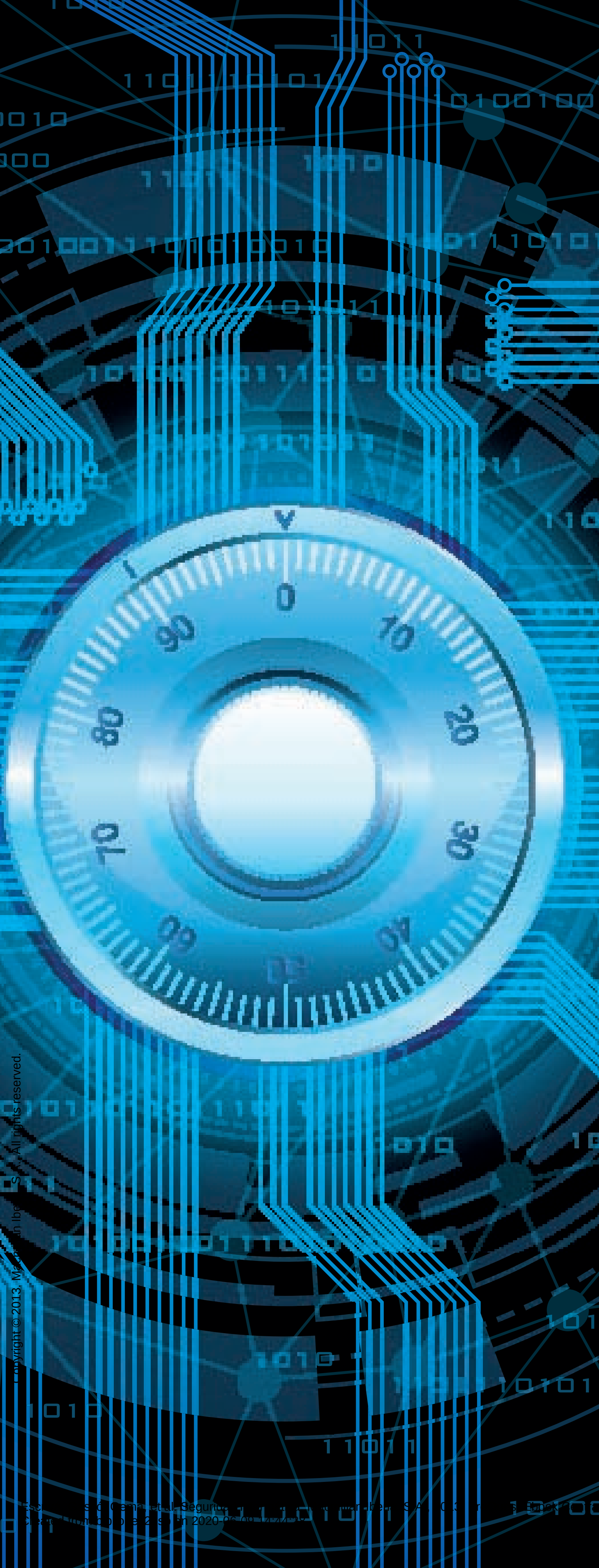


u n i d a d **1**

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.

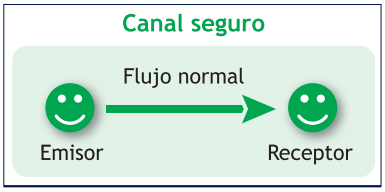
Las organizaciones deben estar preparadas ante cualquier tipo de desastre de manera que se reduzca el impacto que pueda ocasionar. Para ello, desarrollan e implantan planes de contingencia que permiten la prevención y recuperación de desastres informáticos.

Actividades propuestas

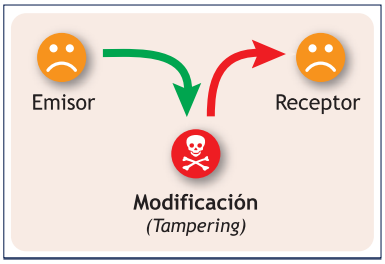
4·· ¿Crees que la evaluación de riesgos será igual para todas las empresas? ¿Por qué?

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.

