

Unidad 1. Conceptos básicos de la seguridad informática

1. Seguridad informática ¿por qué?

El espectacular auge de Internet y de los servicios telemáticos ha hecho que los ordenadores y la red de se conviertan en un elemento cotidiano en nuestras casas y en un instrumento imprescindible la tarea de las empresas.

Ya lo tenemos necesidad de ir al banco para conocer los movimientos realizados en nuestra cuenta bancaria, ni para realizar transferencias... Directamente podemos realizar dichas operaciones desde el ordenador de casa. Lo mismo ocurre con la empresa; sea cual sea su tamaño, disponen de equipos conectados a Internet que les ayudan en sus procesos productivos.

Cualquier fallo en los mismos puede suponer una gran pérdida económica ocasionada por el parón producido, bien por la pérdida de información o por el mal funcionamiento de los equipos informáticos, de modo que es muy importante asegurar un correcto funcionamiento de los sistemas y redes informáticas.

Uno de los principales problemas lo que se enfrenta la seguridad informática en la creencia de muchos usuarios de que a ellos nunca le va a pasar lo que otros. Es impensable que nos vayamos de casa nos dejemos la puerta abierta; lo mismo ocurre con la seguridad de la información.

Con una buena política de seguridad, tanto física como y lógica, conseguiremos que nuestro sistema sea menos vulnerable a las distintas amenazas. Sí, menos vulnerables: Nadie puede asegurar que un sistema sea cien por cien seguro, hasta la seguridad de la NASA y del Pentágono han sido violadas por hackers. Hay una lucha permanente entre los técnicos protectores del sistema y los que buscan rendimiento económico fácil, o simplemente su minuto de gloria al superar el reto de asomarse al otro lado de la barrera de protección.

Tenemos que intentar lograr un nivel de seguridad razonable y estar preparados para que, cuando se produzcan los ataques, los daños puedan ser evitados en unos porcentajes que se aproximen al ciento por cien o en caso contrario haber sido lo suficientemente precavidos para realizar la copia de seguridad y de esta manera volver a poner en funcionamiento los sistemas en el menor tiempo posible.

Gene Spafford, experto en seguridad informática, afirma: “el único sistema verdaderamente seguro en aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Induso entonces yo no apostaría mi vida por ello”.

Ejercicio 1

¿Qué problemas pueden surgir cuando se introduce un virus que formatea equipos en una empresa que vende productos por internet?

Ejercicio 2

¿Qué problemas puede ocasionar un internauta que se conecta a internet utilizando nuestro router wi-fi, el cual no tiene ningún tipo de contraseña?

Ejercicio 3

Busca la definición de los términos Hacker y Cracker. ¿Cuál es la diferencia entre ellos?

Ejercicio 4 (entregable a través de Moodle)

Se debe documentar el ejercicio mediante comentarios y capturas de pantalla.

Vamos a hacer un ejercicio en el que averiguaremos la contraseña de un usuario de un servidor de ftp. Para ello usaremos el software *Brutus*, cuyo cometido es precisamente este, averiguar usuarios y contraseñas de servidores web, ftp, etc.

1.- En primer lugar, vamos a instalar el servidor ftp Filezilla Server y un cliente ftp Filezilla. Vamos a crear un usuario llamado *alumno* con password 123. El directorio por defecto de este usuario puede ser la carpeta Mis Documentos, por ejemplo.

2.- Vamos a tratar de averiguar la contraseña del usuario *alumno* empleando el método denominado de fuerza bruta ¿Cuánto tarda el programa en averiguarla?

3.- A continuación, cambiaremos la contraseña del usuario para que sea 1234. Volvemos a repetir el proceso para encontrar la contraseña por el método de la fuerza bruta. ¿Cuánto ha tardado el programa en averiguarla ahora?

4.- A continuación, añade al diccionario una contraseña, por ejemplo *juande*, y ponle esa contraseña al usuario *alumno* del ftp. Prueba ahora a encontrar la contraseña por el método del diccionario. ¿Cuánto ha tardado el programa ahora?

2. Objetivos de la seguridad informática

Si estudiamos las múltiples definiciones que de seguridad informática dan las distintas entidades, deduciremos los objetivos de la seguridad informática.

Según la ISO 27002, "La seguridad de la información se puede caracterizar por la preservación de:

- **Confidencialidad:** asegura que el acceso a información está adecuadamente autorizado
- **Integridad:** salvaguarda la precisión y completitud de la información y sus métodos de proceso
- **Disponibilidad:** asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan".

