10 Redes de ordenadores y servicios de Internet

Redes de comunicación

A lo largo de la historia han ido apareciendo diversos mecanismos de comunicación cada vez más sofisticados. En la actualidad, el uso de la telefonía móvil e Internet son claros ejemplos de estos avances.

Internet es una red mundial de ordenadores que permite comunicarse y compartir información con todo el mundo. Su nombre procede de las palabras *INTERconnected NETworks*, es decir, redes interconectadas.

Las redes de ordenadores están presentes en todos los rincones de nuestra sociedad, desde los hogares hasta las grandes empresas. Su uso mejora nuestra calidad de vida y proporciona servicios tan variados como el acceso a Internet, intercambio de datos, comercio electrónico, conexión entre dispositivos, VoIP, gestión de la domótica en el hogar, etc.

Las nuevas tecnologías aportan muchos beneficios a los usuarios, pero también implican ciertos riesgos que afectan a derechos fundamentales como la privacidad, por lo que es necesario adoptar medidas de seguridad, especialmente cuando se trabaja en la red Internet.

Cuestiones sobre la lectura

1. Las redes se utilizan prácticamente en todos los ámbitos de la sociedad: empresas, centros de enseñanza, viviendas, etc.

   ¿Qué es una red? ¿Qué diferencia encuentras entre una red de ordenadores y una red social?

2. La finalidad de una red es compartir recursos entre equipos.

   ¿Qué recursos se comparten normalmente en una red?

3. Los dispositivos se pueden conectar mediante redes cableadas o inalámbricas.

   ¿Qué dispositivos de tu casa utilizan una red para comunicarse?

1 Fundamentos de las redes

Las telecomunicaciones se han convertido en uno de los principales motores del desarrollo económico de nuestra sociedad. Las redes de ordenadores y los servicios de Internet permiten superar distancias transmitiendo de forma instantánea voz, textos, datos, imágenes o vídeos a cualquier lugar del planeta que esté conectado. Por ello, es fundamental conocer cómo se lleva a cabo el proceso de comunicación, qué tipos de redes hay, cuáles son las tecnologías de acceso a Internet y las medidas de seguridad básicas que hay que adoptar al trabajar en red.

1.1. Proceso de comunicación

Desde sus orígenes, el hombre ha tenido la necesidad de comunicarse, utilizando desde el lenguaje hasta diferentes mecanismos que han permitido la comunicación a distancia, tales como el telégrafo o el teléfono. En la actualidad, se utilizan las redes de telecomunicaciones e Internet, que han pasado a ser elementos cotidianos en nuestras vidas.

Todo proceso de comunicación requiere un emisor, un mensaje y un receptor. El emisor transmite el mensaje al receptor a través de un canal.

Fig. 1. Elementos que intervienen en la comunicación.

En una red, los dispositivos son emisores y receptores al mismo tiempo y el canal es el medio por el que circulan los datos: cables, fibra óptica, ondas, etc.

Para que el proceso de comunicación sea efectivo, es necesario utilizar un protocolo, es decir, un lenguaje común o conjunto de reglas para que emisores y receptores puedan entenderse. En las redes se suele utilizar la familia de protocolos de Internet, TCP/IP.

1.2. Redes de ordenadores

Una red de ordenadores es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos que permiten enviar y recibir datos.

La principal finalidad de las redes es compartir información, recursos y ofrecer servicios a distancia, tales como la transmisión de voz, sonido, imágenes o vídeos de alta definición. La interconexión de redes, a través de Internet, facilita la disponibilidad y acceso a los recursos desde cualquier lugar y en cualquier momento.

Con los últimos avances tecnológicos, como el incremento de ancho de banda en las redes y el desarrollo de las conexiones inalámbricas, la tendencia es a desarrollar dispositivos móviles y portátiles cada vez más pequeños y sofisticados, capaces de comunicarse entre sí de forma inteligente y transparente al usuario. Estos dispositivos se caracterizan por su capacidad de procesamiento y comunicación en red, por lo que las posibilidades que ofrecen son prácticamente infinitas.

Fig. 2. Las redes comparten información, recursos y servicios.

2 Origen de las redes y modelos de referencia

A principios de 1980, las empresas descubren las ventajas de utilizar tecnologías de conexión, por lo que se produce un enorme crecimiento en la cantidad y tamaño de las redes de ordenadores. El inconveniente de esta gran expansión fue que cada fabricante utilizaba su propia tecnología, por lo que cada vez resultaba más difícil conectar redes que usaban especificaciones diferentes.

Para solucionar esta incompatibilidad entre redes, la Organización Internacional para la Estandarización (ISO) desarrolló el modelo de referencia OSI en 1984, con el objeto de normalizar el diseño de las redes para que pudieran conectarse entre sí. Este modelo es teórico, por lo que no está pensado para hardware o protocolos específicos, sino para establecer de forma clara las funciones y los procesos involucrados. A nivel práctico, uno de los modelos más difundidos es el modelo TCP/IP, que es la familia de protocolos en los que se basa la red Internet.

2.1. Modelo de referencia OSI

OSI, *Open System Interconnection*, es un modelo de interconexión de sistemas abiertos, que ayuda a fabricantes y empresas a crear redes compatibles, independientemente de la tecnología utilizada.

El modelo OSI divide la comunicación que se realiza entre dos equipos en siete niveles, a través de los que se envían los datos entre el emisor y el receptor.

A medida que los datos pasan de una capa a otra inferior, se encapsulan y se les añade información adicional. En cada capa del modelo OSI, las unidades de datos (PDU), con las que se trabaja, reciben nombres diferentes:

- Datos (Aplicación, Presentación y Sesión)
- Segmentos (Transporte)
- Paquetes (Red)
- Tramas (Enlace de datos)
- Bits (Física)

A continuación se especifican los diferentes niveles:

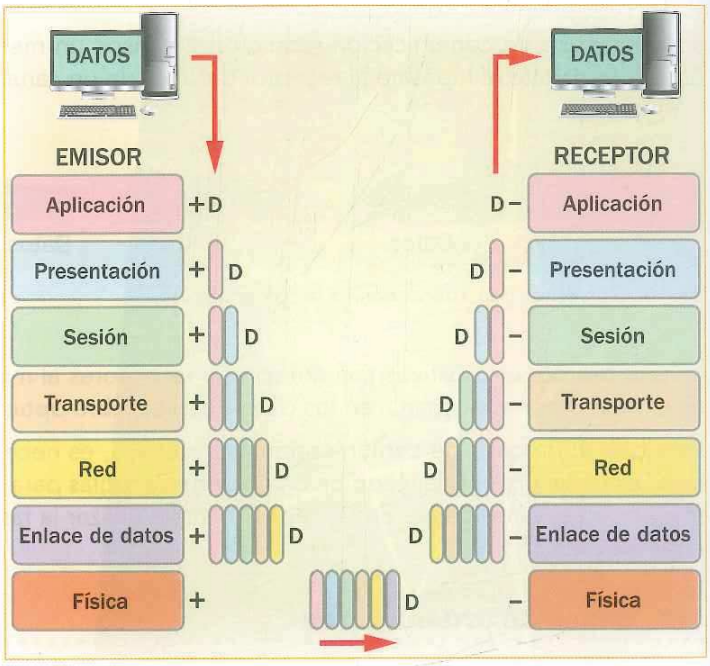


Fig. 3. Esquema de comunicación entre los niveles OSI de dos equipos remotos.

