

2

Seguridad en sistemas informáticos y redes



1. Necesidad de seguridad

Establecer un plan de seguridad

2. Tipos de seguridad

Seguridad activa y pasiva

Seguridad física y seguridad lógica

Seguridad de la persona y de los sistemas de información

Las leyes nos protegen

3. Seguridad en los lenguajes y las aplicaciones.

El hacking ético

Vulnerabilidades. Fortalezas y debilidades

4. Seguridad activa. Técnicas contra el malware.

Sistemas de verificación e identificación

Certificados digitales. La firma electrónica

5. Seguridad pasiva

6. Amenazas y fraudes en las personas

Proteger nuestros datos

Software para proteger a la persona

Hábitos orientados a la protección de la intimidad y de la persona

7. Seguridad en Internet

Las redes sociales y la seguridad

Protocolos seguros

La propiedad intelectual y la distribución del software

Intercambio de archivos: redes P2P

EN LA RED: ENLACES DE INTERÉS

denuncia-online.org

Web con información para los internautas interesados en los delitos en la Red, con recursos para denunciar las situaciones que detecten o sufran directa o indirectamente.

www.agpd.es

Sitio de la Agencia Española de Protección de Datos, con información referente a todos nuestros derechos en cuanto al tratamiento de nuestros datos personales, tanto en Internet como fuera de la Red.

www.gdt.guardiacivil.es

Web del Grupo de Delitos Telemáticos de la Guardia Civil, con información sobre seguridad en la Red y ayuda para hacer denuncias.

www.osi.es

Web de la Oficina de Seguridad del Internauta, con información y soporte para los problemas que puedan surgir en Internet.

1. Necesidad de seguridad

La **seguridad informática** es el conjunto de medidas encaminadas a proteger el hardware, el software, la información y las personas.

La necesidad de seguridad es una constante que ha acompañado a la historia del ordenador. Es necesario asegurar tanto la máquina como la información que contiene, así como garantizar la seguridad de los usuarios. Cualquier fallo puede tener repercusiones graves de tipo económico, social o personal.

Además, en un futuro próximo, la revolución de Internet y su evolución continua conllevarán un cambio radical en la forma de entender los riesgos informáticos. La irrupción del **big data** y el **Internet de las cosas** obligará a elaborar nuevas estrategias de seguridad. Veamos qué significan estos dos conceptos:

- **Big data.** Es la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional. Es útil para hacer pronósticos y diagnósticos que pueden pasar desapercibidos con cantidades de datos más pequeñas y permitirá grandes mejoras en todos los ámbitos de la vida. Sin embargo, los usuarios a menudo facilitan datos personales sin darse cuenta de las implicaciones que ello podrá tener en su privacidad: datos de usuario en las redes sociales, señales de los móviles, pagos con tarjeta...
- **Internet de las cosas.** Es la conexión de objetos de uso cotidiano con Internet para dotarlos de interactividad. Este avance facilitará la interconexión entre personas y objetos y reducirá o eliminará las barreras de distancia y tiempo. Se conectarán a Internet muchas más cosas que personas, pero a la vez se incrementarán notablemente los riesgos informáticos, en comparación con los actuales.

En esta continua evolución, debemos minimizar los riesgos. Si vamos a utilizar el ordenador en una red, tenemos que:

- **Saber utilizarlo** (no usaremos a la ligera herramientas que no conocemos, sobre todo en Internet).
- **Conocer las herramientas de seguridad** de que disponemos (así sabremos si estamos protegidos frente a virus, ciberdelincuentes y páginas de contenido indeseado).
- **Aplicar una serie de normas básicas de seguridad** que rigen nuestra interacción con los otros usuarios de la red.



"Entre el nacimiento del mundo y el año 2003, hubo cinco exabytes de información creada. Actualmente creamos cinco exabytes cada dos días."

Eric Schmidt (Google)

■ Establecer un plan de seguridad

El primer paso para minimizar los riesgos es hacernos las tres preguntas necesarias al establecer un **plan de seguridad**:

1. ¿A quién necesitamos proteger?
2. ¿De qué es necesario protegerlo?
3. ¿Con qué herramientas contamos para ello?



2. Tipos de seguridad

En esta unidad profundizaremos en el conocimiento de los distintos riesgos informáticos; ahora vamos a analizar cómo se clasifican, atendiendo a distintos criterios. Los principales mecanismos de protección para cada uno de ellos se desarrollarán a lo largo de la unidad y se resumen en las figuras 1, 2 y 3.

■ Seguridad activa y seguridad pasiva

De la misma forma que en el coche existen medidas de seguridad activa para **evitar** accidentes (los frenos, el sistema de control de estabilidad o ESP...) y medidas de seguridad pasiva para **minimizar** las consecuencias de un accidente, asumiendo que éstos pueden ocurrir (airbag, cinturón de seguridad...), en la seguridad informática existe una clasificación similar.

Llamamos **seguridad activa** al conjunto de acciones encaminadas a proteger el ordenador y su contenido (por ejemplo, usar contraseñas seguras, tener actualizado un antivirus, etc.). Se trata de reducir las vulnerabilidades todo lo posible.

En la actualidad, las contraseñas no son la forma más segura de trabajar y se están desarrollando otros sistemas más seguros:

- La **biometría**, medidas biológicas que pueden servir para identificar personas, como la huella digital (usada en algunos dispositivos móviles y ordenadores), el reconocimiento facial o la lectura de la retina.
- Los **sistemas de autenticación de doble factor**, que consisten en enviar una segunda contraseña a un dispositivo distinto del que se está usando.

La **seguridad pasiva** es la que pretende minimizar el impacto de un posible daño informático (por ejemplo, realizar copias de seguridad periódicas). Asumiendo que existen vulnerabilidades, es necesario disminuir las consecuencias.

La figura 1 muestra los mecanismos de protección activos y pasivos con los que podemos contar:

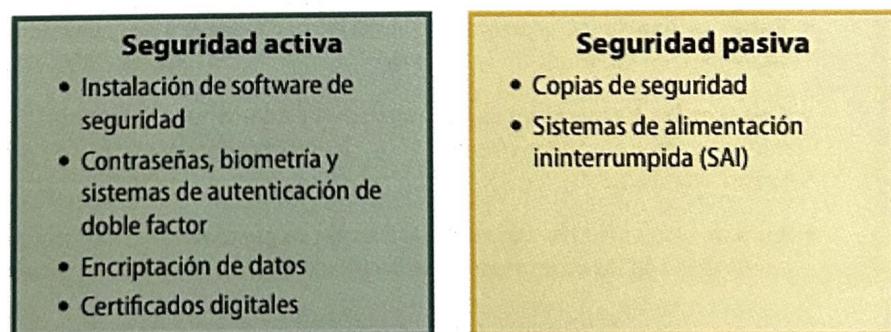


Fig. 1. Mecanismos de protección activos y pasivos

■ Seguridad física y seguridad lógica



La seguridad física cobra especial importancia en los servidores.

