Tema 1 . Seguridad informática

1.1. Seguridad informática. Tipos de seguridad

Cuando salimos a la calle tenemos que tener cuidado en no perder la cartera o en que no nos la quiten. En nuestra cartera además de dinero llevamos nuestro DNI, fotos personales, tarjetas bancarias,..., es decir, información que afecta a nuestra intimidad. ¿No tendremos que poner el mismo cuidado cuando navegamos por internet? En la tranquilidad de nuestras casas nos creemos a salvo del mundo, pero en el momento que nuestro ordenador o smartphone se conecta a internet, nos exponemos a riesgos que hay que tener en cuenta.

La seguridad informática es el conjunto de medidas encaminadas a proteger el hardware, el software, la información y las personas. Un fallo en la seguridad informática puede tener repercusiones graves de tipo económico, social o personal.

La evolución continua de internet hace necesario replantear continuamente las estrategias de seguridad. Pensemos, por ejemplo, en la aparición del **big data** y de **Internet of Things** (**IoT**):

- **Big data** consiste en la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de forma convencional. Su utilidad consiste en hacer pronósticos y diagnósticos relativos a distintos aspectos. Dichos análisis no serían posibles con cantidades de datos más pequeñas. Para el big data es necesario que los usuarios faciliten sus datos personales, como datos de usuario en las redes sociales, pagos con tarjeta, señales de los móviles,… lo que puede afectar a su privacidad y seguridad.
- **Internet of Things** o **Internet de las cosas** es la interconexión digital de los objetos cotidianos con internet, objetos dotados de una identificación IP en internet, como alarmas, termostatos, lavadoras, refrigeradores, lámparas, persianas,… que pueden ser controlados, activados o desactivados a través de la red. Esto aumenta considerablemente los riesgos informáticos.

A la hora de establecer un **plan de seguridad** debemos contestar las siguientes preguntas:

- ¿A quién debemos proteger?
- ¿De qué es necesario protegerlo?
- ¿Con qué herramientas contamos para ello?

Existen diferentes tipos de seguridad informática atendiendo a distintos criterios. De la misma forma que en el mundo del automóvil existen medidas de seguridad activa para evitar accidentes (los frenos, el ESP o sistema de control de estabilidad,…) y medidas de seguridad pasiva para minimizar las consecuencias de un accidente asumiendo que éstos pueden ocurrir (airbag, cinturón de seguridad,…) en el mundo de la seguridad informática ocurre una clasificación similar:

- **Seguridad activa**. Es el conjunto de medidas destinadas a proteger el ordenador y su información reduciendo las vulnerabilidades todo lo posible. La seguridad activa incluye:
    - La instalación de software de seguridad (antivirus, antimalware, cortafuegos, proxy,…).
    - El uso de contraseñas.
    - La encriptación de datos.
    - Los certificados digitales.
- **Seguridad pasiva**. Conjunto de medidas destinadas a minimizar las consecuencias de un daño informático una vez que éste se ha producido. La seguridad pasiva incluye:
    - Copias de seguridad de los archivos.
    - Sistemas de alimentación ininterrumpida (SAI). Son dispositivos con baterías que evitan la pérdida de información durante un apagón eléctrico. También pueden mejorar la calidad de la energía eléctrica filtrando subidas y bajadas de tensión.

Otro criterio utilizado para clasificar los tipos de seguridad informática es el que distingue entre **seguridad física** y **seguridad lógica**:

- **Seguridad física**. Medidas destinadas a proteger el hardware ante posibles desastres naturales (incendios, inundaciones,…), robos, sobrecargas eléctricas,... Este tipo de seguridad es especialmente importante en el caso de los servidores de internet o de ordenadores de empresas. La seguridad física incluye:
    - Sistemas antiincendios y antiinundaciones.
    - Vigilancia para evitar robos.
    - Sistemas para evitar apagones o sobrecargas eléctricas**.**
- **Seguridad lógica**. Medidas destinadas a proteger el software y los datos de los usuarios. Protege la información ante robos o pérdidas con las técnicas de seguridad activa y pasiva.