Capa	Nivel	Función
7	Aplicación	Suministra servicios de red a las aplicaciones de usuario. Algunos ejemplos son los navegadores de Internet, correo electrónico, aplicaciones VoIP, gestores de bases de datos, etc.
6	Presentación	Traduce los datos a un formato de representación común para que puedan ser accesibles y legibles en cualquier sistema.
5	Sesión	Establece, administra y finaliza las sesiones de comunicación entre los equipos que están conectados, sincronizando el intercambio de datos.
4	Transporte	Segmenta los datos del emisor y los vuelve a ensamblar en el receptor. Gestiona aspectos como la seguridad y calidad del servicio.
3	Red	Selecciona la ruta por la que se enviarán los datos por la red entre dos sistemas, que pueden estar ubicados en redes geográficamente distintas.
2	Enlace de datos	Controla el flujo de datos y los distribuye de forma ordenada. Se encarga de aspectos de la red como la topología, el acceso a la red, la notificación de errores, etc.
1	Capa física	Define las especificaciones eléctricas, ópticas, mecánicas y funcionales para realizar la conexión física entre sistemas finales. La información se transmite en secuencias de bits a través del medio.

2.2. Familia de protocolos de Internet: TCP/IP

Un protocolo es un conjunto de conductas, reglas y normas que deben seguirse en ciertos actos o con ciertas personalidades. Por ejemplo, en una ceremonia oficial hace referencia al vestuario de los invitados, a la programación, a las personas que intervienen, etc. En el caso de las redes informáticas, un protocolo es el conjunto de reglas que utilizan todos los dispositivos para ser capaces de comunicarse entre sí.

TCP/IP es la familia de protocolos en los que se basa la red Internet y que permiten la transmisión de datos entre ordenadores. Recibe este nombre en referencia a los dos protocolos más importantes que lo componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron dos de los primeros en definirse y los más utilizados de la familia. Algunos ejemplos del resto de los protocolos son HTTP *(HyperText Transfer Protocol)*, utilizado para acceder a las páginas web, FTP *(File Transfer Protocol)* para transferencia de archivos, SMTP *(Simple Mail Transfer Protocol)* y POP *(Post Office Protocol)* para correo electrónico.

Al igual que el modelo OSI, TCP/IP está formado por capas, en cada una de las cuales se emplean protocolos de comunicación distintos. Pese a no ser idénticas, las capas del modelo TCP/IP guardan analogías con varias de las capas o niveles OSI.

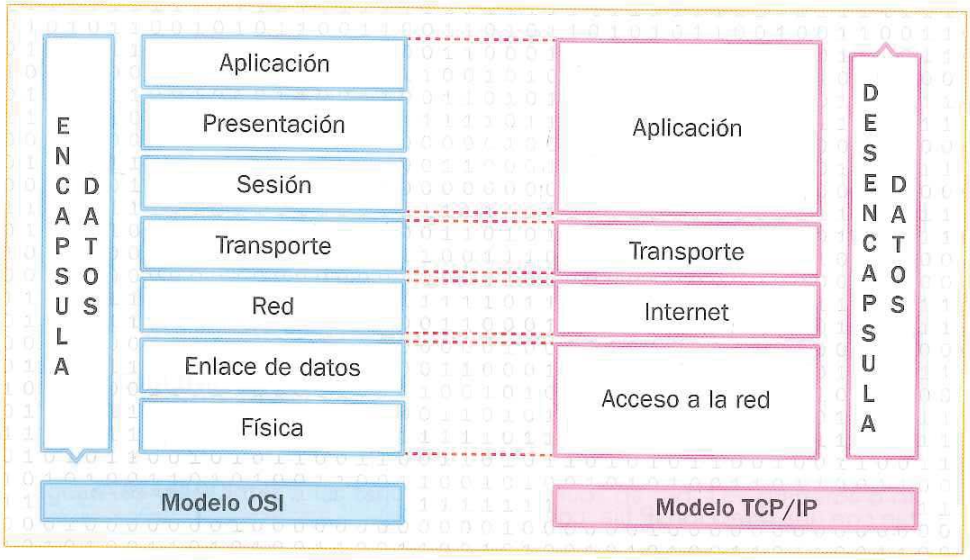


Fig. 4. Equivalencia entre las capas de los modelos OSI y TCP/IP.

Actividades

1. Imagina que asesoras a una empresa donde hay problemas de comunicación entre los empleados. Asistes a una de sus reuniones y observas que cada uno se dirige al resto en su idioma. Algunos de ellos levantan la voz más que el resto y gesticulan de forma inapropiada.

   Diseña un modelo de referencia que establezca las pautas adecuadas de comunicación en esta empresa. Para ello debes definir, al menos, las siguientes capas: mensaje a transmitir, idioma empleado, formas recomendables y canal (voz, gestos, papel, etc.).

2. Elabora una presentación sobre el modelo OSI. Puedes dedicar una o dos diapositivas a cada capa, especificando sus características, funciones, protocolos, etc.

3. Indica el nivel OSI en el que actúan los siguientes elementos: un repetidor, un cable de red, un hub, la app WhatsApp, un router, un switch y un navegador de Internet.

4. Haz una relación de los protocolos más importantes de las capas de OSI y TCP/IP.

3 Protocolo IP

IP es el protocolo de comunicación de datos de la capa de Red del modelo OSI, correspondiente a la capa Internet en el modelo TCP/IP, que se ha convertido en el estándar más utilizado en redes.

Las redes basadas en IP utilizan la tecnología de **conmutación de paquetes,** consistente en enviar la información dividida en bloques a la dirección IP del equipo destinatario. Los paquetes viajan por la red de forma independiente, incluso por caminos diferentes, ensamblándose nuevamente al llegar al destino.

La configuración de red se basa en el uso de direcciones IP y algunos parámetros adicionales como la máscara de subred, dirección MAC, grupo de trabajo, puerta de enlace y DNS.

3.1. Direcciones IP

La dirección IP es un código numérico que identifica de manera única a cada equipo en una red. Existen dos versiones de estas direcciones, que se diferencian por el número de bits que contienen y, por consiguiente, del número de dispositivos a los que se pueden asignar en la red:

- **Direcciones IPv4,** formadas por 4 bytes (32 bits). Para facilitar su representación suelen escribirse con 4 números, comprendidos entre 0 y 255, separados por puntos. Los ordenadores pueden tener cualquier dirección IP, excepto la acabada en 0 (dirección de red) y la acabada en 255 (dirección de broadcast). Las direcciones se clasifican en función del tamaño de la red donde se van a asignar. Por ejemplo, las redes que utilizan el rango de direcciones comprendido entre 0.0.0.0 y 127.255.255.255, se denominan de Clase A.
- **Direcciones IPv6,** formadas por 16 bytes (128 bits). Es una versión diseñada para reemplazar a IPv4, que ya no dispone de direcciones suficientes para asignar a la gran cantidad de dispositivos que se han ido sumando a Internet en los últimos años. Las direcciones IPv6 se escriben como ocho grupos de cuatro dígitos hexadecimales separados por dos puntos. Por ejemplo, 100e:03d1:0000:2351:ac10:882e:a371:1b3c. Los grupos de 4 dígitos formados por ceros se pueden comprimir del siguiente modo: 100e:03d1::2351:ac10:882e:a371:1b3c.

La configuración de las direcciones IP en los equipos se puede realizar de dos modos diferentes:

- **IP estática.** Los equipos se configuran con una dirección IP fija, con la que siempre acceden a la red. Los servidores de Internet emplean direcciones IP públicas y estáticas.
- **IP dinámica.** La dirección IP es asignada al equipo cada vez que se conecta a la red, siendo variable en cada sesión. Para ello, se utiliza el protocolo de red DHCP *(Dynamic Host Configuration Protocol)* que envía automáticamente los parámetros de red a cada equipo.

En una red con conexión a Internet hay que distinguir dos tipos de direcciones:

- **Direcciones públicas.** Permiten que cada dispositivo conectado a una red pueda ser identificado. Cuando un dispositivo se conecta a Internet, se le asigna una dirección IP de las que disponga su proveedor de acceso (ISP).
- **Direcciones privadas.** Son un conjunto de direcciones que se reservan para utilizarse en redes locales. Cada equipo de la red local tendrá una dirección IP privada diferente. Las direcciones reservadas para redes privadas son las que se muestran en el margen.