La **seguridad física** trata de proteger el hardware ante posibles desastres naturales (como incendios, inundaciones...), robos, sobrecargas eléctricas, etc. Este tipo de seguridad cobra especial importancia en el caso de los servidores de Internet o de una empresa.

La **seguridad lógica** complementa la física y trata de proteger el software y los datos de los usuarios.

La figura 2 muestra los mecanismos de protección físicos y lógicos con los que podemos contar:

Conoce

Seguridad física

- Sistemas antiincendios y antiinundaciones
- Vigilancia para evitar robos
- Sistemas para evitar apagones o sobrecargas eléctricas

Seguridad lógica

- Protección de la información ante robos o pérdidas con las técnicas de seguridad activa y pasiva

Fig. 2. Mecanismos de protección físicos y lógicos

■ Seguridad de la persona y de los sistemas de información

Si tenemos en cuenta el factor humano, podemos clasificar la seguridad de la siguiente forma:

- **Seguridad en los sistemas de información** o amenazas a la máquina: consiste en la protección ante las **amenazas** a nuestro ordenador.
- **Seguridad en la persona**: consiste en la protección ante **amenazas y fraudes** a la persona, que es lo más importante (los daños a la máquina no dejan de ser daños materiales, pero los daños causados a las personas permanecen en el tiempo y trascienden a otros aspectos de la vida).

La figura 3 muestra los mecanismos de protección en las personas y en los sistemas de información:

**Seguridad en la persona**

- Nuestra actitud, la mejor protección
- Estar informados
- Usar el sentido común
- Las leyes nos protegen

Seguridad en los sistemas de información

- Protección de la información ante robos o pérdidas con las técnicas de seguridad activa y pasiva

Fig. 3. Mecanismos de protección en las personas y en los sistemas de información



Cuando usamos Internet, debemos tener presentes nuestra **seguridad** y el **respeto** a los demás.

■ Las leyes nos protegen

Debemos tener presente que, en lo relativo a la seguridad informática, las leyes nos protegen: defienden nuestros derechos fundamentales, especialmente la intimidad de las personas físicas en relación con sus datos personales. Las dos leyes más destacables son:

- **Ley Orgánica 3/2018**, de 5 de diciembre, de **protección de datos personales y garantía de los derechos digitales**. Se menciona, por ejemplo, en todos los carteles que indican zonas videovigiladas.
- **Reglamento (UE) 2016/679** del Parlamento Europeo y del Consejo, relativo a la protección de datos.



3. Seguridad en los lenguajes y las aplicaciones. El hacking ético

Vamos a comenzar por conocer las principales amenazas a nuestro ordenador, es decir, de qué es necesario protegerlo y con qué herramientas contamos para ello.

Se llama **malware** (de *malicious software*), **software malicioso** o **software malintencionado** al software elaborado con fines maliciosos, como virus, troyanos, gusanos, spyware, etc.

Virus

Es un **programa** que se instala en el ordenador sin el permiso del usuario con el objetivo de causar daños. Puede autorreplicarse e **infectar** a otros ordenadores. Para propagarse puede valerse de memorias portátiles, de software y de la propia red Internet. Los virus son la amenaza más conocida y la más importante por su volumen de riesgo.



Keylogger

(De *key* "tecla" y *logger* "registrador".) Es un tipo de software que se encarga de obtener y memorizar las pulsaciones que se realizan en un teclado. Puede utilizarse para espionar de forma remota, con el objetivo de **obtener contraseñas** del usuario.



Spyware o software espía

No todos los programas espía son malintencionados. Se pueden considerar programas spyware con código malicioso los **troyanos**, el **adware**, los **hijackers** y el **ransomware**.

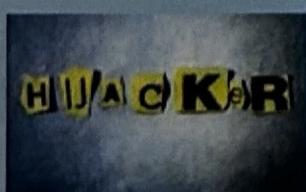


Ransomware

(De *ramson* "rescate" y *software*.) Es un ataque que consiste en restringir el acceso a determinadas partes de un sistema o a un bloque de archivos de la víctima (por ejemplo, cifrándolos) y luego pedir una cantidad de dinero para desinfectarlos o descifrarlos.

Hijackers o secuestradores

Son programas que **"secuestran"** a otros programas para usar sus derechos o para modificar su comportamiento. El caso más habitual es el ataque a un navegador, modificando la página de inicio y redireccionando las páginas de búsqueda sin el consentimiento del usuario.



Gusano

Se trata de un programa malicioso cuya finalidad es **desbordar la memoria** del sistema reproduciéndose a sí mismo.



Adware

(De *advertisement software*.) El **software de publicidad** es publicidad incluida en programas que la muestran después de instalados. Algunos de ellos tienen licencia shareware o freeware e incluyen publicidad para subvencionarse, de forma que si el usuario quiere una versión sin publicidad puede optar por pagar la versión con licencia registrada. El problema viene cuando estos programas actúan como **spyware**, incluyendo código para recoger información personal del usuario (información que no necesariamente tiene por qué usarse de forma maliciosa: a veces se trata de conocer los gustos de los usuarios, pero puede pasar a otras entidades sin su autorización).



Troyano

Es un tipo de virus en el que se han introducido, camufladas en otro programa, instrucciones encaminadas a **destruir** la información almacenada en los discos o bien a **recabar** información. Su nombre hace referencia al caballo de Troya porque estos virus suelen estar alojados en elementos aparentemente inofensivos, como una imagen o un archivo de música, y se instalan en el sistema al abrir el archivo que los contiene.



Hackers

Son expertos informáticos que se dedican a detectar fallos de seguridad en sistemas informáticos. Trabajan en empresas de todo tipo resolviendo vulnerabilidades de los sistemas. También existen empresas de **hacking ético** (o **white hacking**), que ayudan a otras personas y empresas a saber cuál es su nivel de seguridad frente a los hackers maliciosos.

Los hackers maliciosos, también llamados **piratas informáticos** (o **black hackers**), intentan atentar contra la seguridad de sistemas en la Red con fines malintencionados y lucrarse con ello.



Pharming

Es una práctica consistente en redirigir un nombre de dominio a otra máquina distinta, de forma que un usuario que introduzca una URL acceda a la página web del atacante. De este modo, por ejemplo, éste puede **suplantar** la página web de un banco para obtener claves de la víctima.



Man in the middle

El **ataque de intermediario** consiste en interceptar las comunicaciones entre dos usuarios, o un usuario y una fuente (una red cercana, una web conocida, una página de banca online...), e imitar a uno de ellos para robar información pasando desapercibido.



Spam o correo basura

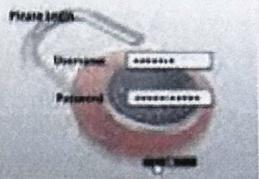
Son mensajes de correo electrónico que inundan la Red con la finalidad de anunciar productos, a veces de dudosa legalidad, para que los destinatarios los comprendan. Se envían de forma masiva porque está demostrado que uno de cada doce millones de los correos enviados obtiene una respuesta positiva. Los estudios indican que actualmente el spam supone el 80% del tráfico de correo electrónico en el mundo.