Otra definición podría ser la siguiente: "Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican".

De estas definiciones podemos deducir que los principales objetivos de la seguridad informática son:

- **Confidencialidad:** consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o emitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas éstas no podrían acceder a la información o a su interpretación.
- **Disponibilidad:** la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento.
- **Integridad:** capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información de que disponemos es válida y consistente.

- **No repudio:** garantizar la participación de las partes en una comunicación. En toda comunicación existe una emisora y un receptor por lo que podemos distinguir dos tipos de no repudio: no repudio en origen y no repudio en destino.

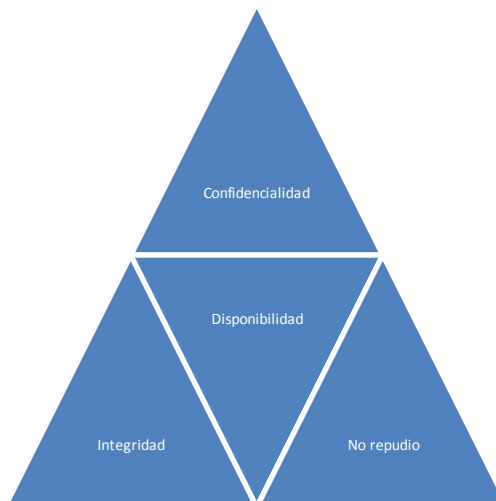


Figura 1.1. Esquema de los objetivos de la seguridad informática

Para conseguir los objetivos mostrados en la figura 1.1 se utilizan los siguientes mecanismos:

- **Autenticación:** permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.
- **Autorización:** controla el acceso de los usuarios a zonas restringidas.
- **Auditoría:** verificar el correcto funcionamiento de las políticas o medidas de seguridad.
- **Encriptación:** ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin algoritmo y clave de cifrado, puede acceder a los datos que se quieren proteger.
- **Realización de copia de seguridad e imágenes de respaldo.**
- **Antivirus:** programa que permite estar protegido contra las amenazas de los virus.
- **Cortafuegos:** programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.
- **Servidores proxy:** consiste en ordenadores con software especial que hacen de intermediarios entre la red interna de una empresa y una red externa, como puede ser Internet. Estos servidores, entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios como el de ftp o el web. Además, suelen disponer de un caché de las páginas más visitadas, con lo que se aumenta la velocidad de acceso.
- **Utilización de firma electrónica o certificado digital,** son mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos. También se utiliza mucho hoy día para establecer comunicaciones seguras entre el pc del usuario y los servidores de internet como las páginas web de los bancos.
- **Conjunto de leyes encaminadas a la protección de datos personales** que obligan a las empresas a asegurar su confidencialidad.

Ejercicio 5

Asocia los mecanismos con los objetivos de la seguridad informática.

3. Clasificación de la seguridad

Se pueden hacer diversas clasificaciones de la seguridad informática en función de distintos criterios.

Según el activo proteger, es decir, tuvo los recursos del sistema de información necesario para el correcto funcionamiento de la actividad de la empresa, distinguir hemos entre seguridad física y lógica. En dependencia del momento preciso de actuación, entre seguridad pasiva y activa, según sea tuve antes de producirse el percance de tal manera que se evite los daños en el sistema, o después del percance minimizando los efectos ocasionados por el mismo.

3.1. Seguridad física y lógica

En este apartado distinguiremos los distintos tipos de seguridad en función del recurso a proteger.

Seguridad física

En aquella que trata de proteger el hardware (y el software que *contiene...*) de los posibles desastres naturales, de incendios, inundaciones, sobrecarga eléctrica a las, robos, etcétera.