– **Clase A:** 10.0.0.0 a 10.255.255.255
– **Clase B:** 172.16.0.0 a 172.31.255.255
– **Clase C:** 192.168.0.0 y 192.168.255.255

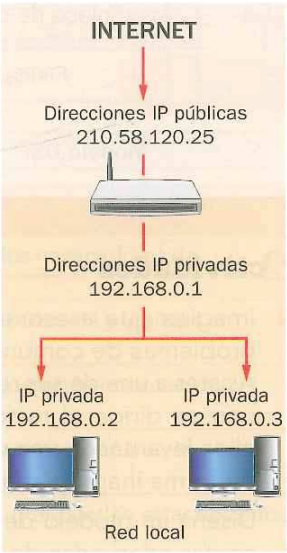


Fig. 5. Esquema de direcciones IPv4 públicas y privadas en una red de área local conectada a Internet.

3.2. Subredes

Una red se puede dividir en subredes para gestionar la seguridad, compartir los recursos, mejorar el tráfico de datos, controlar el acceso de usuarios, etc. Por ejemplo, un instituto que dispone de un solo router para acceder Internet puede crear una subred para el aula de Informática, otra para los departamentos y otra para la gestión administrativa.

Cada dirección IP identifica un equipo y la subred a la que pertenece. La máscara de red delimita con el valor «1» los bits de la dirección IP referidos a la subred y con el valor «0» los relativos al equipo.

Dirección IP	192.168.0.3	=	11000000	10101000	00000000	00000011
Máscara de subred	255.255.255.0	=	11111111	11111111	11111111	00000000
				Subred		Equipo

Fig. 6. La dirección IP 192.168.0.3 con máscara 255.255.255.0 identifica el equipo 3 dentro de la subred 192.168.0.x.

Máscara de red

Las máscaras de red varían en función del tipo de red que se está utilizando Clase A (255.0.0.0), Clase B (255.255.0.0) y Clase C (255.255.255.0). Para la configuración de redes locales se suelen utilizar direcciones IP privadas de clase C.

3.3. Puerta de enlace o Gateway

Una puerta de enlace es un dispositivo que permite interconectar redes con arquitecturas y protocolos diferentes. Un ejemplo característico es el router, ya que suele enlazar redes de área local con la red Internet. Se caracteriza por tener una dirección IP privada y otra dirección pública visible al exterior. La dirección IP utilizada habitualmente para la puerta de enlace suele ser 192.168.0.1.

3.4. DNS

El Sistema de Nombres de Dominio *(DNS, Domain Name Server)* es una base de datos distribuida por numerosos ordenadores de todo el mundo para convertir las direcciones IP en nombres de dominio, y viceversa. Cada vez que se utiliza una dirección web en Internet, como www.anaya.es, el DNS la traduce a la dirección IP correspondiente.

3.5. Dirección MAC

La dirección MAC, o dirección física, es un identificador único de 6 bytes que asignan los fabricantes a las tarjetas y dispositivos de red. Los primeros 6 dígitos hexadecimales hacen referencia al OUI, Identificador Único de Organización, por lo que son iguales para todos los productos de un mismo fabricante. Un ejemplo de dirección MAC es 2C:3F:32:AC:5F:B2.

Actividades

1 Abre la consola de tu sistema operativo y ejecuta la instrucción **ipconfig**, si utilizas Windows, o **ifconfig**, si utilizas Linux.

a) Indica cuáles de los siguientes parámetros de red se muestran: IPv4, IPv6, MAC, Puerta de enlace y DNS.

b) La dirección IPv4 que tiene asignada ¿es de Clase A, B o C?

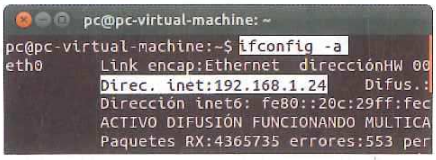


Fig. 7. Consola de comandos.

2 Escribe la siguiente pregunta en el buscador Google «Cuál es mi IP». ¿La dirección IP obtenida pertenece a tu equipo? ¿Es pública o privada?

4 Tipos de redes

Las redes se pueden clasificar atendiendo a diversos criterios, tales como su área de cobertura, topología, tecnología, funcionalidad, etc.

4.1. Según su área de cobertura

La clasificación más habitual suele ser la que distingue entre el tamaño o área de cobertura de una red, diferenciándose:

- **Red de área extensa (WAN, *Wide Area Network*).** Es una red que interconecta equipos de áreas geográficas muy amplias, tales como países o continentes. Las redes se conectan por cables, conexiones móviles y utilizando satélites de comunicaciones. El ejemplo más característico es la red Internet, formada por multitud de redes de diferentes tipos.
- **Red de área metropolitana (MAN, *Metropolitan Area Network*).** Es una red que da cobertura a extensiones de varios kilómetros o incluso regiones. Algunos ejemplos son las redes inalámbricas WiMAX, que dan cobertura a los habitatntes de una población.
- **Red de área local (LAN, *Local Area Network*).** Es el tipo de red más habitual, ya que conecta ordenadores en un área relativamente pequeña, como una habitación, una oficina, una casa o un edificio. Las redes LAN se conectan entre sí formando infraestructuras de tipo MAN y de tipo WAN. Las conexiones entre equipos se suelen realizar por cableado de red o por Wi-Fi.

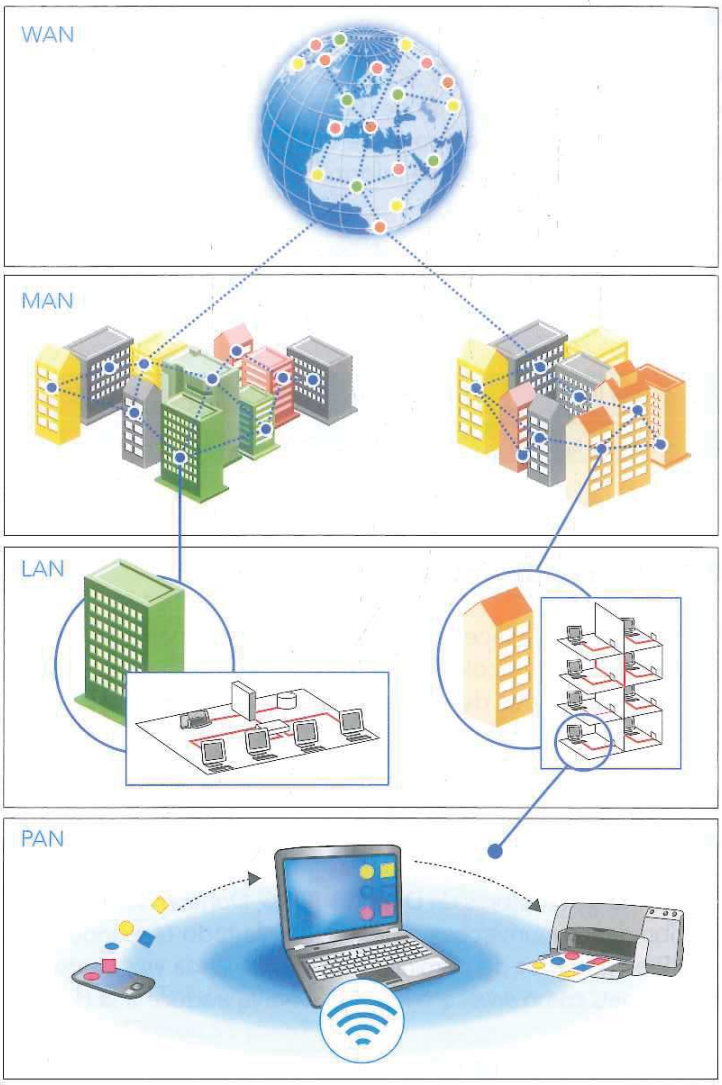


Fig. 8. Esquema de conexiones entre redes WAN, MAN, LAN y PAN.