En relación con el factor humano es posible distinguir entre:

- **Seguridad en los sistemas de información**. Protección ante las amenazas a nuestro ordenador mediante técnicas de seguridad activa y pasiva.
- **Seguridad en la persona**. Consiste en la protección ante amenazas y fraudes a los usuarios. Para ello es importante nuestra actitud, estar bien informados, usar el sentido común y saber que existen leyes que nos protegen.

Dichas leyes defienden nuestros derechos fundamentales, especialmente la intimidad de las personas físicas en relación con sus datos personales. Las dos leyes más importantes son:

- **Ley Orgánica 1/1982** de protección civil del derecho a honor, a la intimidad personal y familiar y a la propia imagen.
- **Ley Orgánica 15/1999 de protección de datos de carácter personal** (**LOPD**) desarrollada en el Real Decreto 1720/2007 y supervisada por la

Agencia Española de Protección de Datos. Se alude a ella en los carteles que indican zonas videovigiladas.

1.2. Amenazas y fraudes en los sistemas de información

El término **malware** (**mal**icious soft**ware**) hace referencia al software malicioso o malintencionado elaborado con fines maliciosos, como virus, troyanos, gusanos, spyware,… En sus comienzos la motivación principal para crear software malicioso era el afán de reconocimiento público o notoriedad de su creador. Por este motivo, las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas para tener relevancia, por ejemplo, eliminar archivos importantes, formatear el disco duro,... Con el tiempo los creadores de software malicioso han pasado a tener una motivación económica, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con el fin de pasar lo más desapercibidos posibles y disponer de tiempo suficiente para robar información, contraseñas, claves bancarias, crear una red de ordenadores zombies o botnet, vender falsos antivirus.

El software malicioso no sólo afecta a los PCs sino también a servidores, smartphones, videoconsolas,... siempre y cuando tengan un Sistema Operativo accesible para el fichero malicioso.

Veamos algunos ejemplos de software malicioso:

- **Virus**. Son programas que se instalan en el ordenador sin el permiso del usuario con el objetivo de causar daños. Tienen la capacidad de autorreplicarse e infectar a otros equipos. Se puede propagar a través de software, de memorias portátiles o de internet**.** No sólo atacan a ordenadores personales, sino también a servidores, smartphones,...

  Los virus infectan normalmente ficheros ejecutables con las extensiones “.exe”, “.bat”, “.com”,... de manera que sólo se ejecutan cuando se ejecuta el archivo infectado. Algunos virus sólo se activan

cuando se cumple una determinada condición, por ejemplo, al llegar a una fecha concreta. Al ejecutarse los virus infectan otros archivos ejecutables. Si estos ficheros se encuentran dentro de un dispositivo extraible o de una unidad de red se propagará con facilidad a otros equipos.

- **Gusanos**. Son programas maliciosos cuyo fin es colapsar la memoria del sistema reproduciéndose continuamente, y ocupando toda la memoria del sistema. A diferencia de los virus, los gusanos no infectan otros ficheros. Se suelen propagar por el correo electrónico con la finalidad de contaminar al mayor número posible de equipos. Hacen que los equipos vayan más lentos.

  Como no infectan otros archivos, para garantizar su autoejecución modifican la carpeta de inicio con el listado de todos los programas que tienen que ejecutarse al arrancar el ordenador. Al no infectar otros archivos, es más fácil eliminarlos del ordenador que los virus.
- **Keylogger**. Software que se encarga de obtener y memorizar las pulsaciones que se realizan en un teclado. Se utiliza para espiar de forma remota con el objetivo de obtener contraseñas del usuario.
- **Spyware**. Es el software espía, a saber:
  - **Hijackers**. Software que "secuestra" a otros programas para usar sus derechos o para modificar su comportamiento. El caso más habitual es el ataque a un navegador, modificando su página de inicio y redireccionando la página de búsqueda sin el consentimiento del usuario.
  - **Troyanos**. Virus que se introducen camuflados en otro programa. Su fin es destruir la información almacenada en el disco duro o recabar información. Suelen estar alojados en archivos tales como imágenes o archivos de música, y se instalan en el sistema al abrir el archivo que los contiene. Su nombre procede del "caballo de Troya" descrito en la Odisea de Homero.
  - **Adware** (advertisement software). Es el software de publicidad incluido en programas que muestran dicha publicidad tras ser instalados. Algunos de ellos tienen licencia freeware o shareware e incluyen publicidad para subvenciones, de forma que si el usuario quiere una versión sin publicidad puede elegir pagar por la versión con licencia registrada. El riesgo está en que estos programas pueden actuar como spyware, incluyendo código para recoger información personal del usuario. Esta información no se usa siempre de forma maliciosa, a veces se trata simplemente de conocer los gustos de los usuarios.
- **Hackers**. Son delincuentes expertos informáticos que, en principio, sólo se plantean retos intelectuales. No tienen por qué pretender causar daños, de hecho, existen empresas de **hacking ético** o **white hacking**, cuyo cometido es ayudar a particulares y empresas a saber cuál es su nivel de seguridad frente a los **piratas informáticos** o **black hackers**, que intentan atentar contra la seguridad de sistemas en la Red y lucrarse con ello.
- **Crackers**. Son personas que se dedican a cambiar el funcionamiento de un programa comercial o a realizar aplicaciones que obtengan números de serie válidos con el fin de usarlos sin licencia (craquearlos).