A continuación vamos a enumerar las principales amenazas y los mecanismos para salvaguardarnos de las mismas:

Amenazas	Mecanismo de defensa
Incendios	El mobiliario del centro de cálculo debe ser ignífugo. Evitar la localización del centro de procesamiento de datos cerca de zonas donde se manejen o almacenen sustancias inflamables o explosivos. Deben existir sistemas antiincendios, detectores de humo, rociadores de gas, extintores... para sofocar el incendio en el menor tiempo posible y así evitar que se propague ocasionando numerosas pérdidas materiales.
Inundaciones	Evitar la ubicación de los centros de cálculo en la planta baja del edificio para protegerse de la entrada de agua superficial. Impermeabilizar las paredes y techos del CPD. Sellar las puertas para evitar la entrada de agua proveniente de las plantas superiores.
Robos	Proteger los centros de cálculo mediante puertas con medidas biométricas, cámaras de seguridad, vigilantes... Con todas estas medidas pretendemos evitar la entrada de personal no autorizado.
Señales electromagnéticas	Evitar la ubicación de los centros de cálculo próximos a lugares con gran radiación de señales electromagnéticas, pues pueden interferir en el correcto funcionamiento de los equipos informáticos y del cableado de red En caso de no poder evitar la ubicación en zonas con grande emisiones de este tipo

	de señales deberemos proteger el centro frente a dicha emisión de mediante el uso de filtros o de cableado especial, o si es posible, utilizar fibra óptica, que no es sensible a este tipo de interferencias.
Apagones	Para evitar los apagones colocaremos sistemas de alimentación de ininterrumpida, SAI, que proporcionan corriente eléctrica durante un periodo de tiempo suficiente para realizar un apagado controlado.
Sobrecargas eléctricas	Los SAI incorporan filtros para evitar picos de tensión.
Desastres naturales	Estando en continuo contacto con el instituto geográfico nacional y la agencia estatal de meteorología, organismos que informan sobre los movimientos sísmicos y meteorológicos de España.

Seguridad lógica

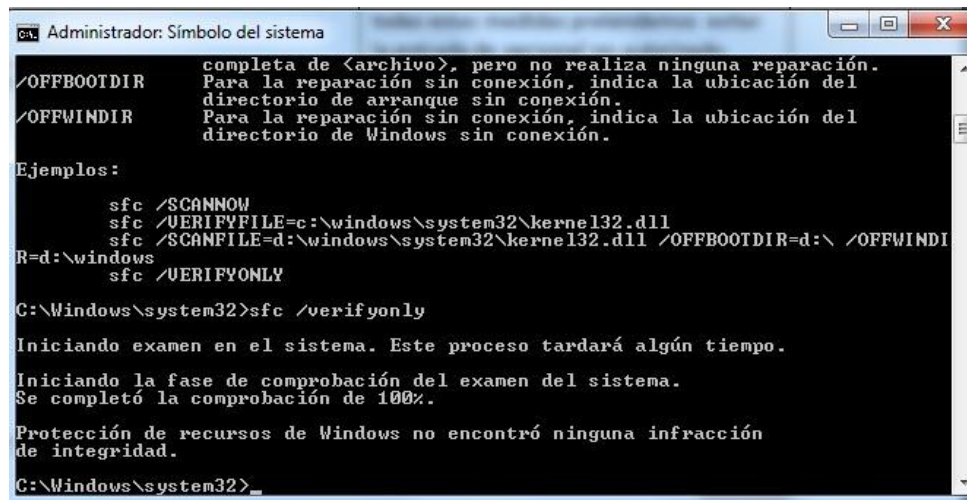
La seguridad lógica complementa la seguridad física, protegiendo el software de los equipos informáticos, es decir las aplicaciones y los datos de usuarios, de robos, de pérdida de datos, entrada de virus informáticos, modificación en autorizada de los datos, ataque desde la red, etcétera.

Amenazas	Mecanismos de defensa
Robos	Cifrar la información almacenada los soportes para que en caso de robo no sea legible. Utilizar contraseñas para evitar el acceso de información. Sistema biométricos.
Pérdida de información	Realizar copias de seguridad para poder restaurar la información perdida. Uso de sistemas tolerante a fallos. Uso de conjunto de disco redundantes.
Perdida de integridad de la información	Uso de programas de chequeos del equipo Firma digital para el envío de información a través de mensajes enviados por la red. Herramientas de sistema operativo para verificar la integridad de la información (SFC en Windows, FSCK el Linux)
Entrada de virus	Uso de antivirus.
Ataques desde la red	Firewall, auditando y autorizando las conexiones permitidas. Programa de monitorización. Servidores proxy.
Modificaciones no autorizadas	Uso de contraseñas. Uso de listas de control de acceso. Cifrado de documentos.

Ejemplo de herramienta de verificación de integridad

Verificación de la integridad de los ficheros del sistema en Windows y Linux.