- **Red de área personal (PAN, *Personal Area Network*).** Son redes que comunican diferentes dispositivos que están en un radio de pocos metros. Utilizan conexiones inalámbricas que varían según el uso: conexión de periféricos (Bluetooth, infrarrojos, Wireless USB...), aplicaciones de domótica (ZigBee, HomeRF...), microdispositivos (Wibree, RFID...), etc.

Cuando los dispositivos de estas redes se comunican de forma inalámbrica (Wireless), se antepone la letra W a su nombre, utilizándose términos como WLAN o WPAN.

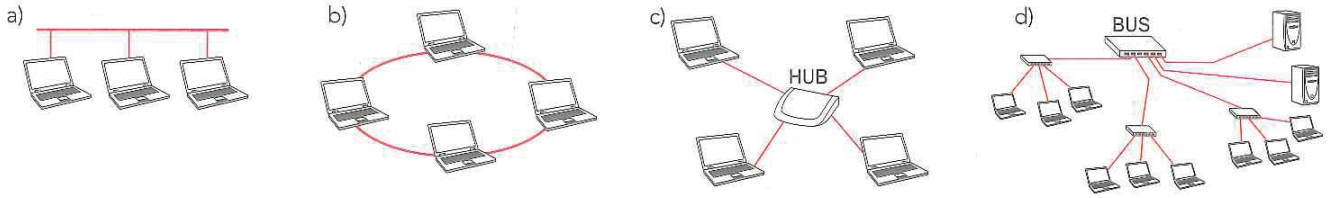
Actividades

1. Crea una presentación de diapositivas ampliando las características de cada una de estas redes. Puedes utilizar algún cuadro comparativo entre ellas.
2. Indica ejemplos de los diferentes tipos de redes, según su área de cobertura. Nombra las que sean próximas a ti o participes en ellas directamente.
3. Imagina que estás jugando a un videojuego en el que tienes que construir una ciudad desde cero. Indica las redes que crearías, justificando la utilidad de cada una de ellas.
4. ¿Qué tipo de redes se utilizan al enviar un email a un amigo que tienes al lado? ¿Y si está en Suecia?

4.2. Según su topología

La topología de una red hace referencia a la distribución física del cableado para la interconexión de los dispositivos. Algunos ejemplos son:

- **Bus.** Esta red, ya en desuso, se caracteriza por tener un único canal de comunicación al cual se conectan los distintos dispositivos. La circulación de toda la información por un mismo canal la convierte en una red lenta, puede quedar sin servicio en caso de rotura del cable principal.
- **Anillo.** Se trata de una red cerrada en la que todos los ordenadores están conectados a ella. La información circula en un sentido por el anillo y cada ordenador analiza si es el destinatario; si no lo es, dejará pasar la información al siguiente, y así sucesivamente. Si algún equipo de la red deja de funcionar, la comunicación se pierde en todo el anillo.
- **Estrella.** Los ordenadores están conectados directamente a un nodo central, a través de un dispositivo que suele ser un switch, hub o router. La rotura de uno de sus enlaces no influye en el funcionamiento del resto. Esta es la topología habitual de las redes de área local.
- **Árbol.** Es un conjunto de redes con una estructura jerárquica. Hay un nodo central que se va ramificando en diferentes nodos, simulando la forma de un árbol. Suelen usarse en sistemas de control, puesto que refleja la jerarquía de los diferentes niveles.
- **Híbrida.** Es una red heterogénea, formada por la combinación de distintas topologías de redes. Un ejemplo característico es la red Internet.



Red en bus | Red en anillo | Red en estrella | Red en árbol

Fig. 9. Tipos de redes según su tipología.

4.3. Según su nivel de acceso o privacidad

Según su nivel de acceso o privacidad, una red informática puede ser:

- **Red pública.** Se caracteriza por ser una red que puede utilizar cualquier persona para comunicarse, compartir información y acceder a sus servicios. Internet es una red de ordenadores pública que conecta diferentes subredes por todo el planeta.
- **Red privada.** Es una red con acceso exclusivo para los usuarios y equipos que la forman, por ejemplo, la red de una universidad. Cuando esta red proporciona servicios similares a los de Internet (páginas web, correo electrónico, FTP, etc.), a los que solamente pueden acceder sus usuarios, recibe el nombre de **Intranet.**
- **VPN (Red Privada Virtual).** Es una tecnología que utiliza la red pública Internet para acceder, de forma segura, a una red privada. El usuario que accede a la VPN, establece una conexión virtual cifrada con la misma funcionalidad, seguridad y política de acceso que si se estuviera físicamente en un equipo de la red. Se suele utilizar para administrar equipos de forma remota, para comunicar empresas, para teletrabajo, etc.

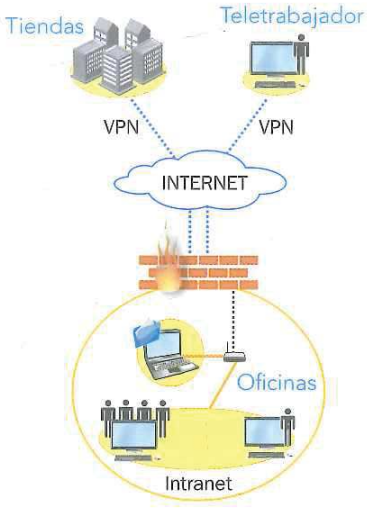


Fig. 10. Conexión entre una cadena de tiendas, teletrabajadores y las oficinas.

4.4. Según su relación funcional

Atendiendo a la relación que se establece entre los diferentes equipos de una red, se distinguen dos arquitecturas básicas:

- **Cliente-Servidor.** Son redes que se basan en la distribución de tareas, distinguiendo dos tipos de equipos en la red:
  - **Servidor.** Es un equipo de la red que provee servicios al resto de equipos, denominados clientes. Algunos de estos servicios son la gestión de usuarios, el almacenamiento, la conexión a Internet, el acceso a bases de datos, el correo electrónico, la impresión, la telefonía, etc.
  - **Cliente.** Son ordenadores que dependen, total o parcialmente, de los recursos de un equipo servidor, a los que acceden a través de la red.
- **Redes entre iguales *(P2P, Peer to Peer).*** Son redes que no diferencian entre clientes ni servidores, ya que todos los nodos se comportan como iguales entre sí. Los equipos actúan simultáneamente como clientes y como servidores respecto a los demás nodos de la red, permitiendo el intercambio directo de información en cualquier formato, entre los ordenadores interconectados. Algunos de los servicios más populares de este tipo de redes son el intercambio de archivos y la telefonía VoIP.
  - **Intercambio de archivos,** consiste en el envío y la recepción de documentos, de forma directa, entre los ordenadores de varios usuarios conectados a Internet. Estas redes se utilizan para compartir todo tipo de ficheros, como música, vídeos y software. Este intercambio se basa en la idea de que todos los usuarios deben compartir para poder descargar usando numerosas aplicaciones como **BitTorrent, eMule, Ares,** etc. El inconveniente de estas redes es que algunos usuarios las utilizan para intercambiar archivos cuyo contenido está sujeto a las leyes de los derechos de autor, lo que siempre ha generado gran polémica entre defensores y detractores de estos sistemas.
  - **VoIP,** es el servicio de telefonía IP utilizado para enviar voz digitalmente a través de la red Internet, con el consiguiente abaratamiento del precio de las llamadas o incluso de forma gratuita. El proceso es el siguiente: la señal analógica de voz se convierte en formato digital para poder ser traducida en paquetes IP que son enviados como datos a través de la red Internet. El dispositivo que recibe la llamada realiza la tarea inversa para obtener nuevamente la voz. Los modos más habituales de comunicación por VoIP se realizan utilizando:
    - **Un teléfono IP,** conectado a la línea fija de Internet y que tenga activado el servicio VoIP.
    - **Un móvil 4G o superior,** que tenga acceso a voz sobre LTE (VoLTE).
    - **Una aplicación o App,** que permita hablar a través de Internet como Skype, Google Hangouts, WhatsApp, LINE, Viber, Tango, ooVoo, etc.