- **Pharming** y **Phishing**. El **Pharming** es una práctica consistente en redirigir un nombre de dominio a otra máquina distinta de forma que un usuario que introduzca una dirección URL acceda a la página web del atacante. Éste puede suplantar la página web de un banco para obtener claves de la víctima. En el **Phishing** los datos bancarios de la víctima se pretenden obtener por supuestos correos de la entidad bancaria donde se pide que confirmemos los datos de acceso a la cuenta bancaria
- **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. 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. Las cookies pueden ser consideradas spyware no malicioso.

  No obstante, las cookies hacen posible un seguimiento de las páginas web que hemos visitado y el acceso a nuestros archivos de manera que pueden llegar a saber nuestros gustos y preferencias. Con ello crean listas de posibles clientes que luego venden a empresas comerciales.
  Por todo ello, es conveniente eliminarlas periódicamente.
- **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 compren. 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. Normalmente las aplicaciones de correo suelen tener filtros antispam, por los cuales, los correos que son considerados spam se mandan a esa bandeja.
- **Hoaxes**. Son cadenas de correo iniciadas por empresas para poder recopilar las direcciones de correo electrónico de muchos de los usuarios y posteriormente hacer mailings, que constituirán a su vez spam. Se aprovechan de la bondad, la credulidad y la buena fe de los usuarios. Una cadena empieza cuando una empresa envía un mensaje del tipo “¡Cuidado, virus peligroso! Reenvía este mensaje a tus contactos” a millones de direcciones inventadas. Algunas de estas direcciones inventadas, las que no den mensaje de error, existen realmente y reciben el mensaje. Algunos de estos destinatarios reenviarán con buena fe el mensaje y se formará de esta forma la cadena. Después de muchos envíos, llegará de nuevo a la empresa que lo inició, ahora repleto de direcciones válidas. Otras veces son simples bulos creados por personas para obtener notoriedad, pero que también pueden usarse para extraer información de las personas o engañarlas.

Ante estas amenazas y fraudes 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 utilizadas 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.

Los propios usuarios también pueden informar de las vulnerabilidades a las empresas, aunque éstas cuentan con departamentos dedicados exclusivamente a la seguridad.

Microsoft 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.

Microsoft hace la siguiente clasificación de las vulnerabilidades:

- **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**. 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.

1.3. Seguridad activa. Certificados digitales. La firma electrónica

La seguridad activa consiste en identificar qué partes del sistema son vulnerables y establecer medidas que minimicen el riesgo. Es fundamental para evitar ataques a nuestro equipo y pérdidas de información.

Los elementos de prevención más importantes son:

- **Antivirus**. Son programas que analizan las distintas unidades y dispositivos, así como el flujo de datos entrantes y salientes, revisando el código de los archivos y buscando cadenas de caracteres características de distintos virus. Para ello, utiliza una base de datos (**archivo de definiciones**) donde se almacenan esas cadenas de caracteres características. Este archivo de definiciones se tiene que actualizar diariamente, ya que continuamente se están creando nuevos virus.