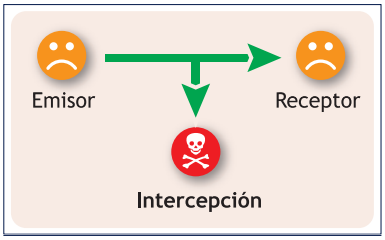


1.2. Violación de la integridad.

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:

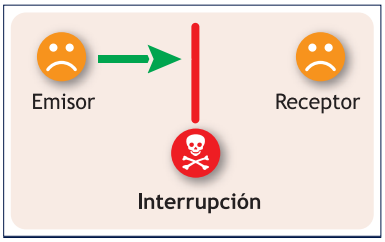
- **Equipo de trabajo.** Se produce una violación de la confidencialidad cuando un atacante consigue acceso a un equipo sin autorización, controlando sus recursos. Un ejemplo sería la obtención de las claves de acceso. Otro ejemplo, mucho más simple, se produce cuando un usuario abandona momentáneamente 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.

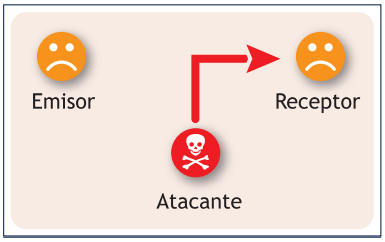


1.4. Violación de la disponibilidad.

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.

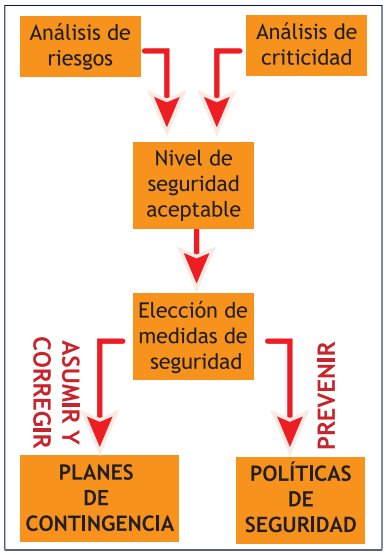
Las medidas de control deben ser efectivas, fáciles de usar, actualizadas periódicamente y, por supuesto, apropiadas a la situación. No hay que olvidar que deben funcionar en el momento adecuado.

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.

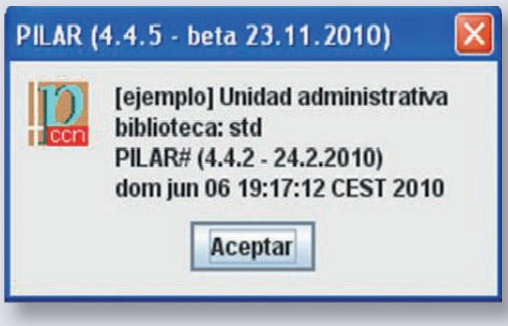
e) Proporciona alguna amenaza más por cada categoría.
f) ¿Qué valoración de las amenazas se da para los activos clasificados como *Equipos?* ¿Y para la *Sala de Equipos?*

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.

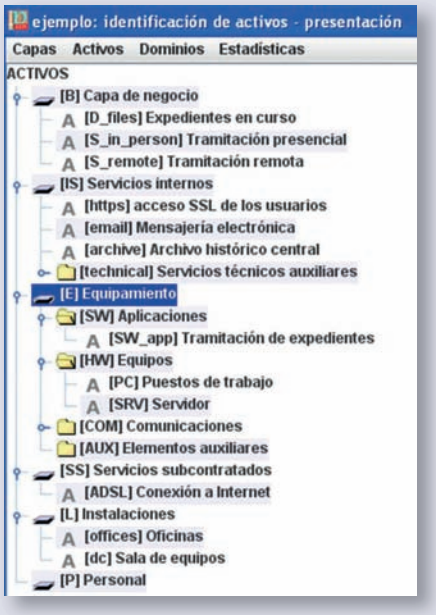
Si tu equipo cumple con los requisitos, descarga la aplicación desde la página https://www.ccn-cert.cni.es/ haciendo clic en *Herramientas / EAR / Pilar.*



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

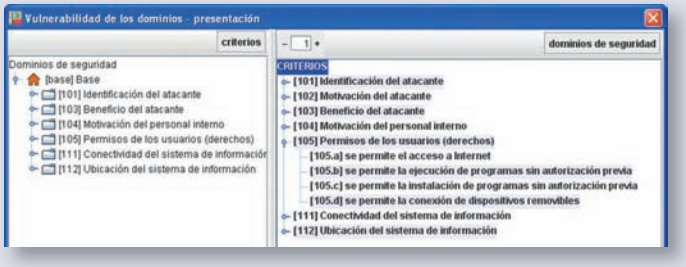
a) Como puedes ver en la imagen, la empresa que se estudia en el ejemplo es una unidad administrativa consistente en una biblioteca.