Redes P2P y piratería

En las redes P2P se pueden intercambiar archivos propios o cuyo contenido no esté protegido con derechos de autor; en caso contrario, además de ser inmoral, se estaría incurriendo en un delito de piratería.

Actividades

5 ¿El aula de tu centro está diseñada con un modelo de arquitectura P2P o cliente-servidor? ¿Qué servicios no puedes utilizar si el servidor de tu aula está apagado?

6 ¿Conoces alguna aplicación para hablar, desde tu teléfono u ordenador, sin tener que pagar por el coste de la llamada? ¿El teléfono de tu casa utiliza VoIP?

7 ¿Consideras que los programas de intercambio de archivos fomentan la piratería?

Fig. 11. Teléfono VoIP que permite realizar videoconferencias.

4.5 Según su tecnología física de conexión

Dependiendo de la disposición física de los equipos y la tecnología de conexión que utilicen, se distinguen dos tipos de redes, que suelen combinarse entre sí:

- **Redes cableadas.** La conexión entre los ordenadores y los dispositivos de red (routers, switches, hubs, etc.) se realiza mediante cables. Existen varios estándares para redes cableadas, aunque el más extendido es Ethernet, que utiliza una topología en estrella y diferencia entre varios tipos de redes, según su velocidad:
  - **Fast Ethernet** o 100BASE-T, cuya tasa de transferencia de datos es de 100 Mbps.
  - **Gigabit Ethernet** o 1.000BASE-T, cuya tasa de transferencia de datos es de 1 Gbps.
  - **10 Gigabit Ethernet,** utilizada como redes troncales en aplicaciones que requieren tasas de transferencia muy altas, hasta 10 Gbps.

  El cableado empleado en estas redes suele ser par trenzado (UTP, STP o FTP), y fibra óptica, cuando se requiere mayor velocidad.
- **Redes inalámbricas.** Como su nombre indica, son redes que no requieren cables para establecer una conexión. En su lugar, la comunicación se realiza a través de ondas. Existen diversas tecnologías de comunicación inalámbrica para este tipo de redes, aunque las más comunes son por ondas electromagnéticas, microondas terrestres, microondas por satélite e infrarrojos.

  Las redes de área extensa y metropolitana suelen utilizar tecnologías WiMAX, LMDS, banda ancha móvil o por satélite, que se estudiarán en los siguientes apartados de esta unidad. En redes locales y redes PAN, algunas de las tecnologías de conexión son:
  - **Wi-Fi** *(Wireless Fidelity)* es una tecnología inalámbrica que realiza la conexión mediante ondas electromagnéticas que se propagan por las antenas de los dispositivos. Las características de la red dependen de la norma IEEE 802.11, que incluye varios estándares IEEE 802.11n, IEEE 802.11ac, etc. La conexión Wi-Fi se emplea para la comunicación y transferencia de información entre dispositivos que pueden estar alejados varios cientos de metros.
  - **Bluetooth,** es un protocolo estándar de comunicaciones entre dispositivos para la transmisión de voz y datos sin cable, mediante una radiofrecuencia segura en la banda de los 2,4 GHz. Permite realizar conexiones de corto alcance. Se utiliza en teclados, ordenadores, impresoras, cámaras digitales, manos libres, etc.
  - **Infrarrojos,** comunican dispositivos visibles entre sí, utilizando luz infrarroja, por lo que deben estar alineados directamente o con una reflexión en una superficie. Se usa habitualmente en mandos a distancia, dispositivos móviles y en algunos periféricos. Uno de los estándares más empleados en estas comunicaciones es el IrDA.

En la práctica, la señal de las redes cableadas se suele ampliar con redes inalámbricas. Para ello, se requiere un punto de acceso que funciona como puente entre las dos redes. Cuando la conexión se realiza directamente entre los dispositivos, sin requerir un punto de acceso, se denomina **ad hoc.**

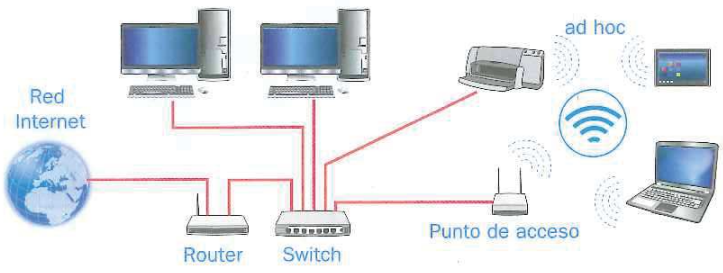


Fig. 12. Combinación de una red cableada y una red inalámbrica.

5 La red Internet

Internet, conocida como la «red de redes», es el conjunto de redes informáticas que se interconectan entre sí por todo el planeta. Las conexiones entre ordenadores se establecen por medio de la familia de protocolos de Internet (TCP/IP).

El acceso a Internet se realiza desde un ordenador u otro dispositivo conectado a través de un proveedor de servicios y, generalmente, utilizando un navegador. Existen diferentes tecnologías que permiten conectarse a Internet, tales como líneas ADSL, conexión móvil, WiMAX, etc.

5.1. Orígenes de Internet

Sus orígenes se remontan al año 1969, cuando la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de los Estados Unidos estableció la primera conexión entre ordenadores que se denominó ARPANET. El objetivo de esta red era descentralizar la información militar duplicándola estratégicamente, de tal manera que si cualquiera de los nodos de la red era destruido o dejaba de funcionar, el resto seguirían totalmente funcionales. Posteriormente, su uso se vincula a sectores académicos, científicos y gubernamentales. A inicios de los 90, con el auge de las nuevas tecnologías se inicia el desarrollo de lo que actualmente es la red Internet.

5.2. Servicios de Internet

La red Internet es una fuente de servicios prácticamente innumerables. En esta red es posible encontrar todo tipo de información, música, arte, cultura, medicina, literatura, ingeniería y mucho más. Por medio de texto, audio, vídeo, música e imágenes insertadas en sitios web, la red Internet permite a los usuarios aprender, comunicarse, divertirse, crear, interactuar, compartir, etc.

Los servicios que proporciona Internet eluden las diferencias sociales y las distancias, ya que permiten expresarse libremente, y propician que la información, el conocimiento y el mundo entero estén al alcance de todas las personas, por lo que ha pasado de ser una tecnología a convertirse en la base de la sociedad del conocimiento en la que vivimos.

Fig. 13. Servicios de Internet.

5.3. La web

La web está formada por un conjunto de sitios, aplicaciones y tecnologías diseñados para que los usuarios puedan interactuar y participar publicando sus contenidos, compartiéndolos con el resto de usuarios, buscando y recibiendo información de interés o colaborando.

Un **sitio web** es un conjunto de páginas web relacionadas entre sí y agrupadas alrededor de un dominio de Internet. La navegación a través de las distintas páginas que lo componen se realiza habitualmente por medio de enlaces o hipervínculos.

Las **aplicaciones web** suelen estar contenidas en los sitios web y su finalidad es la de ofrecer diferentes servicios. No requieren instalación, ya que los datos y los programas que los gestionan se alojan en servidores de Internet.

Algunas características comunes de las aplicaciones y sitios web actuales son: facilitar el intercambio de información, promover el diseño centrado en el usuario, eliminar barreras en el intercambio de datos entre aplicaciones y dotar a la red de significado.