Con privilegios de administración, ejecutamos el comando SFC con la opción /verifyonly para verificar la integridad de los archivos del sistema de Windows.



```

C:\Windows\system32> /OFFBOOTDIR completa de <archivo>, pero no realiza ninguna reparación.
Para la reparación sin conexión, indica la ubicación del
directorio de arranque sin conexión.
/OFFWINDIR Para la reparación sin conexión, indica la ubicación del
directorio de Windows sin conexión.

Ejemplos:

sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\
C:\Windows\system32>sfc /verifyonly

Iniciando examen en el sistema. Este proceso tardará algún tiempo.
Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 100%.

Protección de recursos de Windows no encontró ninguna infracción
de integridad.
C:\Windows\system32>
  
```

Figura . Ejecución del comando sfc en Windows 7

En Linux, para verificar la integridad de una partición, hay que desmontarla y posteriormente chequearla con el comando fsck.

Por ejemplo, si queremos comprobar la integridad de disco sda2, hemos de hacer:

```

sudo umount dev/sda2
sudo fsck -cfy dev/sda2
  
```

Si queremos comprobar la integridad del sistema, que estará montado en /, hemos de arrancar un Linux en modo Live, y desde ahí desmontar la partición donde tenemos el sistema y proceder al chequeo.

Ejercicio 6

(entregable a través de Moodle)

Se debe documentar el ejercicio mediante comentarios y capturas de pantalla.

Verifica la integridad del sistema en Windows XP y de una partición cualquiera en Linux.

3.2. Seguridad activa y pasiva

Como se comentó al inicio del apartado 3, aquí el criterio de clasificación es el momento en que se ponen en marchas las medidas oportunas.

Seguridad activa

La podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

A continuación, vamos a enumerar las principales técnicas de seguridad activa:

<i>Técnicas</i>	<i>¿Qué previene?</i>
Uso de contraseñas	Previene el acceso a recursos por parte de personas no autorizadas.
Listas de control de acceso	Previene el acceso a los ficheros por parte de personal no autorizado.
Encriptación	Evita que personas sin autorización puedan interpretar la información.
Uso de software de seguridad	Previene de virus informáticos y de entradas indeseadas al sistema informático.
Firmas y certificados digitales	Permite comprobar la procedencia, autenticidad e integridad de los mensajes.
Sistemas de ficheros con tolerancia a fallos	Previene fallos de integridad en caso de apagones, o fallos de sincronización o comunicación.

Seguridad pasiva

La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

A continuación enumeramos las técnicas más importantes de seguridad pasiva:

<i>Técnicas</i>	<i>¿Cómo minimiza?</i>
Conjunto de discos redundantes (RAID)	Podemos restaurar información que no es válida ni consistente.
SAI	Si la corriente se pierde, las baterías del SAI proporcionan la potencia necesaria durante un periodo de tiempo que debe ser suficiente para realizar apagados controlados y evitar fallos de inconsistencia e integridad de los datos.
Realización de copias de seguridad	A partir de las copias realizadas, podemos restaurar la información en caso de pérdida de ésta.

4. Amenazas y fraudes en los sistemas de información

Durante los primeros meses de 2009, en España hemos vivido una época de crisis financiera, lo que ocasionó numerosos despidos en las empresas. La situación produjo un aumento en los casos de robos de información confidencial por parte de algunos de los empleados despedidos, y puso en evidencia la falta de seguridad informática de dichas empresas.

El objetivo final de la seguridad es proteger lo que la empresa posee. Todo aquello que es propiedad de la empresa se denomina **activo**. Un activo puede ser tanto el mobiliario de la oficina, como los equipos informáticos, como los datos que manejan (datos de clientes, facturas, personal...). Cualquier **daño** que se produzca sobre estos activos tendrá un **impacto** en la empresa. Una **vulnerabilidad** es cualquier problema que compromete la seguridad.

4.1. Actuaciones para mejorar la seguridad

Los pasos a seguir para mejorar la seguridad son los siguientes:

- Identificar los activos, es decir, los elementos que la empresa quiere proteger.
- Formación de los trabajadores de las empresas en cuanto a materias de seguridad.
- Concienciación de la importancia de la seguridad informática para los trabajadores de la empresa.
- Evaluar los riesgos, considerando el impacto que pueden tener los daños que se produzcan sobre los activos y las vulnerabilidades del sistema.
- Diseñar un plan de actuación, que debe incluir:
 - Las medidas que traten de minimizar el impacto de los daños ya producidos. Es lo que hemos estudiado respecto a la seguridad pasiva.
 - Las medidas que traten de prevenir los daños minimizando la existencia de vulnerabilidades. Se trata de la seguridad activa.
- Revisar periódicamente las medidas de seguridad adoptadas.