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

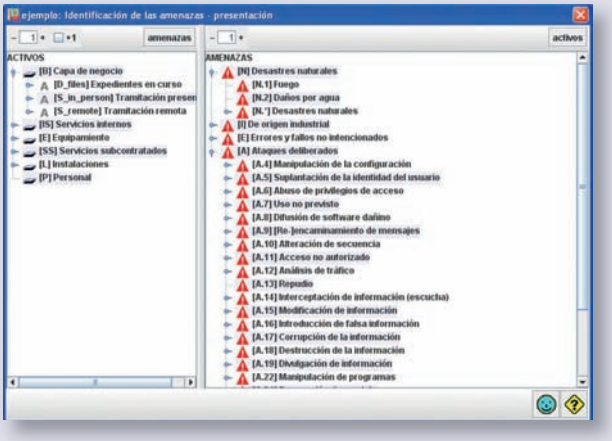


Estos activos utilizan la siguiente aplicación: *[SW_app] Tratamiento de Expedientes*

c) Se muestran las siguientes vulnerabilidades de los dominios:



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



2

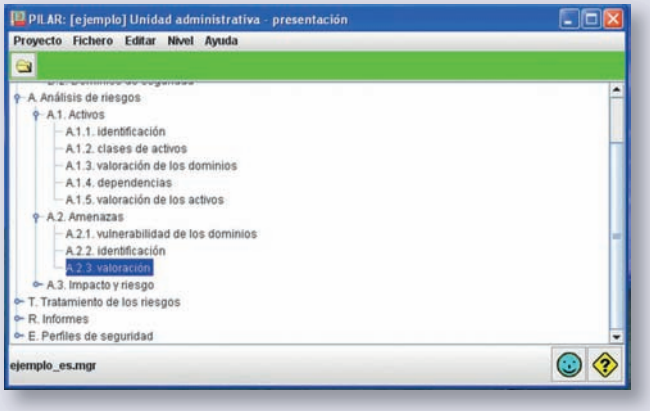
Como también se puede ver en la imagen, la categorización de las amenazas indicadas es la siguiente:

- 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*

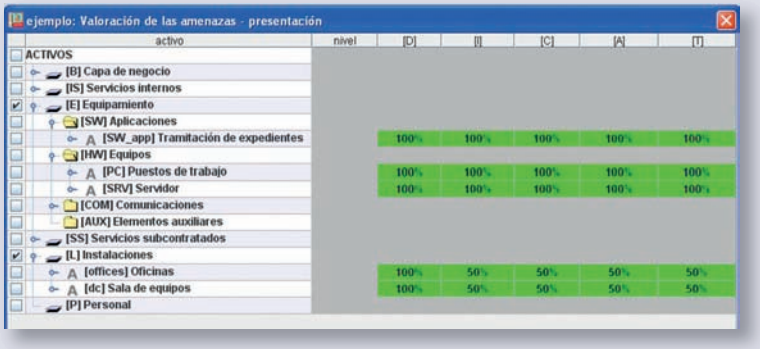
e) Además de las expuestas, se podrían incluir algunas amenazas más en las distintas categorías:

- 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.