5.4. Evolución de la web

Los avances tecnológicos y la generalización del uso de las redes por los usuarios, implican que Internet esté en constante evolución proporcionando nuevas aplicaciones y servicios. Algunos de los cambios más significativos han sido:

- **Web 1.0 o web estática.** Es una web que se limita a mostrar información y en la que el usuario tiene un papel pasivo, actuando meramente como observador.
- **Web 2.0 o web social.** Es una web dinámica, participativa y colaborativa, donde los usuarios se convierten en protagonistas activos, creando y compartiendo contenidos, opinando, participando y relacionándose. La web 2.0 se basa en el uso de blogs, wikis, foros, grupos sociales, etc.
- **Web 3.0 o web semántica.** Es una web inteligente, dotada de significado, que utiliza bases de datos, accesibilidad, inteligencia artificial, geoespacialidad y 3D. Permite el acceso y la interacción con la información de modo más eficiente y encuentra respuestas a las preguntas de forma rápida, clara y sencilla.

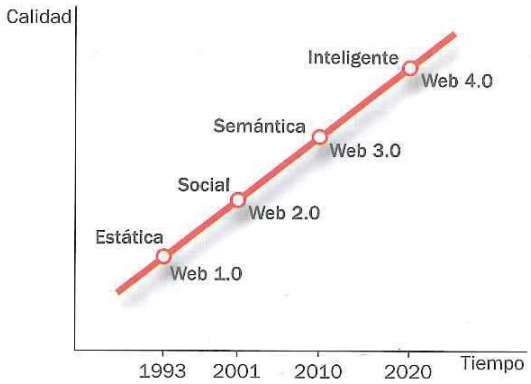


Fig. 14. Evolución de la web.

Actividad resuelta: Videoconferencia

1 Describe los principales servicios de la red Internet, tal y como se ha hecho con la videoconferencia:

La videoconferencia es un sistema de comunicación que permite mantener reuniones virtuales entre varias personas que se encuentran en lugares distantes. Esta comunicación se realiza en tiempo real y transmite, en ambos sentidos, tanto la imagen como el sonido. Los interlocutores se ven y se hablan como si estuvieran en un mismo lugar, incluso pueden intercambiar documentos, presentaciones, vídeos, etc.

Se puede realizar desde un terminal de videoconferencia, un ordenador multimedia o cualquier dispositivo móvil que tenga capacidad para ello.

Fig. 15. Videoconferencia con Skype.

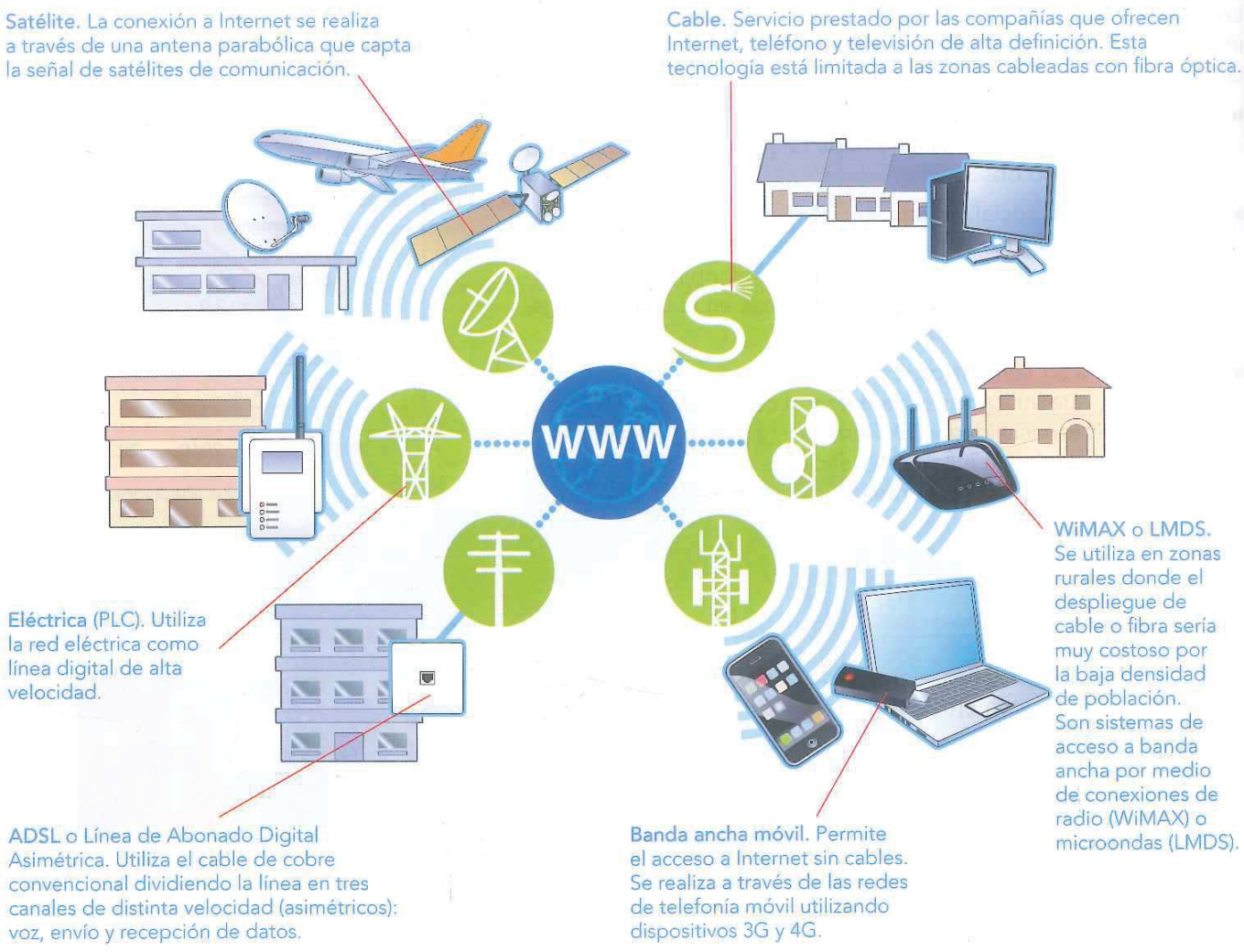
6 Tecnologías de acceso a Internet

Los usuarios se conectan a Internet a través de proveedores de acceso a Internet (**ISP**) que ofrecen diferentes servicios de comunicaciones y tecnologías de acceso. Estas tecnologías se clasifican en tres grupos según la infraestructura que emplean para transmitir la información:

- **Acceso cableado.** Requieren una conexión por medio de un cable hasta el terminal del usuario, siendo el punto de acceso a Internet fijo. Este es el caso de las tecnologías que utilizan la línea telefónica, fibra óptica y PLC.
- **Acceso inalámbrico.** La comunicación se produce de forma inalámbrica, a través de ondas electromagnéticas, por lo que el usuario debe estar dentro del área de cobertura de la señal. Algunos ejemplos son WiMAX, LMDS y los satélites de telecomunicaciones.
- **Acceso móvil.** Permiten gran movilidad del usuario, ya que la conexión se realiza a través de múltiples puntos de acceso a la red de telefonía. Entre estas tecnologías se encuentran UMTS (3G) y LTE (4G).

La elección de un proveedor suele realizarse en función de factores como el tipo de tecnología que oferta, la cobertura en el área del usuario, el ancho de banda, la calidad de la señal y el coste. El **ancho de banda** es la velocidad de transmisión de datos y se mide en Mbps (Megabits por segundo) o «Megas» en el lenguaje cotidiano.

Fig. 16. Acceso a la red Internet a través de diferentes tecnologías.



6.1. Línea telefónica

La línea telefónica fue creada para transmitir la voz humana. Al realizar una llamada, el teléfono traducía las ondas sonoras de la voz en impulsos eléctricos que se enviaban de forma analógica a través de los hilos de cobre de la red de telefonía básica (RTB). Actualmente, la línea ha evolucionado utilizando los pares de cobre para la transmisión de forma digital.

