental llamada MIRAME. Al revisar la documentación de la empresa, descubre que a los pacientes no se les informa de que sus datos van a ser incorporados a un fichero para su tratamiento. Además, el informático anterior no ha dado de alta en la AEPD ninguno de los ficheros que utiliza la empresa. Estos ficheros incluyen datos de los pacientes, mientras que una gestoría externa se ocupa de la elaboración de las nóminas y seguros sociales.

La clínica tiene dos ordenadores, uno en la consulta y otro en recepción. En la clínica trabajan con un sistema Windows en red y los datos están incluidos en una base de Access, guardada en el ordenador de recepción, que hace las veces de servidor web. No utilizan ningun control de acceso a la información, por lo que cualquier persona que acceda desde uno de los ordenadores de la clínica tiene acceso a los datos recogidos en los ficheros.

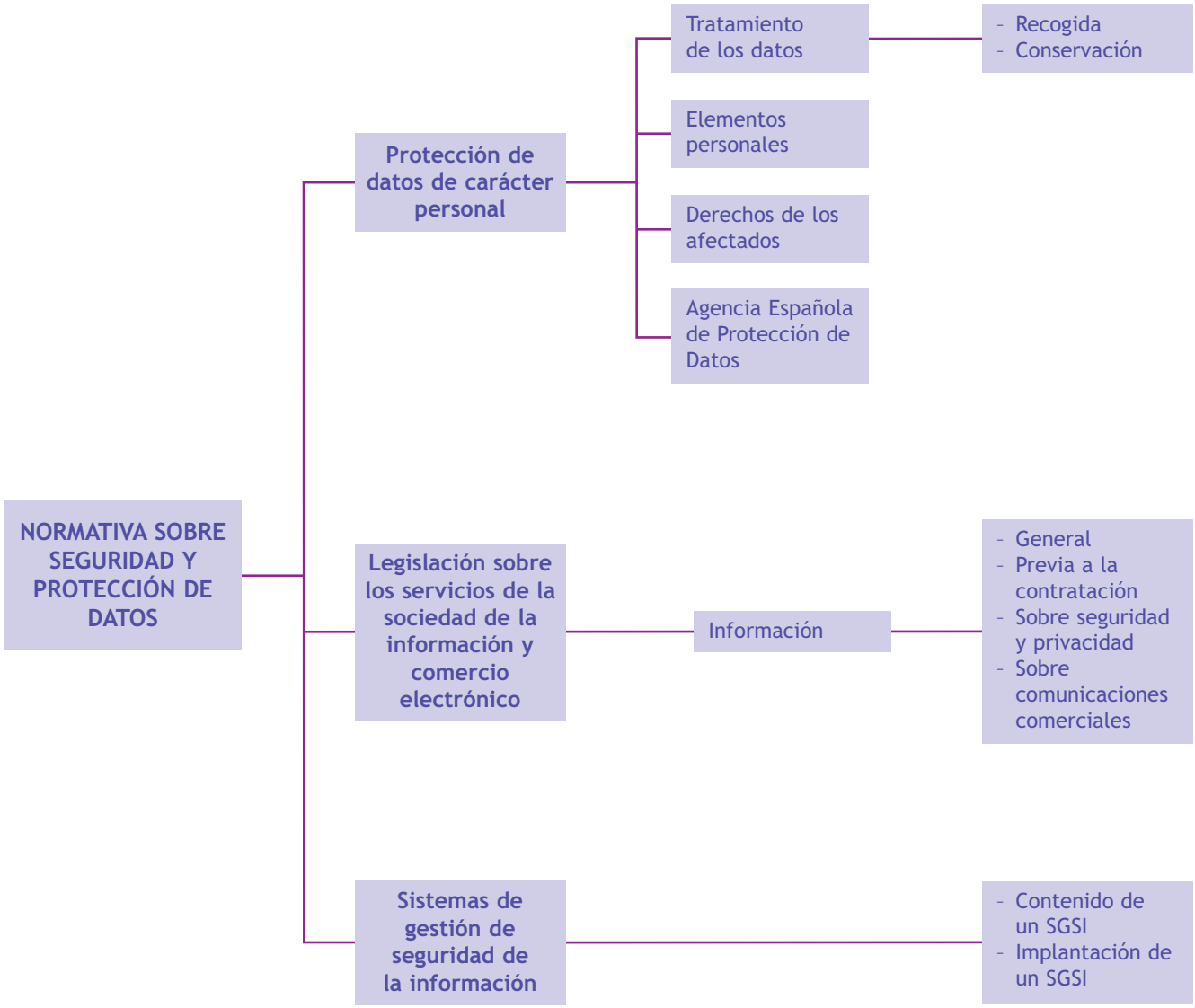


Como nuevo responsable de informática, le han encomendado que indique las medidas que debería tomar la empresa para cumplir la LOPD.

Solución •• Esta empresa no cumple ninguno de los requisitos exigidos por la legislación de protección de datos, por ello, vamos a dividir las medidas por áreas.

- **Identificación de usuarios:** el primer paso será restringir el acceso a la información. Para ello, se recomienda que se establezcan en cada uno de los equipos distintas contraseñas de inicio de sesión que, por un lado, impidan el acceso de personas no autorizadas y, por otro, identifiquen a las personas que acceden a la información. Para evitar que los datos incluidos en la base se modifiquen por personal no autorizado, se recomienda que se ubique en una carpeta en la que únicamente los usuarios autorizados tengan permisos de lectura y escritura.
- **Copias de seguridad:** no se indica nada, pero se supone que no se realizan, por ello, debería copiarse al menos semanalmente el contenido de la base en un dispositivo externo, por ejemplo una memoria USB que debería depositarse en un lugar distinto a la consulta. Dada la naturaleza de los datos, el contenido de dicho disco debería estar cifrado.
- **Declaración de ficheros:** habría que dar cuenta a la AEPD de los ficheros que contienen datos de carácter personal (proveedores, pacientes, personal) a través del formulario NOTA o por correo certificado.