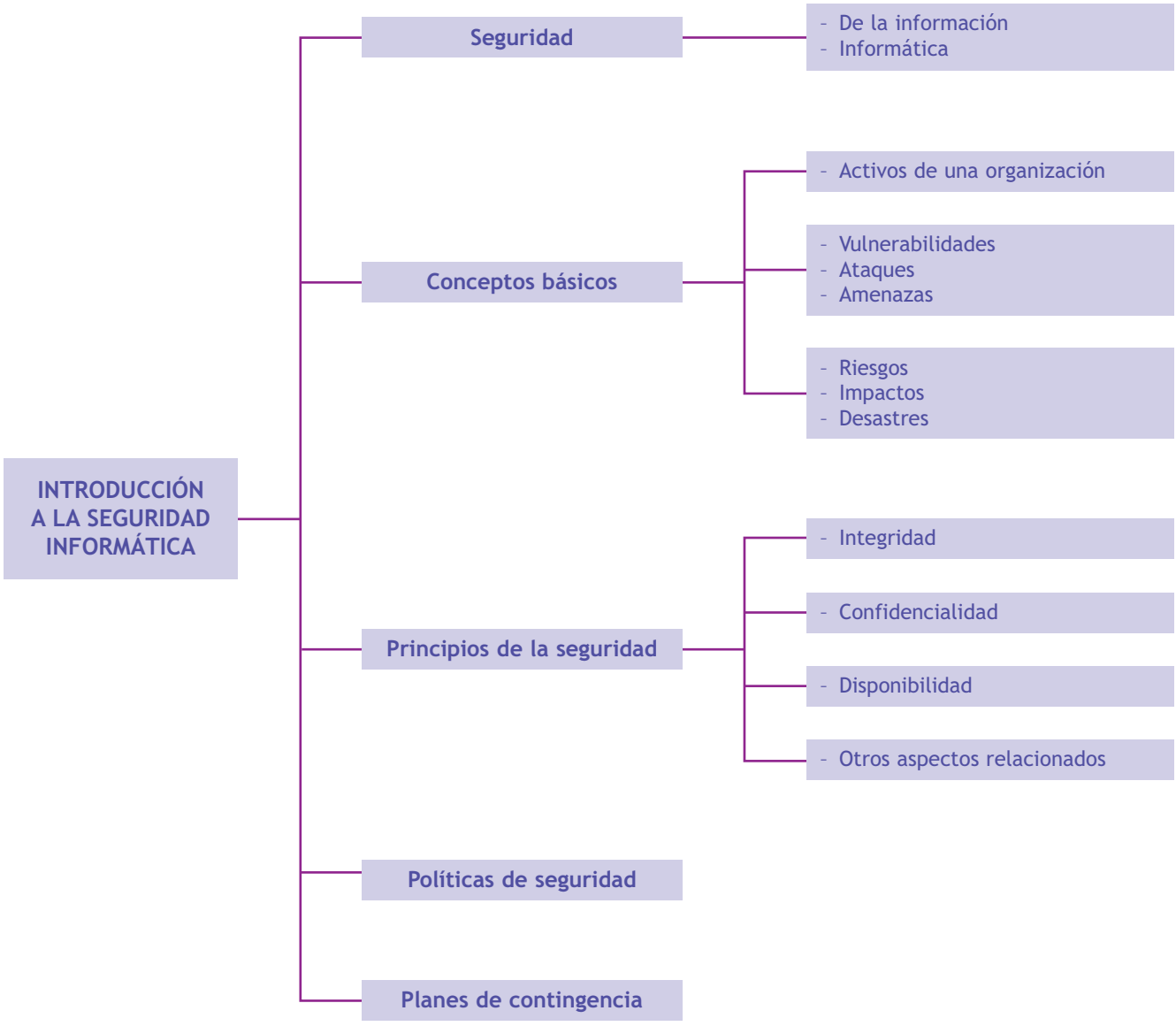
f) Para acceder a la valoración de las amenazas, en el árbol de categorías, debes desplegar la opción *Análisis de riesgos* / *Amenazas* / *valoración*.



- 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

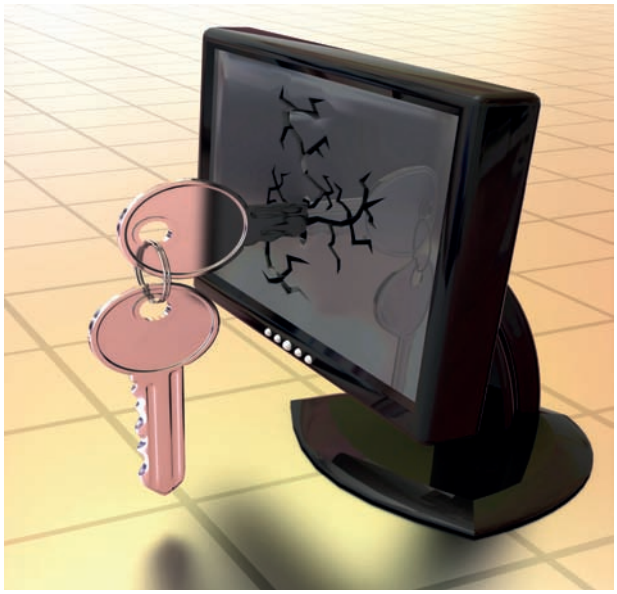


Exceso de confianza de las pymes frente a los ciberataques

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?

u n i d a d 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?

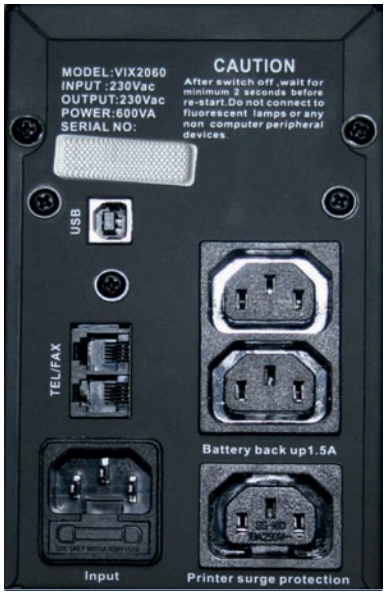
Solución •• El consumo total del equipo será de 270 W (200 + 50 + 10 + 10).