  Al finalizar el análisis, se elimina el virus. Para ello, el antivirus se conecta todos los días a la web del creador para descargar la última base de datos y, de esa forma, tener el antivirus actualizado. Los antivirus suelen tener un **sistema heurístico** por el cual, cuando detectan un programa potencialmente peligroso por tener un patrón parecido al virus, lo envía a un baúl. El sistema heurístico detecta la presencia de instrucciones concretas y comunes a los diferentes códigos maliciosos, incluso cuando el código analizado no pertenece a un virus y antes de que se haya diagnosticado ese código como virus y se haya creado una vacuna. De esta forma, cuando llega un cierto tiempo y las nuevas firmas (muestra de virus cargadas en la base de datos) no lo consideran virus, se puede restablecer, sacar del baúl.

El antivirus se ejecuta al arrancar el ordenador en modo residente, de forma que analiza cada actividad de la máquina (abrir documentos, leer correos, visita de páginas web, etc). Esto no garantiza que en algún momento no hayamos podido contaminar la máquina con algún programa malicioso, por lo cual, es importante ejecutar el antivirus de vez en cuando con un análisis completo del sistema. En algunas ocasiones, el virus no permite que el antivirus le elimine con el sistema operativo activo. En esos casos, el antivirus requiere que se ejecute al inicio y antes de ser cargado el S.O.

Los antivirus protegen contra virus, troyanos y gusanos, y además, muchos contienen también antispyware y filtros antispam.

- **Cortafuegos** o **firewall**. Se trata de un sistema de defensa que controla y filtra el tráfico de datos de entrada y salida de un equipo 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. Hay que configurarlo correctamente. Por ejemplo, para un servidor donde tenemos instalado un blog y sólo queremos que se lea y poder escribir en el mismo, podemos usar el firewall para decirle que solo se comunique con Internet por el puerto 80, que es el puerto que se usa para ver las páginas web. Con ello evitamos que algún hacker intente entrar en nuestro servidor y hackee nuestra web.

  La mayoría de los sistemas operativos incluyen un cortafuegos, aunque también se pueden instalar otro freeware o de pago.

- **Proxy**. Es un software instalado en un PC que funciona como puerta de entrada; se puede configurar como cortafuegos o como filtro de páginas web.
- **Contraseñas**. Pueden ayudar a proteger la seguridad en un archivo, una carpeta o un ordenador dentro de una red local o en internet. Se recomienda que tengan entre 6 y 8 caracteres para que sean seguras. Consejos para crear una contraseña segura son:
  - Alternar mayúsculas y minúsculas.
  - Utilizar número y caracteres no alfabéticos
  - Que se puedan teclear rápidamente.
  - Que no estén contenidas en un diccionario.
  - Que no se relacionen con datos personales (DNI, apellidos, fecha de nacimiento,...)
- **Criptografía**. Es el cifrado de información para proteger archivos, comunicaciones y claves. La necesidad de proteger mensaje ha existido desde la antigüedad. Ya en tiempos de los romanos Julio César introdujo un sistema de cifrado para comunicarse con sus generales. Tal método consistía en sustituir cada letra del alfabeto por otra que resultaba de desplazarla 13 posiciones en el alfabeto. Así, por ejemplo la letra “A” era sustituida por la “M”, la letra “B” por la “N”, y así, sucesivamente. La clave para cifrar el mensaje era el “desplazamiento de 13 letras”.

  El mensaje cifrado sólo puede ser legible por el destinatario tras su desencriptación.

- **Cetificados digitales** o **electrónicos**. Son documentos en formato digital que contienen datos identificativos de una persona validados de forma electrónica y que pueden ser identificados 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.

  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 lo expide el Ministerio del Interior.

  Cualquier certificado digital permite acceder a los servicios públicos de manera 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. Los certificados electrónicos se obtienen de forma gratuita solicitándolos por Internet a un prestador de servicios de certificación. El usuario debe acreditar personalmente su identidad personándose en una oficina de registro. Posteriormente se puede descargar el certificado desde internet.

  Los certificados electrónicos sirven para autenticar la identidad del usuario ante terceros, firmar electrónicamente de forma que se garantice para que solo el destinatario del documento pueda acceder a su contenido.