Ejercicio 7 (entregable en Moodle)

- Especificar los activos, daños e impacto que sufre una empresa denominada SiTour (agencia de viajes) que almacena los datos de los clientes únicamente en un portátil que utiliza el director.
- Analiza si aumenta o disminuye el riesgo en caso de que daño sufrido por SiTour sea, además de la pérdida de datos de los clientes, la pérdida de facturas y datos de proveedores. Identifica activos, daños, impactos y vulnerabilidades.
- Analiza si aumenta o disminuye el riesgo en caso de que se instale un cortafuegos y se mantenga un antivirus actualizado en el portátil del director de SiTour.

Ejercicio 8 (entregable en Moodle)

- Supón que en el ordenador portátil con cámara web integrada que tienes en tu habitación, no tiene cortafuegos activo, no hay instalado un antivirus y lo tienes siempre conectado a Internet. Un desconocido toma el control del portátil y te das cuenta porque te encuentras la cámara web encendida y tú no la has conectado. Analiza activos, vulnerabilidades y riesgos, y detalla cuales podrían ser los daños producidos y el impacto de los mismos.
- Imagina ahora que la persona que ha tomado el control de tu ordenador no hace nada en tu ordenador y tú no te das cuenta de esta situación. Un día dejas conectado tu DNI electrónico en el lector del ordenador. Analiza los posibles riesgos y el impacto de los mismos.

4.2 Vulnerabilidades

Las vulnerabilidades de un sistema son una puerta abierta para posibles ataques, de ahí que sea tan importante tenerlas en cuenta; en cualquier momento podrían ser aprovechadas.

Lograr que los sistemas y redes operen con seguridad resulta primordial para cualquier empresa y organismo. Esto ha llevado a que empresas como Microsoft dispongan de departamentos dedicados exclusivamente a la seguridad, como es Microsoft Security Response Center (MSRC). Sus funciones son, entre otras, evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, y preparar y divulgar revisiones y boletines de seguridad que respondan a estos informes.

Para ellos, se clasifican las vulnerabilidades en función de su gravedad, lo que nos da una idea de los efectos que pueden tener en los sistemas. En la siguiente tabla se puede ver dicha clasificación:

Clasificación	Definición
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

En el siguiente enlace puedes ver un ejemplo de boletín de seguridad emitido por Microsoft sobre una vulnerabilidad encontrada en Microsoft Word

<http://technet.microsoft.com/es-es/security/bulletin/ms09-027>

Ejercicio 9 (Entregable en Moodle, por parejas)

Busca una de las últimas vulnerabilidades publicadas por Microsoft que afecte a uno de sus sistemas operativos. La vulnerabilidad la puedes buscar en la siguiente dirección:

<http://technet.microsoft.com/es-es/security/bulletin/>

Realiza un informe con los siguientes puntos:

- Descripción de la vulnerabilidad.
- A qué software afecta.
- Qué clasificación le ha dado Microsoft.
- Qué impacto podría tener, si bajo tu punto de vista afecta a los sistemas que tenemos en clase.
- Qué medidas tenemos que tomar para corregir esta vulnerabilidad.

4.3. Tipos de amenazas

En este apartado veremos una pequeña introducción a las clasificaciones más importantes, y trataremos este tema con más detalle en la Unidad 5: Seguridad activa en el sistema.

Para identificar las amenazas a las que está expuesto un sistema informático realizaremos tres clasificaciones: la primera de los tipos de atacantes, la segunda de los tipos de ataques que puede sufrir y la tercera de cómo actúan esos ataques.