NO SPAM

Crackers

Son personas que se dedican a cambiar el funcionamiento de un programa comercial o bien a realizar aplicaciones que obtengan números de serie válidos en ese tipo de programas con el fin de **usarlos sin licencia** (piratearlos).



Cookies

Son **archivos de texto** que se almacenan en el ordenador a través del navegador cuando visitamos una página web, para que esa web los lea en visitas posteriores. No son un riesgo ni una amenaza mientras sólo pretendan facilitarnos el acceso al sitio. Así, es habitual, por ejemplo, que la segunda vez que visitemos una web de compras online desde el mismo ordenador ya estén completados algunos parámetros, tengamos la configuración que habíamos seleccionado en la visita anterior o incluso tengamos un saludo de bienvenida personalizado, todo ello fruto de las cookies almacenadas en la primera visita. Se puede considerar spyware no malicioso.



Fake news

Bulos, noticias falsas, fraudes... ¿Pero qué está pasando en Internet? Con la expansión de las redes sociales, la información se extiende a una velocidad increíble, pero no toda esa información es veraz.



¿Qué podemos hacer para que no nos manipulen con informaciones falsas? Nosotros te ofrecemos estos consejos: investiga la fuente de la noticia; busca el autor; intenta informarte por varios medios; intenta encontrar información contraria a tus opiniones y no te quedes sólo con lo que quieras oír.

Vulnerabilidades. Fortalezas y debilidades

La calidad de los sistemas operativos, las aplicaciones y los programas se mide por sus **fortalezas y debilidades**.

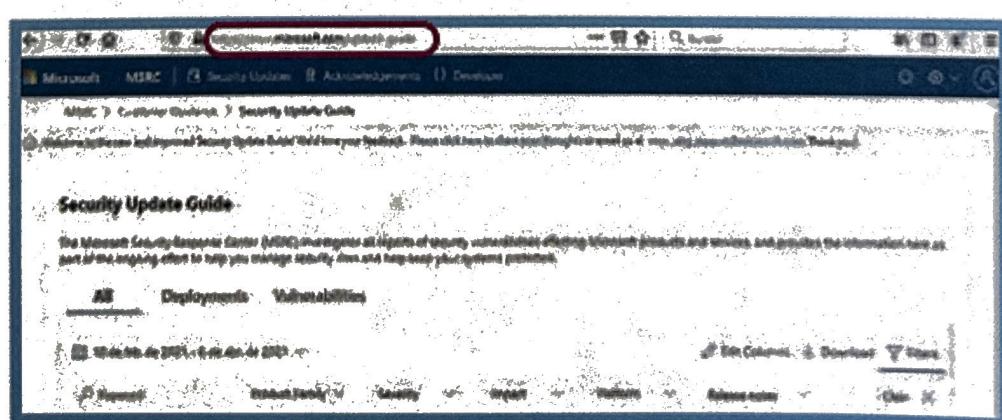
Las **vulnerabilidades** son puntos débiles de un sistema que pueden ser aprovechados para atacarlo. Las empresas que desarrollan software van detectándolas y solucionándolas con actualizaciones. Si aún no han sido detectadas por las empresas desarrolladoras, un ciberdelincuente podría utilizarlas contra los equipos que tienen instalado ese software.

A veces son los propios usuarios quienes informan de las vulnerabilidades a las empresas, pero lo normal es que éstas dispongan de departamentos dedicados exclusivamente a la seguridad.

Microsoft, por ejemplo, publica periódicamente boletines de seguridad en los que se clasifican las vulnerabilidades detectadas, se describen las soluciones y se proporcionan vínculos a las actualizaciones correspondientes del software afectado.

La siguiente tabla recoge la clasificación que hace Microsoft de las vulnerabilidades:

Calificación	Definición
Critica	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	Vulnerabilidad cuyo impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacarle partido a dicha vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.



4. Seguridad activa. Técnicas contra el malware. Sistemas de verificación e identificación

La seguridad activa consiste en identificar qué partes del sistema son vulnerables y establecer medidas que minimicen el riesgo. Mantener al día la seguridad de nuestro equipo es una labor fundamental para evitar ataques al mismo y pérdidas de información.

El software y los elementos de prevención del equipo son:

- **Antivirus.** Un antivirus es un **programa** que analiza las distintas unidades y dispositivos, así como el flujo de datos entrantes y salientes, revisando el código de los archivos y buscando fragmentos de caracteres. Utiliza una base de datos con cadenas de caracteres características de distintos virus. El antivirus puede detectar virus y sólo a veces identificarlos. Aunque la creación de virus es rápida y siempre va a ir por delante de la protección de los fabricantes de antivirus, podemos estar tranquilos si tenemos uno instalado y actualizado. En realidad, los antivirus protegen contra virus, troyanos y gusanos, y la mayor parte contienen también antispyware e incluso filtros antispam.
- **Cortafuegos o firewall.** Se trata de un sistema de defensa que **controla y filtra el tráfico** de entrada y salida a una red. El cortafuegos se configura para que controle el tráfico de los puertos (las conexiones de nuestro ordenador se hacen a través de ellos) y nos muestre alertas para pedir confirmación de cualquier programa que utilice la conexión a Internet. Por ello, es muy importante realizar esta configuración con criterio. Normalmente están incorporados en los sistemas operativos y existen además otros de software libre o de pago.
- **Proxy.** Es un **software** instalado en el PC que funciona como puerta de entrada; se puede configurar como cortafuegos o como limitador de páginas web.
- **Contrasenñas.** Pueden ayudar a proteger la seguridad en un archivo, una carpeta o un ordenador dentro de una red local o en Internet.
- **Red privada virtual (VPN).** Es la mejor forma de navegar por Internet de forma segura protegiendo los datos privados, ya que cifra el tráfico de Internet y oculta la dirección IP y, por tanto, la ubicación virtual. Desde que un usuario se conecta a un servidor VPN, los datos que envía y recibe dejan de ser visibles para los proveedores de Internet y para terceros. El navegador Opera, por ejemplo, integra el servicio VPN. Junto con el firewall, se considera la mejor técnica de **seguridad perimetral** de los sistemas, esto es, entre la red local de una vivienda o empresa y la red pública Internet.
- **Sistemas de detección de intrusos (IDS).** Son mecanismos que monitorizan las máquinas y analizan los sistemas en busca de patrones que puedan denotar un intento de ataque. Por ejemplo, los verificadores de integridad del sistema (SIV) monitorizan archivos para detectar cambios no autorizados, como accesos a usuarios no registrados.
- **Biometría y sistemas de autenticación de doble factor,** que mejoran el sistema de contraseñas. Como se ha explicado anteriormente, la biometría estudia las medidas biológicas que pueden servir para identificar personas, como la huella digital, el reconocimiento facial o la lectura de la retina, y los sistemas de autenticación de doble factor consisten en enviar una segunda contraseña a un dispositivo distinto del que se está usando.
- **Criptografía.** Es el cifrado de información para proteger archivos, comunicaciones y claves. Un algoritmo criptográfico es una función matemática que, en combinación con una clave, se utiliza para encriptar y desencriptar datos y cuya finalidad es hacer lo más difícil posible la desencriptación de los datos si no se tiene la clave.