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

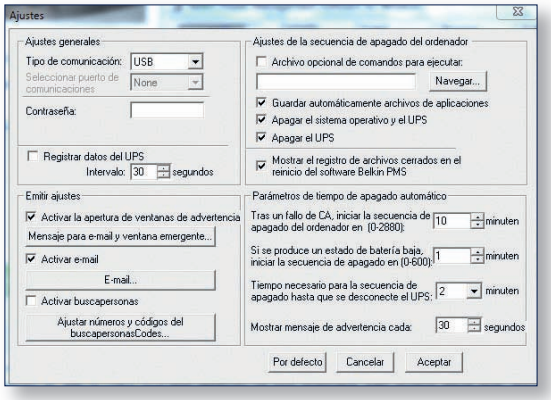
El primer paso será conectar el SAI al PC. Podemos hacer esto bien a través del puerto serie o a través del puerto USB. Nos aseguraremos de que, en función de la conexión elegida, el selector de la conexión RS-232 o USB esté en la posición correcta, pues no podemos usar ambas opciones a la vez. A continuación,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

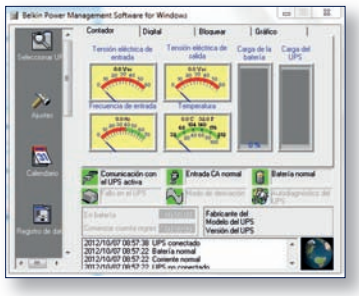
Configuración del SAI



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.

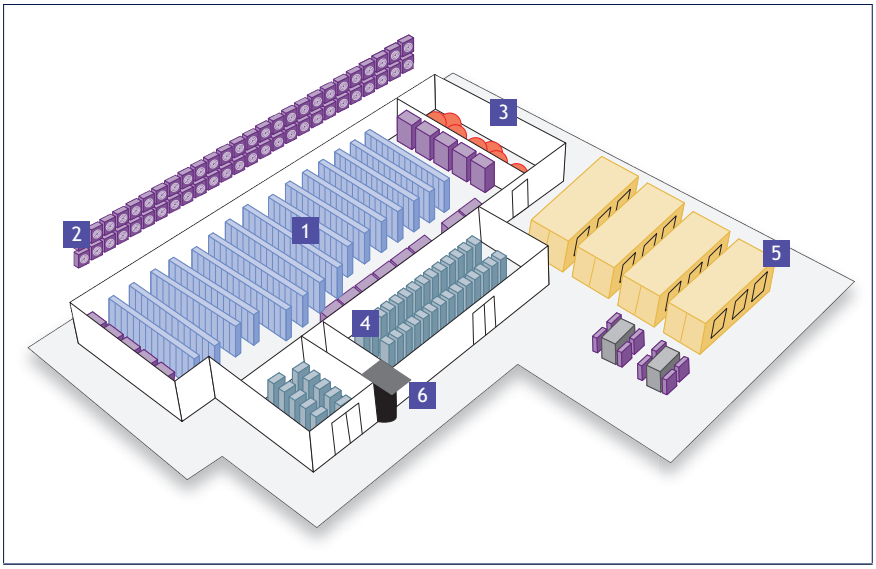
3 >> Centros de proceso de datos

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.

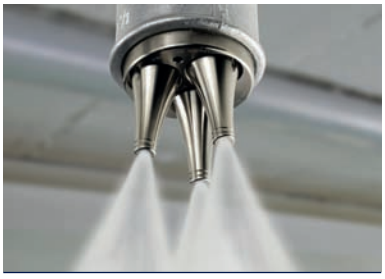
3.2 > Sistemas de seguridad del CPD

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

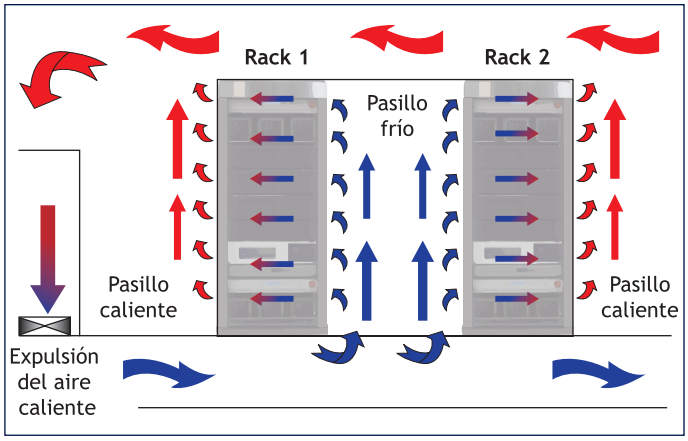
Más de la mitad del consumo de energía de un CPD procede de los sistemas de refrigeración, la iluminación y otros equipos auxiliares, por lo que la elección del sistema de climatización es algo muy importante, así como la óptima configuración del mismo (una excesiva refrigeración supondría un gasto innecesario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