Los primeros accesos a Internet se realizaban a través de la línea telefónica RTC que, con la digitalización de las comunicaciones, evolucionó a la RDSI y, en la actualidad, a la popular ADSL.

- **RTC** (Red de Telefonía Conmutada). Utiliza la red de telefonía para establecer la conexión a Internet. Se realiza una llamada al servidor de Internet, a través de un módem, que transforma la señal digital del ordenador en analógica, para ser enviada por la línea telefónica, y a la inversa. La baja velocidad de esta tecnología, que alcanza un máximo de 56 Kbps, junto al hecho de no permitir el uso telefónico mientras se está conectado a Internet, propició la evolución hacia la RDSI.
- **RDSI** (Red Digital de Servicios Integrados). Envía la información codificada digitalmente, dividiendo la línea telefónica en tres canales: dos portadores por donde circula la información a la velocidad de 64 Kbps y un tercer canal para gestionar la conexión. Se pueden utilizar los dos canales de manera independiente (es posible hablar por teléfono por uno de ellos y conectarse a Internet por el otro), o bien utilizarlos de manera conjunta, lo que proporciona una velocidad de transmisión de 128 Kbps. No es necesario un módem para transformar la información en analógica pero sí un adaptador de red (módem RDSI o tarjeta RDSI) para adecuar la velocidad entre el PC y la línea. Este tipo de conexión ha evolucionado a la ADSL.
- **ADSL** (Línea de Abonado Digital Asimétrica). Tecnología que divide el cable de cobre convencional de la línea telefónica en tres canales independientes: envío de datos, recepción de datos y servicio telefónico tradicional. Los dos canales de datos son asimétricos, siendo generalmente de mayor velocidad el de recepción que el de envío de datos. La evolución de estas líneas a ADSL2 y ADSL2+ ha traído consigo nuevas versiones mejoradas de esta tecnología, con un aumento sustancial de las velocidades de transferencia que permiten ofrecer servicios como la televisión digital, música o vídeo de alta calidad a un precio razonable, convirtiéndose en uno de los tipos de conexión a Internet más utilizados.

Actividad resuelta

1 ¿Cuánto tiempo tardarán en descargarse 100 MB de Internet si la velocidad de la conexión es de 10 Mbps?

1 byte (B) = 8 bits (b)

$$\frac{100\ \text{MB}}{10\ \text{Mbps}} \cdot 8\ \text{bits} = 80\ \text{s}.$$

Actividades

1 ¿A qué hacen referencia la velocidad de bajada y la velocidad de subida que aparecen en la ilustración?

Fig. 17. Test de velocidad de una línea ADSL.

2 Realiza un test de velocidad para comprobar el ancho de banda del que dispones en tu equipo.

¿Cuánto tiempo tardarías en subir a la nube un archivo de 1 GB, utilizando las líneas anteriores?

3 Calcula el tiempo necesario para descargar un programa de 1,30 GB que está alojado en la nube, utilizando:

a) Una línea RTC.

b) Una línea RDSI con los dos canales dedicados a datos.

c) Una línea ADSL cuya velocidad de bajada es de 100 Mbps y la de subida de 15 Mbps.

6.2. Cable o HFC

La tecnología de acceso por cable utiliza redes **HFC** ***(Hybrid Fibre Coaxial)***, combinando fibra óptica y el cable coaxial como soportes de la transmisión de datos. Los proveedores de servicio de cable emplean cable coaxial para conectar el domicilio del abonado hasta un nodo zonal y fibra óptica para interconectar los nodos zonales. La fibra óptica proporciona la ventaja de cubrir distancias razonablemente largas con un mínimo de amplificación y regeneración de la señal. El cable coaxial proporciona una capacidad de ancho de banda considerable, utilizándose para dar servicio a muchos usuarios a la vez.

6.3. Fibra óptica hasta el hogar

La tecnología de telecomunicaciones **FTTH** ***(Fiber To The Home)***, también conocida como fibra hasta el hogar, se basa en la utilización exclusivamente de cables de fibra óptica para ofrecer acceso a Internet de banda ancha, telefonía y televisión. Son las redes más rápidas, pudiendo proporcionar hasta varios Gbps, debido a la gran capacidad de la fibra óptica para transmitir datos. Su uso está sustituyendo paulatinamente a los accesos tradicionales basados en cables de cobre.

6.4. Internet por satélite

La conexión por satélite es una más de las múltiples tecnologías de banda ancha que permiten tener acceso a Internet a alta velocidad. Debido a su elevado coste, su uso suele estar restringido a lugares remotos, especialmente en el ámbito rural y las zonas de alta montaña así como barcos y aviones, donde no se puede acceder con otros tipos de conexiones. Los datos se transmiten, en forma de ondas electromagnéticas, utilizando los satélites artificiales situados en órbita alrededor de la Tierra, por lo que el usuario utiliza un módem conectado a una antena parabólica.

6.5. WiMAX y LMDS

WiMAX y LMDS son tecnologías inalámbricas para el acceso a Internet, por ondas de radio, que se utilizan habitualmente en zonas rurales, residenciales o empresariales, donde el despliegue de cable o fibra sería muy costoso por la baja densidad de población.

- **LMDS** tiene una cobertura máxima de 35 km, aunque suele cubrir distancias de hasta 5 km y necesita visibilidad directa entre las antenas.
- **WiMAX** utiliza ondas electromagnéticas con cobertura de hasta 50 km y no necesita visibilidad directa entre las antenas, por lo que es el más empleado.

6.6. Red eléctrica

Sistema que proporciona el acceso a Internet a través de la red eléctrica. Es suministrado por algunas compañías eléctricas y su ventaja es que no requiere ningún tipo de instalación.

Es suficiente con colocar un adaptador **PLC** ***(Power Line Communications,*** Comunicaciones por Línea Eléctrica) en cualquier enchufe de la vivienda, ya que se utiliza la red eléctrica como línea digital de alta velocidad para la transmisión de datos, de la misma forma que la red Ethernet usa cables o la Wi-Fi el aire. Su uso permite, entre otras cosas, el acceso a Internet mediante banda ancha, la transmisión de vídeo de alta definición y el uso de telefonía IP.

6.7. Conexión por telefonía móvil

La conexión por medio de la telefonía móvil se agrupa en diferentes generaciones según su orden de aparición y prestaciones:

- **Primera generación (1G).** Los sistemas de comunicaciones móviles de primera generación representan el conjunto de estándares que emplean tecnologías analógicas. Se trataba de sistemas pioneros que introducían por primera vez una característica revolucionaria para los servicios de comunicación comerciales de los años 80, como era la movilidad. Además de la voz, estos sistemas permitían la transmisión de datos empleando módems analógicos convencionales, aunque con una capacidad muy limitada.
- **Segunda generación (2G).** Nace a principios de los años 90, con la digitalización de los servicios móviles de voz. Estos sistemas permitían la transmisión de datos a baja velocidad (desde 9.6 Kbps hasta 14.4 Kbps) y el intercambio de mensajes SMS entre usuarios. En Europa, el estándar más destacado es **GSM *(Global System for Mobile)***, basado en la conmutación de circuitos que mejoró sus servicios para dar lugar a **GPRS *(General Packet Radio Service)***, que utiliza conmutación de paquetes y se considera la generación 2.5G. El GPRS permite el uso de MMS, WAP, correo electrónico y navegación web, con velocidades de datos de hasta 114 Kbps. A partir de ese momento, el modo de facturación no se realiza por tiempo de conexión sino por volumen de datos transmitidos, y la evolución tecnológica facilita la aparición de nuevos estándares con mayor ancho banda, tales como **EDGE *(Enhanced Data Rates for GSM Evolution)*** que permite el uso de aplicaciones como vídeo y otros servicios multimedia.
- **Tercera generación (3G).** Está basada en el uso del sistema de comunicación **UMTS *(Universal Mobile Telecommunication System)***, que se caracteriza por sus posibilidades multimedia, velocidad de acceso a Internet elevada y transmisión de voz con calidad equiparable a la de las redes fijas. El término 3.5G se emplea para referirse a las nuevas versiones que ofrecen mejoras de capacidad, rendimiento y eficiencia del estándar UMTS, entre las que destaca **HSPA+ *(High Speed Packet Access)***, con tasas de transmisión de hasta 84 Mbps de bajada y 22 Mbps de subida.
- **Cuarta generación (4G).** Es el conjunto de tecnologías basadas completamente en el protocolo IP, siendo una red exclusivamente de paquetes de datos, frente a las generaciones anteriores que contemplan canales diferenciados para voz y datos. La comunicación por voz se realiza mediante VoIP. Las velocidades máximas de transmisión de datos están entre 100 Mbps para una movilidad alta y 1 Gbps para movilidad baja. Las dos variantes más conocidas de 4G son **WiMAX** y **LTE *(Long Term Evolution)***, que es la tecnología utilizada por la mayoría de operadoras de telefonía.