Consejos para crear una contraseña segura

Se recomienda que las contraseñas tengan entre seis y ocho caracteres para que no se puedan vulnerar fácilmente, aunque el nivel de seguridad será distinto en nuestra clave de usuario del ordenador que en un router Wi-Fi, por ejemplo.

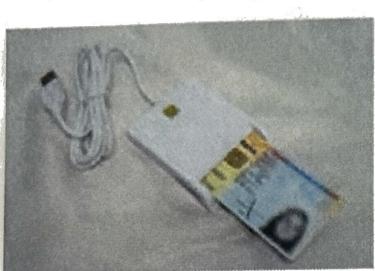
Se aconseja:

- Alternar mayúsculas y minúsculas
- Utilizar números y caracteres no alfabéticos
- Que se pueda teclear rápidamente
- Que no esté contenida en un diccionario
- Que no se relacione con datos personales (DNI, apellido, etc.)

Escanea este código QR para ver el video "Cómo generar contraseñas seguras", del canal OSISeguridad.



Certificados digitales. La firma electrónica



Existen mecanismos que pueden ayudarnos a proteger nuestra identidad en Internet y **evitar el fraude**, como es el caso de los certificados digitales.

Un **certificado digital** (o **electrónico**) es un documento en formato digital que contiene datos identificativos de una persona validados de forma electrónica y que pueden ser utilizados como medio para identificar al firmante.

El certificado digital permite realizar gestiones desde el ordenador personal con seguridad, las veinticuatro horas del día, sin necesidad de desplazarse o de hacer colas.

En particular, se llama **firma electrónica** al tipo de certificado digital que tiene la misma validez que la firma manuscrita. Otro certificado digital es el **DNI electrónico**, que expide el Ministerio del Interior.

Cualquier certificado digital permite acceder a los servicios públicos de forma que las dos partes implicadas en una gestión (el usuario y una administración pública) puedan identificarse mutuamente con la seguridad de que son ellos los que están interactuando. Además, evita que otras personas puedan conocer la información que se intercambia.

¿Cómo se obtienen?

Obtener un certificado electrónico es gratuito; para hacerlo, se ha de seguir el siguiente procedimiento:

1. En un ordenador con acceso a Internet, solicitar el certificado a un prestador de servicios de certificación.
2. Acreditar la identidad personándose físicamente en una oficina de registro.
3. Descargar el certificado desde Internet.

¿Para qué sirven?

Según la Sede Electrónica del Instituto Nacional de Estadística, un certificado electrónico sirve para:

- Autenticar la identidad del usuario, de forma electrónica, ante terceros.
- Firmar electrónicamente de forma que se garantice la integridad de los datos trasmítidos y su procedencia. Un documento firmado no puede ser manipulado, ya que la firma está asociada matemáticamente tanto al documento como al firmante.
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

¿Qué se puede hacer con un certificado digital?

- Tramitar becas y ayudas.

- Presentar la declaración de la renta.

- Consultar los puntos y las sanciones de tráfico.

- Solicitar certificaciones.

¿Cómo sé si tengo un certificado digital instalado en el ordenador?

Para ver el certificado digital una vez instalado en un navegador, ve a **Herramientas / Opciones de Internet**. En la pestaña **Contenido**, pulsa el botón **Certificados** y, una vez en la nueva ventana, haz clic en **Ver**. Se mostrará una pantalla con la relación de certificados personales instalados en tu navegador.

5. Seguridad pasiva

La **seguridad pasiva** consiste en minimizar el impacto de un posible daño informático, asumiendo que, por mucho que pongamos en funcionamiento la seguridad activa, cualquier sistema es vulnerable. En este caso, se trata de disminuir las consecuencias de ataques, pérdidas de información involuntarias, accidentes, descuidos, etc.

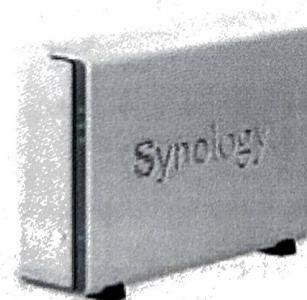
Los principales mecanismos de actuación pasivos son:

- **Sistemas de alimentación ininterrumpida (SAI).** El ordenador toma la corriente eléctrica de estos dispositivos en lugar de conectarse a la red directamente. Protegen a los equipos frente a apagones y también frente a picos o caídas de tensión que podrían estropear el sistema. Cuando se produce un corte de suministro eléctrico, el SAI proporciona el tiempo suficiente al usuario para guardar la información que esté generando o utilizando y apagar correctamente el equipo.



SAI

- **Dispositivos NAS (network-attached storage, almacenamiento conectado en red).** Son dispositivos de almacenamiento específicos a los que se accede a través de una red, por lo que suelen ir conectados a un router. Permiten sistemas de almacenamiento **en espejo**, es decir, con dos discos duros que se copian de forma automática, lo que facilita la recuperación de la información en caso de rotura de uno de los discos.



NAS

- **Política de copias de seguridad (o backups).** Permiten restaurar sistemas o datos si es necesario. Es importante planificar en qué soporte se realizan, con qué periodicidad y de qué elementos del sistema. Por ejemplo, en el sistema operativo Windows se llama **copia de seguridad completa** a la que se realiza con aplicaciones y datos, y **copia de archivos** a aquella en que sólo se copian datos.

Recomendaciones de Microsoft para las copias de seguridad

- No haga la copia de seguridad de sus archivos en el mismo disco duro en el que está instalado Windows.
- Almacene siempre los medios usados para las copias de seguridad (discos duros externos, DVDs o CDs) en un lugar seguro para impedir el acceso de usuarios no autorizados a los archivos; recomendamos usar una ubicación ignífuga independiente del equipo. También dispone de la opción de cifrar los datos de la copia de seguridad.

A veces es difícil distinguir si nuestro ordenador está siendo atacado o bien está funcionando mal por otros motivos. A continuación se recogen los síntomas que nos pueden indicar si está sufriendo algún ataque, así como una serie de pautas para prevenirlo.

¿Cómo saber si nuestro PC ha sido atacado?

Los síntomas de que nuestro PC ha sido atacado pueden ser:

1. El ordenador trabaja con una ralentización exagerada de los procesos o la conexión a la Red.
2. Disminuye el espacio disponible en el disco (salen avisos de que no hay espacio suficiente).
3. Aparecen programas desconocidos, se abren páginas de inicio nuevas en el navegador o se añaden elementos que no se pueden eliminar.
4. Aparecen iconos desconocidos en el escritorio (a veces no se pueden eliminar).
5. El teclado y/o el ratón hacen cosas extrañas.