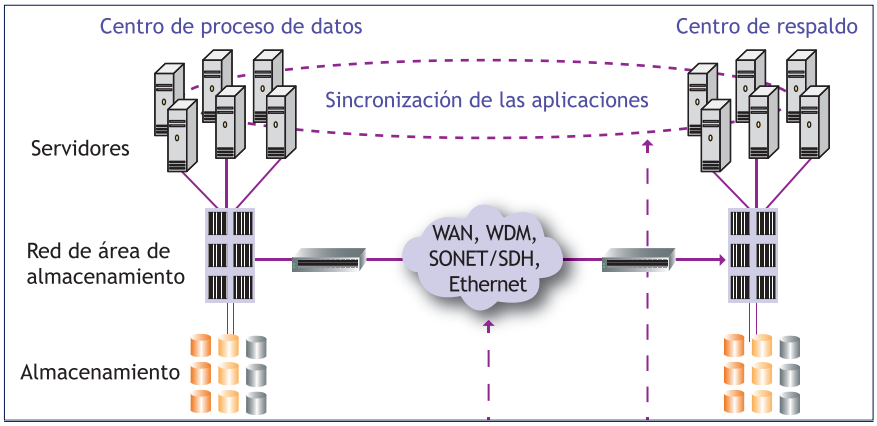
Esto hace, que, de forma adicional a todas las medidas expuestas, muchas empresas mantengan o contraten **centros** o **salas de respaldo** (en inglés DRS, *Disaster Recovery Sites*), que son réplicas, más o menos exactas, del CPD principal, diseñadas para que, en caso de fallo de este, puedan tomar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

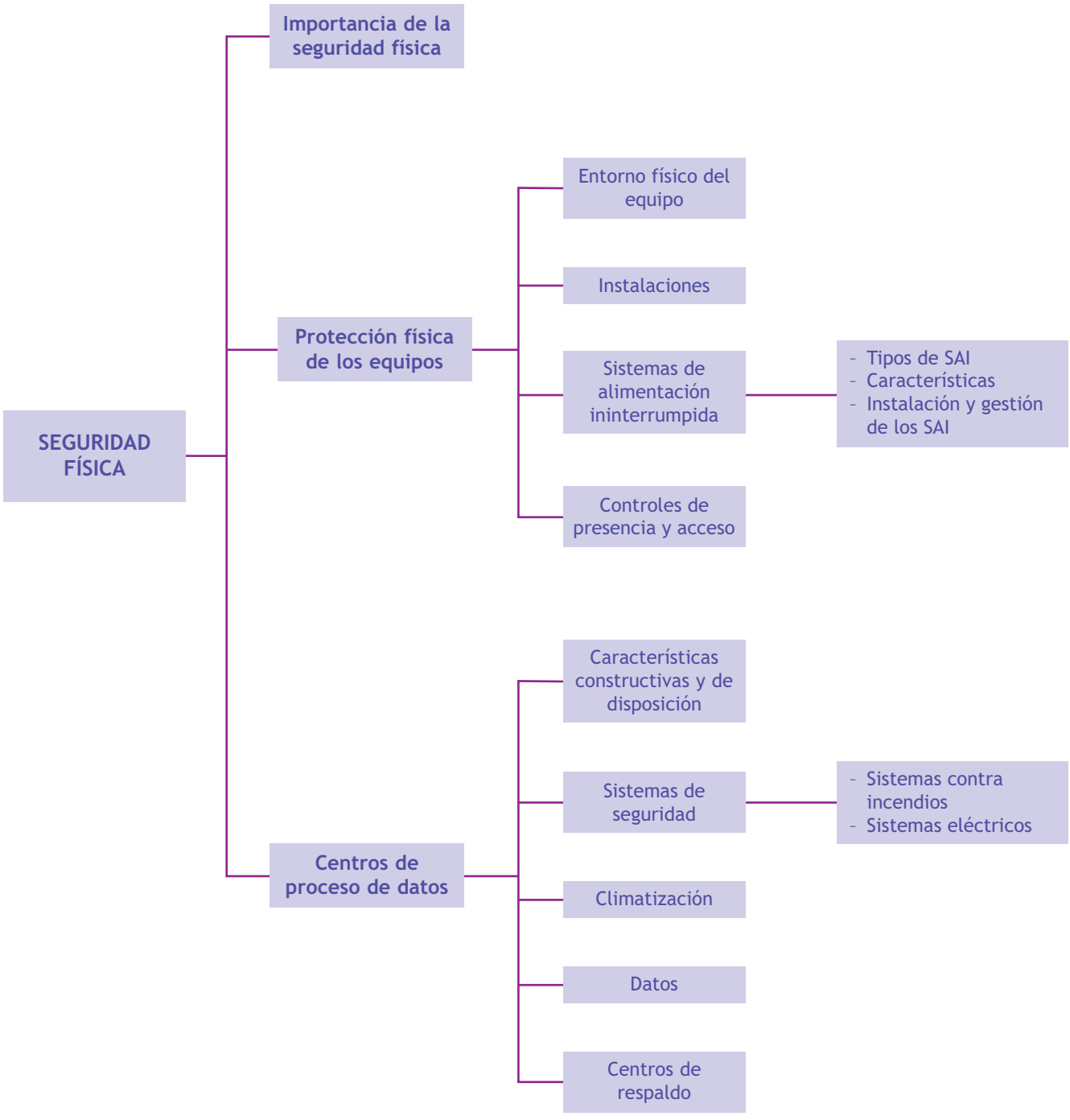
- La información de la empresa está distribuida entre varios servidores que realizan las mismas funciones.
- Las copias se seguridad se realizan de cuando en cuando y no se lleva a cabo copia de toda la información, sino solo de aquella que es considerada importante en el momento de realizar la copia.
- 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.