  Con un certificado digital podemos, entre otras cosas, tramitar becas y ayudas, presentar la declaración de la renta, consultar los puntos y las sanciones de tráfico y solicitar certificados.

1.4. Seguridad pasiva

La seguridad pasiva consiste en minimizar el impacto de un daño informático una vez que este se ha producido. Los principales mecanismos de seguridad pasiva 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 de 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.
- **Dispositivo NAS** (network area storage o sistemas de almacenamiento 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.
- **Política de copias de seguridad** (**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. No es recomendable hacer la copia de seguridad en el mismo disco duro en el que tenemos instalado el sistema operativo.

Las copias de seguridad se pueden realizar de forma automática en una unidad externa o en la nube. Para ello, es necesario un programa para crear copias de seguridad, como Cobian backup.

- **Sistemas de restauración.** En la mayoría de los Sistemas Operativos existe una opción para poder restaurar el equipo a un estado anterior. Esto es muy útil si por algún motivo, se ha instalado un programa que provoca fallos en el ordenador o se ha instalado algún virus en nuestro PC. Pero además de esta tarea, existe otra muy útil que traen los equipos nuevos, denominada **restauración a configuración de fábrica.** La restauración hace que el equipo se configure como venía de fábrica, eliminando cualquier programa y borrando todos los archivos que nosotros hayamos instalado y, por tanto, el equipo queda exactamente igual a como se encontraba el día que lo compramos. Evidentemente, lo primero que tenemos que hacer si optamos a esta tarea, es hacer una copia de seguridad de los archivos que sean importante para nosotros (fotos, archivos de texto, etc).

1.5. Identidad digital y fraude

A lo largo de la historia el ser humano ha desarrollado sistemas de seguridad que le han permitido comprobar en una comunicación la identidad de su interlocutor. En la mayoría de los casos este sistema de seguridad está basado en la identidad física de las personas, contrastada con el DNI. El problema es que en internet no existe ese contacto físico entre las personas. Para resolver este inconveniente se han desarrollado elementos de seguridad como las contraseñas, la criptografía o los certificados digitales.

En la seguridad informática lo más importante es proteger a las personas. Los daños a la máquina no dejan de ser daños materiales, pero los causados a las personas permanecen en el tiempo y trascienden a otros aspectos de la vida. La seguridad hacia las personas afecta también a su salud. Pensemos, por ejemplo, en las malas posturas al utilizar el ordenador o en los riesgos de adicción al ordenador.

Las amenazas más importantes para las personas en internet son:

- El acceso involuntario a información ilegal o perjudicial.
- La suplantación de la identidad en robos y estafas. Ya hablamos del **phishing**, delito informático que consisten en estafar a los usuarios haciéndose pasar por otra persona o entidad para robarles datos bancarios, claves,... El ejemplo más habitual es el de un correo electrónico que llega a un usuario suplantando la comunicación de un banco y pidiéndole las 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**, acoso consistente en amenazas, chantajes,... entre iguales a través de internet, el smartphone o los videojuegos.

Existen programas que facilitar el control parental del uso de Internet. Pueden limitar las búsquedas o permitir o bloquear el acceso a sitios web, controlar los programas de mensajería instantánea, establecer filtros según la edad del menor,...Por ejemplo, KidsWatch.

Todo lo que hacemos en Internet deja rastro, una huella digital. Toda esta información sobre nosotros constituye nuestra **identidad digital**. Debemos cuidarla, y las leyes nos ayudan a protegerla. Los certificados digitales nos ayudan también a protegerla y evitar los fraudes.

Pero la mayor protección está en nosotros, en nuestro sentido común al utilizar internet. Debemos actuar con **responsabilidad digital**.

1.6. Seguridad en internet. Protocolos seguros. IPV6 frente a IPV4

Hablar de seguridad informática es hablar de seguridad en Internet en la medida en que la mayoría de las amenazas y fraudes vienen a través de la Red.

Redes sociales y seguridad. Una red social es un sitio web 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. En relación con la seguridad tenemos que observar las siguientes cuestiones:

- Para poder acceder a las redes 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 nuestra 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 sociales 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.