Seguridad activa y pasiva

Como en tantos otros aspectos de la vida, la mayor seguridad es la **prevención**. Unas sencillas medidas de prevención serán suficientes para utilizar con seguridad nuestro equipo de uso educativo o doméstico, eso sí, teniendo en cuenta que no existe la seguridad absoluta. Es aconsejable:

1. Realizar periódicamente **copias de seguridad** (o **backups**) del sistema que permitan restaurarlo si es necesario.
2. Utilizar **contraseñas seguras** en todos los dispositivos y aplicaciones, y, cuando sea posible, reforzar la protección con **biometría** o **sistemas de autenticación de doble factor**.
3. Usar solamente **redes Wi-Fi abiertas** que sean de confianza para intercambiar datos privados.
4. Tener instalado y actualizado un programa **antivirus** (y conocer sus **funciones y limitaciones**).
5. Tener actualizado el **sistema operativo**.
6. Revisar sistemáticamente los **dispositivos** introducidos en el equipo.
7. Llevar cuidado con las **descargas de archivos** con programas del tipo P2P o *peer to peer* (eMule, Ares, Bit-Torrent, etc.), que son una vía de entrada de archivos desconocidos que pueden contener virus.
8. Tener cuidado a la hora de configurar el **cortafuegos** para permitir la comunicación de estos programas.
9. Prestar atención a las **descargas gratuitas** de programas.

6. Amenazas y fraudes en las personas

En la seguridad, lo más importante es proteger a las personas. Los daños a la máquina no dejan de ser daños materiales, pero los daños causados a las personas permanecen en el tiempo y trascienden a otros aspectos de la vida.

Debemos tener en cuenta que la seguridad hacia las personas abarca muchas otras áreas, como por ejemplo la seguridad postural frente al ordenador o el riesgo de adicciones al ordenador.

Todos somos vulnerables, y nuestra vulnerabilidad aumenta cuanto más nos expomos. En Internet nos mostramos a los demás en mayor o menor medida. Entre los peligros que pueden amenazarnos están:

- El **acceso involuntario** a información ilegal o perjudicial.
- La **suplantación** de la identidad, los robos y las estafas. Por ejemplo, el **phishing** es un delito informático de estafa que consiste en adquirir información de un usuario (datos bancarios, claves, etc.) a través de técnicas de engaño para usarlos de forma fraudulenta. Su nombre alude al hecho de "pescar" contraseñas (en inglés, pescar es *to fish*). El ejemplo más habitual es el de un correo que llega al usuario suplantando una comunicación de un banco y pidiéndole sus claves de acceso bajo una falsa amenaza de seguridad.
- La **pérdida** de nuestra intimidad o el **perjuicio** a nuestra identidad o imagen.
- El **ciberbullying** o **ciberacoso**, que es un tipo de acoso que consiste en amenazas, chantajes, etc., entre iguales a través de Internet, el teléfono móvil o los videojuegos.
- La **adicción al uso de dispositivos**.

Aunque es difícil tener datos, estudios recientes apuntan a que una de cada diez personas ha sido acosada alguna vez, y una de cada tres ha participado en un acoso de alguna forma.



■ Proteger nuestros datos

La **privacidad** es el ámbito de nuestra vida privada que tenemos derecho a proteger de cualquier intromisión.

Por la época en que has nacido, tienes más difícil que nunca proteger esa privacidad, que es uno de nuestros bienes máspreciados. Proteger nuestros datos no consiste solamente en llevar cuidado con la información que subimos a Internet, sino también con decidir bien a qué sitios subimos esa información. Piensa que cualquier sitio web de los que usas de forma gratuita, y que forman parte de una gran empresa tecnológica, puede que se mantenga a costa de tener datos nuestros.

Cuando un producto no te cuesta dinero, es que el producto eres tú.

¿Por qué esos datos dan dinero? Porque permiten tener información personalizada sobre ti, que hace que la publicidad que te dirigen tenga más oportunidades de surtir efecto. No se trata de vender tus datos, sino de incluirlos en un algoritmo que dirija hacia ti la publicidad más idónea y ofrecerte contenidos que van a hacer que utilices más horas los dispositivos o a llamar tu atención con notificaciones que te hagan coger el dispositivo cuando lo has dejado, con lo que te podrán ofrecer más publicidad.

¿Y qué datos son? Pues tus gustos, aficiones, opiniones políticas y religiosas... Dicho así, parece increíble, pero se deduce de todo lo que tú has subido alguna vez a las redes sociales, o de aquellas cosas por las que te has interesado haciendo clic en contenidos relacionados... Se puede controlar todo: el tiempo que miras una imagen, el número de clics que has hecho en un contenido...

■ Software para proteger a la persona

Existen programas que facilitan el **control parental** del uso de Internet. Pueden limitar las búsquedas, permitir o bloquear sitios web, controlar los programas de mensajería instantánea, establecer filtros según la edad del menor, etc. Son ejemplos de programas de control parental **KidsWatch** (www.kidswatch.com) y **K9 Web Protection** (www.1.k9webprotection.com).

■ Responsabilidad digital



Todo lo que hacemos en Internet deja rastro, una **huella digital** que habla de ti. Esa información es tu **identidad digital**. Es tu deber cuidarla y las leyes te protegen para ese fin. Además de las precauciones que hemos visto a lo largo del tema, existen otros mecanismos para ayudarnos a proteger nuestra identidad en Internet y evitar el fraude, como es el caso de los certificados digitales.

Además del software que tengamos a nuestra disposición, debemos tener claro que la mayor protección está en nosotros mismos y en los adultos de confianza: padres, profesores y especialistas. Como hemos visto ya antes, nuestra actitud es la mejor protección. Debemos actuar con **responsabilidad digital**.

■ Hábitos orientados a la protección de la intimidad y de la persona

Te ofrecemos unas recomendaciones básicas para protegerte, que pueden considerarse un código básico de responsabilidad digital.

- 1.** **Habla con tus padres** respecto a la navegación por Internet, ellos siempre van a ayudarte. Si recibes algo raro o desagradable, habla de ello con un adulto o **denúncialo**.
- 2.** **No solicites ni entregues** por Internet **datos** como direcciones, contraseñas, números de teléfono, lugar de estudios, sitios donde habitualmente te reúnes o cualquier otra información que pueda identificarte. Utiliza **alias** o nicks que no contengan tu fecha de nacimiento o datos sobre ti.
- 3.** **No te relaciones con desconocidos** y ten presente que no siempre las personas son lo que dicen que son. Desconfía de la persona que quiere saber demasiado sobre ti. Recuerda que existen otras formas más seguras de hacer nuevos amigos.
- 4.** **Gira la cámara hacia un ángulo muerto o tápala** con una pegatina cuando no la estés usando, para impedir que capture imágenes. Recuerda que la **cámara web puede ser manipulada de forma remota usando software malicioso**. Desde hace años, la Policía alerta de que a menudo las imágenes que creemos que vienen de la webcam de otra persona son en realidad imágenes trucadas por ella.
- 5.** **No pubiques** fotos o vídeos tuyos **a la ligera**; si decides publicar algo, que sea en sitios con acceso restringido y siempre que no dañen tu imagen actual o futura y con el permiso de tus padres. Recuerda que no puedes publicar imágenes de nadie sin su consentimiento. Sé **respetuoso** con los demás.
- 6.** **Mantente al día** con la tecnología y **limita el tiempo de navegación** por Internet.
- 7.** **Respecta la edad mínima** para poder acceder a los sitios. Esta edad se encuentra en las **condiciones de uso** de la página que debemos leer antes de pulsar el botón "Acepto". Si lo pulsamos sin leer, podemos estar autorizando a los propietarios del sitio a usar nuestros datos, nuestras imágenes, etc.
- 8.** **Infórmate sobre los sitios**. En algunos sitios no es posible "darse de baja", así que hay que tener cuidado con los contenidos que introducimos en ellos, pues a veces cedemos nuestros datos para siempre.
- 9.** Nunca intercambies datos privados en **redes Wi-Fi abiertas** que no sean de confianza. Tanto el administrador como alguno de los usuarios conectados pueden utilizar técnicas para robarte información.