En la siguiente tabla se recoge la definición de las personas que llevan a cabo los ataques:

Nombre	Definición
Hackers	Expertos informáticos con una gran curiosidad por descubrir las vulnerabilidades de los sistemas pero sin motivación económica o dañina.
Crackers	Un hacker que, cuando rompe la seguridad de un sistema, lo hace con intención maliciosa, bien para dañarlo o para obtener un beneficio económico.
Phreakers	Crackers telefónicos, que sabotean las redes de telefonía para conseguir llamadas gratuitas.
Sniffers	Expertos en redes que analizan el tráfico para obtener información extrayéndola de los paquetes que se transmiten por la red.
Lammers	Chicos jóvenes sin grandes conocimientos de informática pero que

	se consideran a sí mismos hackers y se vanaglorian de ello.
Newbie	Hacker novato.
Ciberterrorista	Expertos en informática e intrusiones en la red que trabajan para países y organizaciones como espías y sabotadores informáticos.
Programadores de virus	Expertos en programación, redes y sistemas que crean programas dañinos que producen efectos no deseados en los sistemas o aplicaciones.
Carders	Personas que se dedican al ataque de los sistemas de tarjetas, como los cajeros automáticos.

En la siguiente tabla se recogen los principales ataques que puede sufrir un sistema si se aprovechan sus vulnerabilidades.

Ataque	Definición
Interrupción	Un recurso del sistema o la red deja de estar disponible debido a un ataque
Intercepción	Un intruso accede a la información de nuestro equipo o a la que enviamos por la red.
Modificación	La información ha sido modificada sin autorización, por lo que puede no ser válida.
Fabricación	Se crea un producto (por ejemplo una página Web) difícil de distinguir del auténtico y que puede utilizarse para hacerse, por ejemplo, con información confidencial del usuario.

Los tipos de amenazas pueden clasificarse también en función de cómo actúan los ataques, siendo los principales los que se han incluido en la tabla que aparece a continuación:

Ataque	¿Cómo actúa?
Spoofing	Suplanta la identidad de un PC o algún dato del mismo (como su dirección MAC).
Sniffing	Monitoriza y analiza el tráfico de la red para hacerse con información.
Conexión no autorizada	Se buscan agujeros de seguridad de un equipo o un servidor, y cuando se descubren, se realiza una conexión no autorizada a los mismos.
Malware	Se introducen programas malintencionados (virus, troyanos, gusanos, etc...) en nuestro equipo, dañando el sistema de múltiples formas.
Keyloggers	Se utiliza una herramienta que permite conocer todo lo que el usuario escribe a través del teclado, e incluso se pueden realizar capturas de pantalla.
Denegación de Servicio (DoS)	Interrumpe el servicio que se está ofreciendo en servidores o redes de ordenadores.
Ingeniería social	Se obtiene información confidencial de una persona u organismo para utilizarla con fines maliciosos. Un ejemplo es el <i>phishing</i> .
Phishing	Se engaña al usuario para obtener su información confidencial suplantando la identidad de un organismo o página web (por ejemplo, de un banco).

5. Leyes relacionadas con al seguridad de la información

En los siguientes apartados vamos a tratar las principales leyes relacionadas con al seguridad de la información:

- LEY DE PROTECCION DE DATOS DE CARÁCTER PERSONAL
- Ley de servicios de la información y el comercio electrónico.

5.1 Normativa que protege los datos personales

Un muy a menudo, en nuestra vida diaria, nuestros datos personales son solicitados para realizar diversos trámites en empresas o en organismos tanto públicos como privados; por ejemplo, cuando cambiamos de numero de movil o contratamos un nuevo proveedor de servicios de internet. Desde ese instante, nuestro nombre, apellidos, dirección, etc, pasan a formar parte de una serie de ficheros. Su gestión está regulada por la Ley de Protección de Datos de Carácter Personal (Ley Orgánica 15/1999), más conocida como LOPD, que se desarrolla en el Real Decreto 1720/2007, y es supervisada por la Agencia Española de Protección de Datos.

El objetivo de esta ley es garantizar y proteger los derechos fundamentales y, especialmente, la intimidad de las personas físicas en relacion con sus datos personales. Es decir, especifica para qué se pueden usar, cómo debe ser el procedimiento de recogida que se debe aplicar y los derechos que tienen las personas a las que se refieren, entre otros aspectos.

Cuando la LOPD habla de ficheros se refiere no sólo a datos en soporte informático de tipo textual, sino tambien a documentos impresos, videos, grabaciones de audio, etc.

Siempre que se vaya a crear un fichero de datos de carácter personal, es necesario solicitar la aprobación de la Agencia de Protección de Datos.