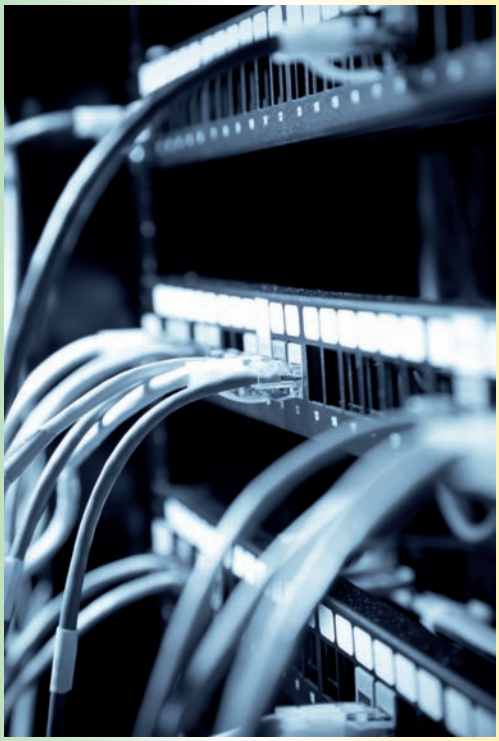
Solución ••

- 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



¿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

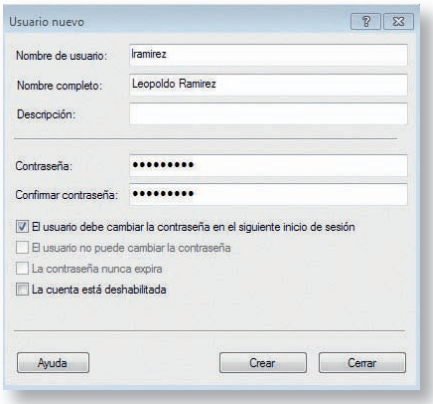
Administración de políticas de contraseñas

•• 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.

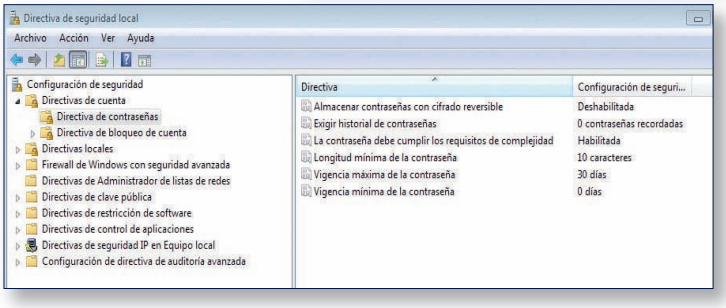
Solución •• Para establecer las contraseñas y poder gestionarlas adecuadamente, en primer lugar se debe crear una cuenta para cada usuario, a la que se podrán atribuir ciertos derechos y privilegios.