En definitiva: usa el sentido común y no hagas en el ordenador cosas que no harías en tu vida cotidiana.

7. Seguridad en Internet

Internet es una red que conecta ordenadores y personas de todo el mundo. Es una forma de comunicación con muchas ventajas, pero también con riesgos: es un mundo de información en el que tenemos que manejarlos con seguridad.

Hablar de seguridad informática es hablar de seguridad en Internet. La mayoría de las amenazas y fraudes vienen a través de la Red, por lo que le dedicaremos un apartado.

■ Las redes sociales y la seguridad

Una **red social** es una estructura que permite intercambios de distintos tipos (financieros, amistosos, de temas especializados...) entre individuos y se basa en la relación entre los miembros de la red.

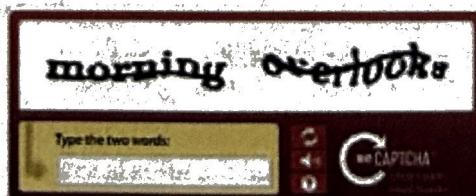
Cuando usamos una red social, debemos tener presentes nuestra **seguridad** y el **respeto** a los demás. La **netiqueta** es un conjunto de normas que debemos respetar para tener un comportamiento adecuado en la Red. Desde que comenzó la interacción entre usuarios en Internet, surgió la figura del **trol**, que es una persona que se ampara en su identidad desconocida para provocar, opinar de forma irrelevante y molestar. Muchas veces, los troles son personas cobardes que no se atreverían a hacer algo similar en la vida real. En Internet, como en el mundo real, debemos comportarnos con educación.

Por lo demás, las redes sociales cumplen la función para la que han sido diseñadas y no tienen por qué representar un peligro. Eso sí, ten en cuenta lo siguiente:

- Para poder acceder a las redes sociales es necesario tener una **edad mínima**. Esta edad se encuentra en las condiciones de uso de la página, las cuales debemos leer antes de pulsar el botón de aceptar.
- Al pulsar dicho botón, estamos aceptando tanto las **condiciones de uso** como la **política de privacidad**. Si lo pulsamos sin leer las condiciones, puede ocurrir que estemos dando autorización a los propietarios de la red social para que usen nuestros datos, nuestras imágenes, etc.
- Una vez que nos hemos dado de alta, nos suelen solicitar **datos muy personales**, como creencias religiosas, ideología política, etc., que no debemos facilitar. Ni debemos tampoco proporcionar datos como nuestro número de teléfono o el centro donde estudiamos, ya que permiten que nos puedan localizar.
- En algunas redes no es posible **darse de baja**. Los datos quedan para siempre a disposición de la empresa propietaria y el usuario solamente puede desactivar la cuenta (pero no la elimina), así que hay que tener cuidado con los contenidos que difundimos en la Red.

¿Qué es un CAPTCHA?

Cuando nos registramos en cualquier aplicación de Internet, nos aparece algo similar a lo que te mostramos en la imagen. Se trata de un CAPTCHA (*completely automated public Turing test to tell computers and humans apart*, prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos). Es decir, es una simple prueba que demuestra que es un ser humano y no un ordenador quien intenta acceder a una cuenta protegida con contraseña.



Para más información puedes visitar el sitio oficial www.captcha.net.



facebook

Linkedin

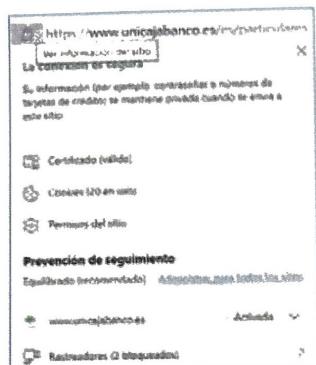


Telegram



WhatsApp

■ Protocolos seguros



La forma en que nuestro ordenador se comunica con otros sigue una serie de reglas comunes que constituyen un **protocolo**.

- Los **servidores** emplean el **protocolo HTTP** (*hypertext transfer protocol*, protocolo de transferencia de hipertexto) para enviar y recibir documentos a través de Internet.
- Los **paquetes** de información siguen el protocolo **TCP/IP** (*transfer control protocol / Internet protocol*).

Vamos a conocer dos versiones seguras de estos protocolos: el **HTTPS** y el **IPv6**.

- **HTTPS.** En Internet podemos encontrar páginas que utilizan una conexión segura: emplean un protocolo criptográfico seguro llamado **HTTPS** (*hypertext transfer protocol secure*). El cifrado de estas páginas se basa en certificados de seguridad SSL (*secure sockets layer*), creando un canal codificado que no puede ser interpretado en el caso de que alguien intercepte la conexión. Además de utilizarse en el comercio electrónico, se usa en entidades bancarias y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.



- **IPv6** es la última versión del protocolo IPv4 (versión actual). Es un protocolo seguro, ya que trabaja de manera cifrada. Si se intercepta una comunicación, la información no podrá ser leída sin antes descifrarla.