Cuando se realiza esta solicitud es obligatorio especificar los datos que contendrá el fichero y el nivel de seguridad que se aplicará al fichero. Los niveles de seguridad son tres: básico, medio y alto. Los datos implicados en cada uno de ellos son:

Nivel de Seguridad	Datos del fichero
Básico	Todos los datos de carácter personal tienen que tener como mínimo este nivel.
Medio	Referidos a infracciones administrativas (o penales), a gestión tributaria, datos fiscales o financieros Datos que proporcionan información sobre las características o personalidad de los afectados.
Alto	Referidos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

Ejemplo práctico

La agencia de viajes SiTour ha decidido hacer una ficha a cada cliente que solicite información sobre algún viaje, con el objetivo de enviarle nuevas ofertas y promociones.

Vamos a describir el proceso que un técnico informático debe realizar para poder almacenar y gestionar dichos datos de acuerdo a la normativa vigente.

En primer lugar, según la LOPD se debe solicitar a la Agencia de Protección de Datos la creación de dicho fichero. En esta solicitud habrá que especificar:

- Responsable del fichero: Agencia de viajes SiTour
- Finalidad: El objetivo es comercial, enviar ofertas y promociones.
- Tipo de datos de carácter personal que contiene: Nombre y apellidos, DNI, teléfono, dirección postal y email.
- Medidas de seguridad: nivel básico, según especifica la LOPD.

Los datos que se deseen almacenar en el fichero tendrán que ajustarse a los objetivos, es decir, no se puede solicitar al cliente sus ingresos anuales. Estos datos solo podrán ser utilizados para el objetivo para el que se han recogido y tendrán que ser cancelados una vez que no sean necesarios para este objetivo.

La Agencia de Protección de Datos se pronunciará sobre la solicitud en un plazo de un mes y si no se entenderá que el fichero se ha inscrito correctamente.

En el momento de la recogida de datos de carácter personal, hay que informar al cliente de:

- La incorporación de sus datos a un fichero de datos de carácter personal.
- La finalidad de estos datos, que en este caso es el envío de ofertas y promociones.
- De su derecho de acceso, rectificación y cancelación, así como del procedimiento que el cliente debe seguir, y a donde debe dirigirse para ejercitar dicho derecho.
- De la identidad y dirección del responsable del tratamiento de los datos.

Además, tanto la persona responsable del fichero como quienes intervengan sobre él tienen deber de secreto sobre los datos que contiene.

El documento informativo que se proporcionará a los clientes, de que la empresa guardará una copia firmada por éste, podría ser el siguiente:

En cumplimiento de lo establecido en la ley orgánica 15/1999 de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007, que aprueba su reglamento de desarrollo, los clientes quedan informados y prestan su consentimiento a la incorporación de sus datos a los ficheros existentes en SiTour y al tratamiento de los mismos. Los datos personales serán tratados exclusivamente con la finalidad de informar al cliente sobre nuevas ofertas y promociones. No se realizará ninguna cesión de estos datos.

Según lo dispuesto en la misma ley, los clientes tienen derecho a consultar, modificar o cancelar los datos proporcionados a SiTour, dirigiéndose al departamento de informática de SiTour.

(Entregables en Moodle)

Ejercicio 10

Dadas las siguientes situaciones, identifica el tipo de infracción que SiTour está cometiendo. Para ello consulta el artículo 43 de la LOPD:

- SiTour realiza el envío de ofertas y promociones sin solicitar la creación del fichero de datos de sus clientes.
- SiTour no está realizando copias de seguridad del fichero de datos.
- SiTour realiza la recogida de datos a sus clientes sin informarles de la finalidad del fichero.

Ejercicio 11

Las infracciones de la actividad anterior tienen asignada una sanción económica recogida en el artículo 45 de la LOPD. Búscala e indica cual es en cada caso.

Ejercicio 12

Supón que terminado el ciclo SMR, entras a formar parte del personal del departamento de informática de una empresa de nueva creación. Indica qué pasos deberás realizar, según la LOPD, en los siguientes supuestos:

- La empresa es una empresa en Internet que se va a dedicar a vender productos informáticos. Los datos necesarios de los clientes son nombre, apellidos, correo electrónico, teléfono y dirección postal.
- La empresa es un buffet de abogados. Los datos necesarios son, además de los mencionados en el punto anterior, los siguientes: información sobre antecedentes penales de los clientes.
- La empresa es un partido político. Los datos que es necesario almacenar de los afiliados a dicho partido son, además de los indicados en el primer punto, los siguientes: afiliación sindical.