Protocolos seguros. Como vimos en el tema 2, un **protocolo de comunicación** es un conjunto de reglas comunes que hacen posible la comunicación de un ordenador con otros. También estudiamos algunos de los protocolos más importantes, entre ellos:

- El **protocolo HTTP** (hypertext transfer protocol) es el que utilizan los servidores para enviar y recibir documentos a través de internet.
- El **protocolo TCP/IP** (transfer control protocol/internet protocol) es el que siguen los paquetes de información.

Existen dos versiones seguras de estos protocolos:

- **HTTPS** (hypertext transfer protocol secure). Es el protocolo que utilizan las conexiones seguras en Internet. Es un protocolo criptográfico seguro. El cifrado de estas páginas se basa en certificados de seguridad **SSL** (secure sockets layer), creando un canal de comunicación 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 y contraseñas.

  La confianza en el HTTPS está basada en una Autoridad de certificación superior que viene preinstalada en el software del navegador. El protocolo HTTPS es utilizado por navegadores como Google Chrome, Internet Explorer o Mozilla Firefox, entre otros. Los navegadores utilizan un icono en forma de candado en la barra de direcciones para indicar la existencia de un protocolo de comunicaciones seguro. Para saber si la página web que estamos visitando utiliza el protocolo HTTPS, y es por tanto, segura en cuanto a la transmisión de datos, debemos observar si en la barra de direcciones de nuestro navegador aparece “https” al comienzo en lugar de “http”.
- **IPv6** es la última versión del protocolo **IPv4**. Como ya estudiamos en el tema anterior el protocolo TCP/IP asigna a cada nodo de una red informática una dirección IP, que le identifica en la red. La dirección IP equivaldría a nuestro DNI.

  Entre las características más importantes del protocolo IPv6 están:

  - **La mejora de la seguridad**. IPv6 es un protocolo seguro ya que trabaja de forma cifrada. Si se intercepta una comunicación, la información no podrá ser leída sin antes descifrarla.

    Uno de los grandes problemas achacable a Internet es su falta de seguridad en su diseño base. Este es el motivo por el que han tenido que desarrollarse, por ejemplo, el **SSH** o **SSL**, protocolos a nivel de aplicación que añaden una capa de seguridad a las conexiones que pasan a través suyo.

    IPv6 incluye **IPsec**, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.
  - **Mayor espacio de direccionamiento.** El IPv4 asigna a cada dispositivo una serie de cuatro números (cada uno de ellos comprendidos entre el 0 y el 255). Pero el IPv4 sólo permite aproximadamente 4.000 millones de direcciones, insuficientes para el espacio de direcciones de Internet. El IPv6 amplía este

espacio de direcciones a una cantidad casi ilimitada: 340 sextillones de direcciones. Estas direcciones tienen una notación en ocho grupos de cuatro dígitos hexadecimales.

- **Mejora la movilidad o roaming.** El Ipv6 permite la conexión y desconexión automáticas de nuestro terminal de redes Ipv6 de manera que podemos viajar con él sin necesidad de otra aplicación informática que se encargue de esa función.

La propiedad intelectual y la distribución del software. El software, al igual que los libros y las obras musicales, teatrales o pictóricas, 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 de autor sobre la disposición y la 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. En relación con las licencias que los regulan existen diferentes tipos de software:

- **Software propietario.** El acceso a su código fuente no es libre, es decir, sólo se encuentra a disposición de su desarrollador y no se permite su libre modificación, adaptación o incluso lectura por parte de terceros. Puede ser:
  - **Software comercial**. Es comercializado por una empresa con ánimo de lucro. Por ejemplo, Windows 10 o Microsoft Office.
  - **Freeware**. Es software gratuito, pero no libre. Por ejemplo, Internet Explorer o Adobe Flash Player.
- **Software Libre**. Su código fuente está disponible, es decir, es código abierto. Se puede usar, copiar, modificar y redistribuir libremente.
- **Copyleft**. Es la licencia de uso que acompaña al software libre para poder ser modificado y distribuido.
- **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.

Redes P2P. Todo el software que el usuario utiliza o adquiere a través de las distintas vías disponibles (tiendas, descargas, internet,…) 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.

Un de las formas más extendidas para obtener software en la red son las **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 estos 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.