El IPv4 asigna a cada dispositivo una serie de cuatro números (cada uno de ellos comprendido entre el 0 y el 255). Pero el IPv4 sólo permite aproximadamente 4.000 millones de direcciones, e Internet necesita un mayor espacio. El IPv6 amplía el número de direcciones disponibles a una cantidad prácticamente ilimitada: 340 sextillones de direcciones. Estas direcciones tienen una notación en ocho grupos de cuatro dígitos hexadecimales. Puedes ver una dirección IPv4 y una IPv6 en la ventana de comandos de la figura 4:

```
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . . : telefonica.net
Descripción . . . . . : Qualcomm Atheros AR956x Wireless Network Adapter
Dirección física. . . . . : 32-C4-00-A7-6F-E4
DHCP habilitado . . . . . : si
Configuración automática habilitada . . . . . : si
Vínculo: dirección IPv6 local. . . . . : fe80::160d:d216:fe16%15(Preferido)
Dirección IPv4. . . . . : 192.168.1.35(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : sábado, 7 de mayo de 2016 21:55:42
La concesión expira . . . . . : domingo, 8 de mayo de 2016 23:06:02
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 184634621
DUID de cliente DHCPv6. . . . . : 00-01-00-F9-1D-8F-D1-F7-F8-32-E4-35-F7-32
Servidores DNS. . . . . : 80.58.61.250
80.58.61.254
Servidor WINS principal . . . . . : 192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Fig. 4

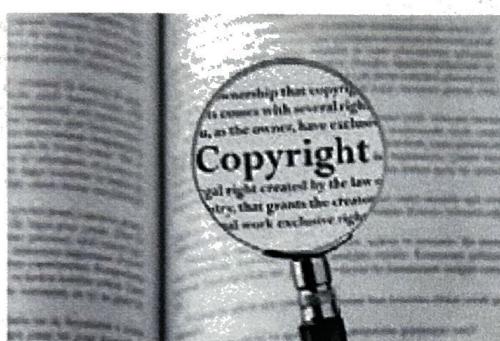
Se puede averiguar si un dispositivo tiene IPv6. Para comprobarlo, puedes visitar la página ipv6test.google.com.

■ La propiedad intelectual y la distribución del software

Internet puede proporcionarnos mucha información y servicios de interés. También podemos encontrar en la Red software de todo tipo que nos puede interesar conseguir.

Es muy importante saber que el software, al igual que otras creaciones artísticas, como libros, canciones, obras pictóricas, etc., está protegido por la ley de propiedad intelectual.

Los derechos de autor son un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley reconoce a los autores por la creación de una obra publicada o inédita. La **propiedad intelectual** agrupa todos los derechos del autor sobre la disposición y explotación de su creación.



Cuando accedemos a una página web para descargarnos alguna aplicación, es muy importante que conozcamos con qué tipo de licencia se corresponde el software que queremos descargar. No todas las descargas son ilegales o atentan contra la propiedad intelectual.

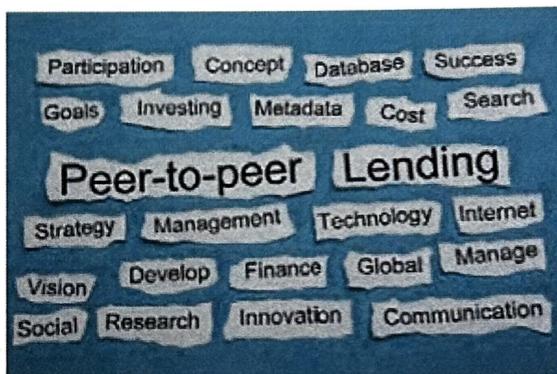
La siguiente tabla recoge los principales tipos de software disponibles según las licencias que los regulan:

Software comercial	Software de una empresa que se comercializa con ánimo de lucro. A veces se le llama <i>software propietario</i> , ya que todo el software comercial es propietario, pero esto no sucede al revés. Ejemplos: Microsoft Office, Windows 11.
Freeware	Software gratuito pero no libre. Es software propietario. Ejemplos: Microsoft Edge, Adobe Flash Player.
Software libre	Se puede usar, copiar, modificar y redistribuir libremente. Su código fuente está disponible, lo que se conoce como <i>código abierto</i> . Ejemplos: LibreOffice, GIMP, Audacity.
Copyleft	Licencia de uso que acompaña al software libre para poder ser modificado y redistribuido.
Licencia GNU/GPL (licencia pública general)	Licencia que acompaña a los paquetes distribuidos por el Proyecto GNU. El autor conserva los derechos y permite la redistribución y modificación bajo la misma licencia.
Licencias Creative Commons	Sirven para otorgar el derecho a utilizar una publicación protegida por derechos de autor. Hay diferentes licencias de este tipo, según los permisos que otorga. Por ejemplo: <ul style="list-style-type: none"> • Licencia CC BY: permite la distribución, adaptación y creación de obras derivadas, siempre y cuando se reconozca al autor original del material. • Licencia CCO: con ella, los creadores renuncian a los derechos de sus trabajos y los ceden al dominio público.

■ Intercambio de archivos: redes P2P

Todo el software que un usuario utiliza o adquiere a través de las distintas vías disponibles (tiendas, descargas, Internet, etc.) tiene una **licencia de uso**, es decir, un contrato, una serie de términos y condiciones que el usuario deberá cumplir a la hora de instalarlo y usarlo.

Una de las formas más extendidas para obtener software en la Red son las llamadas **redes P2P** (redes *peer to peer* o redes entre iguales). Los ordenadores que componen estas redes se comportan como iguales entre sí, actuando a la vez como clientes (solicitantes de información) y servidores (proveedores de información). Esto posibilita el intercambio directo de información entre los equipos que forman parte de la red. Las redes P2P optimizan el ancho de banda de todos los usuarios de la Red, aprovechando la conectividad entre ellos.



La información se trocea y se envía por la red. Los usuarios intercambian esos paquetes de información, que son reconstruidos cuando el usuario ha recibido todos los componentes. Esto posibilita el intercambio de archivos grandes y es una de las características que han popularizado su uso.

Sin embargo, el hecho de que el intercambio de información se produzca de forma directa entre los usuarios ha propiciado que se distribuyan de esta forma aplicaciones cuya difusión no es gratuita, lo que ha generado mucha controversia sobre la legalidad o no del intercambio de contenidos protegidos por la ley de propiedad intelectual y los derechos de autor.



Este extremo merece una reflexión: debemos valorar objetivamente el esfuerzo y el trabajo de los creadores para obtener una obra (software, música, libros, etc.) y el perjuicio causado cuando esa obra es apropiada indebidamente por otros sin satisfacer los derechos de los autores.

En Internet existen gran cantidad de sitios desde los cuales puedes descargar contenidos de forma legal, e incluso, en muchos de ellos, gratuitamente.

RESUMEN DE LA UNIDAD

■ Seguridad informática

- El **big data** es la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional.
- El **Internet de las cosas** es la conexión de objetos de uso cotidiano con Internet para dotarlos de interactividad.
- La **seguridad informática** es el conjunto de medidas encaminadas a proteger el hardware, el software, la información y las personas (por ejemplo, usar contraseñas seguras, tener un antivirus actualizado, etc.).
- Debemos distinguir varios **tipos de seguridad**:
 - Activa y pasiva
 - Física y lógica
 - De la persona y de los sistemas de información

■ Seguridad en los lenguajes y las aplicaciones. El hacking ético

- Se llama **malware**, **software malicioso** o **software malintencionado** al software elaborado con fines maliciosos:
 - Virus
 - Gusanos
 - Troyanos
 - Keyloggers
 - Hijackers
 - Etc.
- Podemos sufrir los siguientes **ataques**:
 - Piratas informáticos
 - Ramsomware
 - Pharming
 - Man in the middle