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*

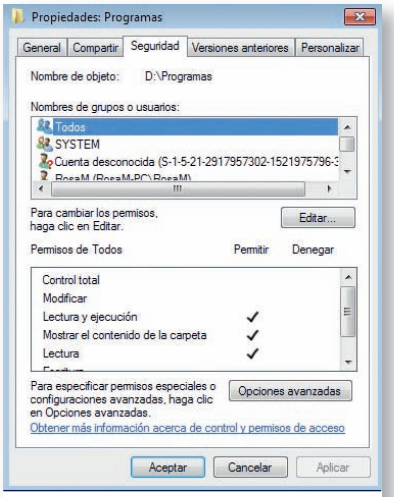
En los *routers* se pueden establecer listas de control de acceso de las siguientes formas:

- **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.

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.

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.

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.**

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.

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:

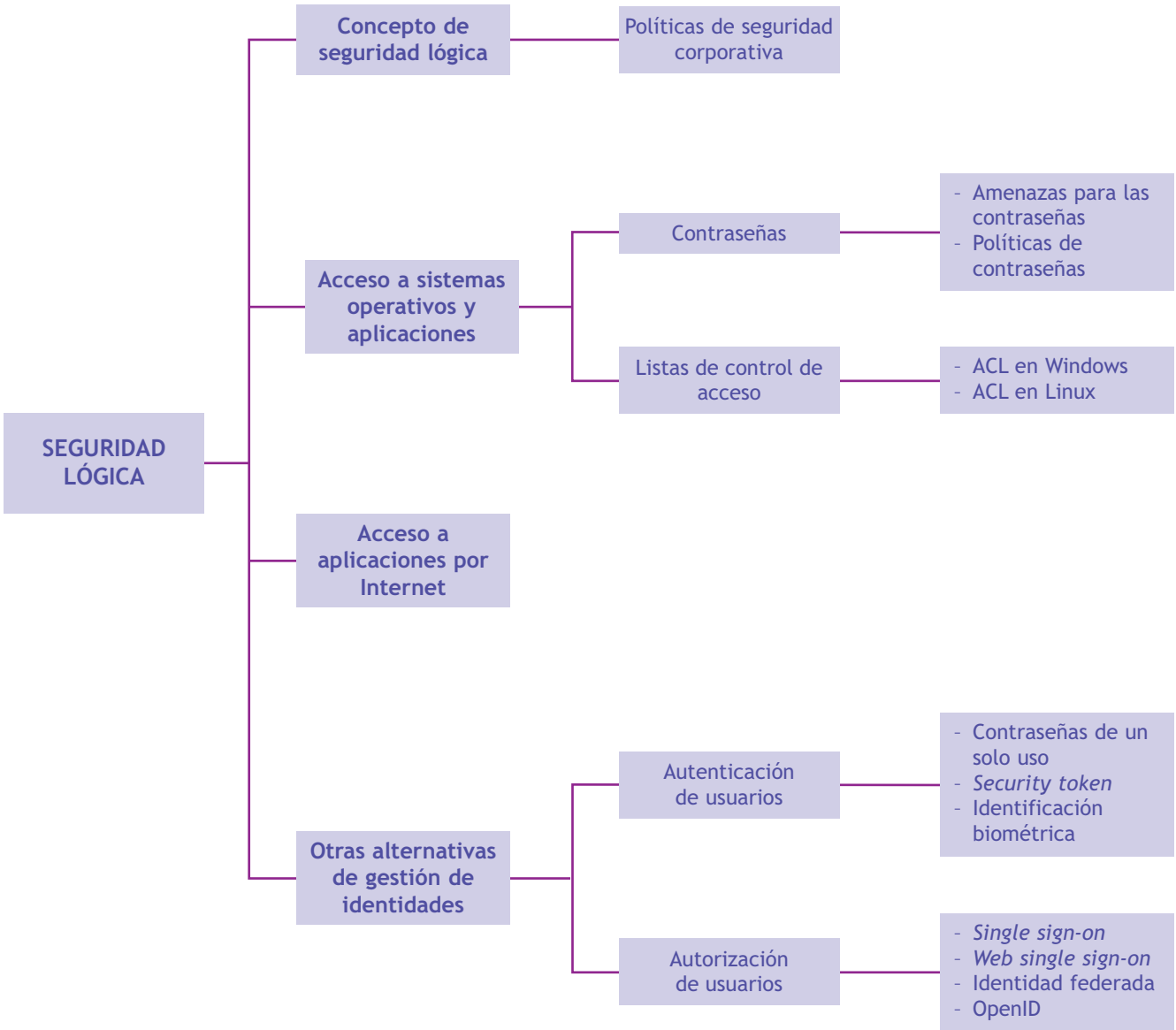
```
#chmod a+r mypasswd
```

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



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?