- **Documento de seguridad:** debe elaborarse el documento y recoger todas las medidas adoptadas, así como la gestión de las posibles incidencias.
- **Designación del responsable de seguridad.**
- **Clausulado:** en los documentos en que se recojan los datos de los pacientes debe incluirse una cláusula donde estos, expresamente, autoricen a la clínica a proceder al tratamiento de sus datos.
- **Gestión de los datos por terceros:** dado que se transfieren los datos de los trabajadores a la gestoría para que elabore sus nóminas, habrá que suscribir con ella un contrato de acceso a datos por cuenta de terceros. En este caso, la gestoría pasaría a ser el encargado del tratamiento.
- **Auditoría de seguridad:** al menos cada dos años deberá llevarse a cabo una auditoría detallada sobre la seguridad de la empresa.

Ideas clave


NORMATIVA SOBRE SEGURIDAD Y PROTECCIÓN DE DATOS
Protección de datos de carácter personal
Tratamiento de los datos
- Recogida
- Conservación
Elementos personales
Derechos de los afectados
Agencia Española de Protección de Datos
Legislación sobre los servicios de la sociedad de la información y comercio electrónico
Información
- General
- Previa a la contratación
- Sobre seguridad y privacidad
- Sobre comunicaciones comerciales
Sistemas de gestión de seguridad de la información
- Contenido de un SGSI
- Implantación de un SGSI

Datos falsos en los procesos de matriculación escolar

Por todos es conocida la polémica que todos los años rodea al proceso de selección de alumnos en los colegios, que se basa en la asignación de puntos atendiendo a la renta familiar y a la proximidad del domicilio o lugar de trabajo al centro escolar.

Pues bien, esta polémica estalló cuando se descubrió, o mejor dicho, se comenzaron a denunciar, los trucos o engaños que llevaban a cabo algunos padres para obtener más puntos en el proceso de selección, tales como falsear los datos del domicilio (empadronándose en domicilios de familiares, en pisos vacíos o incluso en garajes), los datos del lugar de trabajo, e incluso simular el padecimiento de una alergia o intolerancia alimentaria de sus hijos para excluir determinados centros que carecieran de la dieta necesaria para atenderlos.