■ Seguridad activa y seguridad pasiva. Técnicas contra el malware

- La **seguridad activa** consiste en identificar qué partes del sistema son vulnerables y establecer medidas que minimicen el riesgo. Mantener al día la seguridad de nuestro equipo evita ataques al mismo y pérdidas de información.
- El **software y los elementos de prevención del equipo** son:
 - Antivirus
 - Cortafuegos
 - Proxy
 - Contraseñas
 - Biometría y sistemas de autenticación de doble factor
 - Criptografía
- La **seguridad pasiva** consiste en minimizar el impacto de un posible daño informático, asumiendo que, por mucho que pongamos en funcionamiento la seguridad activa, cualquier sistema es vulnerable.
 - Sistemas de alimentación ininterrumpida (SAI)
 - Dispositivos NAS (network area storage)

■ Amenazas y fraudes en las personas

- Entre los **peligros** que pueden amenazarnos están:
 - El acceso involuntario a información ilegal o perjudicial
 - La suplantación de la identidad, los robos y las estafas
 - La pérdida de nuestra intimidad o el perjuicio a nuestra identidad o imagen
 - El ciberbullying
- Todo lo que hacemos en Internet deja rastro, una **huella digital** que habla de ti. Esa información es tu **identidad digital**. Es tu deber cuidarla y las leyes te protegen para ese fin. Debemos actuar con **responsabilidad digital**. Cuando usamos Internet, debemos tener presentes nuestra **seguridad** y el **respeto** a los demás. Las leyes nos protegen.

■ Seguridad en Internet

- Algunas páginas con conexión segura usan el protocolo criptográfico **HTTPS**.
- El **IPv6** es un protocolo seguro, ya que trabaja de manera cifrada.

2**Seguridad en sistemas informáticos y redes****Amplia y profundiza****Amplia 1. Elaborar un plan de seguridad: presentación y esquema de bloques**

Elabora un plan de seguridad para una red de ordenadores (la de tu aula o la de todo tu centro). Con tu plan de seguridad debes contestar estas tres preguntas:

- ¿A quién necesitamos proteger?
 - ¿De qué es necesario protegerlo?
 - ¿Con qué herramientas contamos para ello?
- Recopila la información necesaria para responder esas preguntas, consultando el apartado "Conoce" de esta unidad: quién usa el aula de informática, qué peligros hay, qué dispositivos tenemos, con qué software podemos contar.
 - Con esa información, planteáte si es posible mejorar la seguridad con alguna de las herramientas que hemos visto en la unidad.
 - Elabora tu plan de seguridad estructurando todos los datos recopilados en un programa de presentaciones (PowerPoint, Impress o Prezi, por ejemplo). Debe contener al menos tres apartados para contestar las tres preguntas propuestas.
 - Elabora un esquema de bloques con los elementos de protección física frente a ataques externos para una pequeña red considerando los elementos hardware de protección. Dibuja el esquema con un programa específico para diagramas de flujo, como Dia Diagram Editor o la galería de diagramas de flujo de LibreOffice Draw.
 - Guarda todos los archivos como X1_nombreapellido.



Dia Diagram Editor

Baremo orientativo de calificación

1.	Recopilación de información	1 punto
2.	Propuestas realizadas	3 puntos
3.	Elaboración del plan	2 puntos
4.	Diagrama de bloques	4 puntos

Amplia 2. Infografía de un plan de seguridad con Piktochart

Representa con una infografía el plan de seguridad que has elaborado en el ejercicio anterior, teniendo en cuenta los elementos de protección física frente a ataques externos para una red y considerando los elementos hardware de protección. Utiliza para ello la versión gratuita de Piktochart (la de pago dispone de más opciones).

- Accede a Piktochart y regístrate (o accede con tu cuenta de Gmail o de Facebook). Si no tienes cuenta de Gmail, puedes crear una entrando en www.gmail.com.
- En Piktochart, elige el formato que deseas para tu infografía. Selecciona la plantilla y haz clic en el botón **Create**.
- Carga imágenes que representen la red y las medidas de seguridad. Añade textos explicativos.
- Cuando hayas acabado, puedes descargar la infografía a tu ordenador en formato PNG, imprimirla después, compartirla por correo electrónico y también publicarla. Haz clic en el icono **Download** de la barra superior de herramientas para descargar tu infografía.
- Guarda el archivo como X2_nombreapellido.png.

Baremo orientativo de calificación

1.	Imágenes representativas	2 puntos
2.	Elementos de protección física usados	2 puntos
3.	Software de protección usado	2 puntos
4.	Infografía en conjunto	4 puntos

Amplia 3. Elaborar un video: "La seguridad falló, malas noticias"

Vamos a hacer un vídeo de seguridad con noticias sobre fallos de seguridad.

1. Recopila noticias sobre fallos de seguridad que sean actuales. Haz una captura de pantalla de cada una de ellas y ve guardándolas en una carpeta.
2. Ordena las noticias siguiendo una de las clasificaciones que hemos visto en la unidad: en las personas o en los sistemas de información. Presta especial atención a las noticias sobre ciberbullying.
3. Elabora el vídeo usando cualquier editor de vídeo, como por ejemplo Canva, con las imágenes, la clasificación y tus comentarios. Titúlalo "La seguridad falló, malas noticias".
4. Guárdalo como X3_nombreadellido.mp4.

**Baremo orientativo de calificación**

1.	Recopilación de noticias	2 puntos
2.	Inclusión de noticias de ciberbullying	2 puntos
3.	Inclusión de un audio de explicación con voz propia	2 puntos
4.	Vídeo en conjunto	4 puntos

Amplia 4. Muro de Padlet sobre tipos de seguridad

En esta actividad deberás confeccionar un muro de Padlet con la información aprendida sobre los tipos de seguridad.



1. Entra en es.padlet.com. Haz clic en **Registrarse** y regístrate con tu cuenta de Gmail (si no tienes cuenta de Gmail, puedes crearte una cuenta de Padlet).
2. Tras el registro, en la pantalla que aparece, pulsa el botón **Hacer un padlet**.
3. En la pantalla siguiente, pulsa **Seleccionar** en la opción **Muro**.
4. Haz doble clic sobre el título que te ha asignado Padlet y te aparecerá una ventana donde puedes cambiar el título y la descripción. Pon "Tipos de seguridad" como título y "Riesgos y soluciones" como descripción.
5. Pulsa **Guardar** y luego **Cerrar**.
6. Ahora haz doble clic en el papel tapiz de la pantalla, para empezar a publicar entradas. Como título de la primera entrada escribe "1. Seguridad activa" y explica en qué consiste ese tipo de seguridad. Busca una imagen representativa e insértala.
7. Completa el muro con los seis tipos de seguridad vistos en el apartado 2 de la unidad.
8. Comparte el muro a través de un enlace con tu profesor o bien haz una captura de pantalla de tu trabajo, pégala en un documento de texto y guárdalo como X4_nombreadellido.

Baremo orientativo de calificación

1.	Por cada elemento del tapiz	1 punto (6 en total)
2.	Por la representatividad de las imágenes	2 puntos
3.	Por la ampliación de la información expuesta	2 puntos