Muchas comunidades, como Andalucía, han tomado cartas en el asunto, azuzados por las denuncias de aquellos padres que han visto cómo sus hijos no han sido admitidos en el colegio deseado frente a otros que sí lo han sido pese a no contar con los requisitos exigidos.

Tal es así que, cuando se conoce la existencia de fraude en los datos de solicitud, los alumnos pierden todos los puntos del baremo, cuando antes se quedaban sin los de domicilio. Cataluña anunció hace unos meses que durante el proceso de matriculación escolar las familias podrían tener acceso al nombre y domicilio de otro solicitante, animando con ello a que los propios padres denuncien los fraudes, pero ¿esto no vulneraría el derecho a la protección de los datos personales de dichos padres? Los padres aportan sus datos personales en los impresos de solicitud de plaza en un centro escolar con la única y exclusiva finalidad de obtener plaza en dicho centro o, en su caso, en alguno de los que les corresponden según baremo y disponibilidad, pero no para que sean comunicados públicamente a terceros.

Según el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), cuando se utilicen cuestionarios u otros impresos para la recogida de datos personales, figurarán en los mismos, en forma claramente legible, las advertencias relativas, entre otras, a la finalidad de la recogida de los datos personales y a los destinatarios de los mismos. Se hace necesario, por tanto, articular un sistema o procedimiento que evite o elimine los fraudes en las matriculaciones de los alumnos sin que se conculque el derecho fundamental a la protección de datos personales.

Fuente: *N. Garcia, publicado el 13 de noviembre de 2012 en www.delitosinformaticos.com*

Actividades

1·· ¿Crees que los centros educativos que están publicando los datos indicados en el artículo están violando la normativa en materia de protección de datos? Debate con tus compañeros sobre esta medida.

© MACMILLAN IBERIA, S.A. empresa que pertenece al **GRUPO MACMILLAN**
c/ Capitán Haya, 1 — planta 14ª. Edificio Eurocentro
28020 Madrid (ESPAÑA)
Teléfono: (+34) 91 524 94 20

Agradecimientos: Centro Criptológico Nacional (CCN), ClamAV, Clonezilla, Cryptophane, Debian, Fedora, fwbuilder, GetDataBack, Google, iptables, Linux, Microsoft, Mozilla Firefox, rsync, Spybot - Search & Destroy, TechTracker, Thunderbird, TrueCrypt.

Edición: Luis Ángel Ramos
Revisión técnica y corrección: Lydia López
Coordinación de maquetación: Ángeles Marcos
Maquetación: Artes Gráficas G3
Diseño de cubierta e interiores: equipo Macmillan Profesional
Realización de cubierta: Silvia Pasteris, Ángeles Marcos
Ilustraciones: Artes Gráficas G3
Fotografías: Agencia Española de Protección de Datos, Belkin, East of England Broadband Network (E2BN), ING image, Netgear, QNAP, RSA

ISBN EDICIÓN ELECTRÓNICA: 978-84-15991-41-0

Seguridad Informática

www.macmillanprofesional.es

Este libro analiza, con un enfoque práctico y actual, los conceptos básicos en materia de seguridad informática. Partiendo de la importancia que la seguridad tiene en el uso de sistemas informáticos, se desarrollan los procedimientos y herramientas necesarios para proteger equipos informáticos, redes y aplicaciones. Además, se aborda el estudio del marco jurídico relacionado con la protección de la información y los datos personales.

Los contenidos están distribuidos en diez unidades de trabajo. Cada una de ellas se desarrolla mediante explicaciones teóricas acompañadas de numerosos ejemplos, casos prácticos resueltos y actividades de consolidación y aplicación que permiten una eficiente asimilación de los conocimientos adquiridos.

Cada unidad finaliza con un caso práctico resuelto y un esquema de ideas clave que facilitan la comprensión de los contenidos, así como una revista de informática con informaciones útiles relacionadas con los objetivos de la unidad.

MACMILLAN Profesional