Actividades

4 Investiga cuál es la velocidad máxima para la descarga de datos de las diferentes tecnologías de acceso. Calcula el tiempo que tardaría en descargarse un vídeo de 1 Gbps, en cada caso.

5 Investiga y responde:

¿Para cuándo está previsto el lanzamiento de la generación 5G ? ¿Qué mejora con respecto a la 4G?

6 Completa la línea del tiempo con la fecha aproximada en que aparece cada una de las siguientes tecnologías:

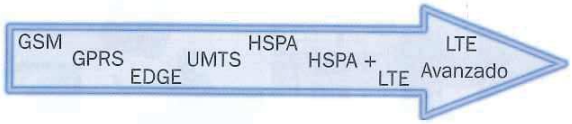


Fig. 18. Evolución de la tecnología móvil.

7 Configuración de una red

Una red es básicamente un grupo de dispositivos conectados con el objetivo de compartir información y acceso a Internet. Su configuración y diseño es muy variable, porque depende del entorno donde se va a instalar, la tecnología a emplear, los dispositivos que se van a conectar, la topología de la red a implementar, etc.

La configuración más común suele ser de una red de área local, que básicamente está formada por equipos conectados (ordenadores, periféricos, electrodomésticos, consolas, etc.) y el hardware de red necesario: router, switch, cables de red, etc.

7.1. Instalar y conectar los componentes

Los dispositivos que ofrecen la posibilidad de trabajo en red se pueden conectar entre sí de diferentes modos:

- Los dispositivos cableados como ordenadores, impresoras, electrodomésticos, etcétera, incluyen una tarjeta de red que hay que conectar al router o a un switch, en caso de no disponer de puertos suficientes. También es posible conectarlos a un adaptador PLC que los comunicará con el router a través de la red eléctrica.
- Los dispositivos inalámbricos no requieren ninguna instalación y es suficiente con realizar la configuración de su software de red.

A modo de ilustración, se muestra un ejemplo de la red que se establece entre los dispositivos de un hogar, donde se combinan diferentes tecnologías y tipos de redes.

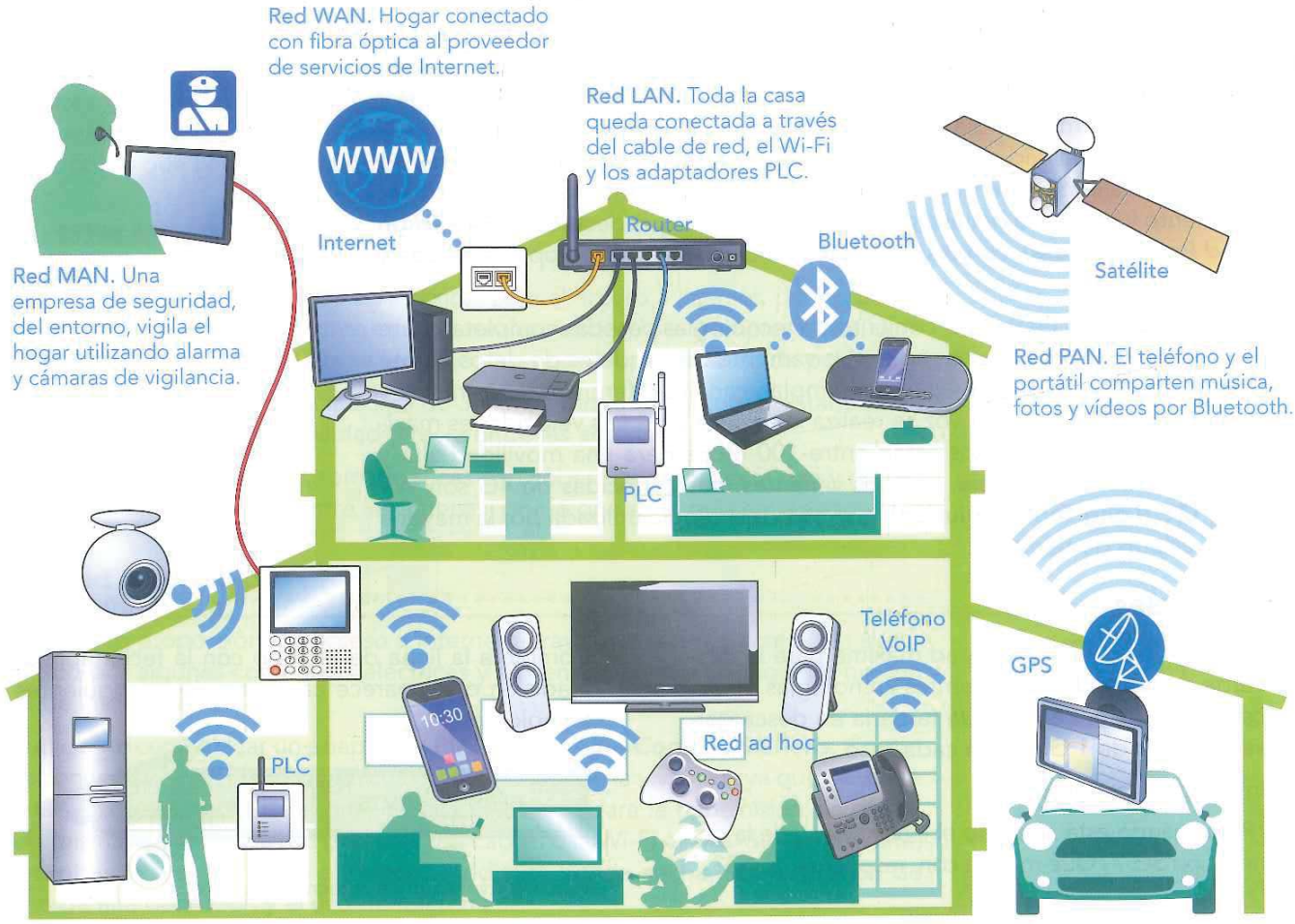


Fig. 19. Vivienda conectada en red, dotada de sistemas de domótica y electrodomésticos inteligentes.

7.2. Adaptadores de red

Una vez instalados los elementos que componen una red, el siguiente paso es configurar el software del adaptador o tarjeta de red. El sistema operativo establece, por defecto, la configuración **Automática (DHCP).** No obstante, en cualquier momento se puede cambiar a la configuración **Manual** o **Estática** para poder establecer los parámetros de red deseados. Para ello, se procederá de la siguiente forma:

1. Abrir las **Conexiones de red,** desde la **Configuración del sistema** o el **Panel de control.**
2. Hacer doble clic sobre la conexión cableada o inalámbrica deseada.
3. Editar los ajustes del **Protocolo TCP/IPv4** y elegir una de las siguientes opciones:
   - **Asignación automática.** Los datos de red son proporcionados por el servidor DHCP del router (opción habitual).
   - **Asignación de IP estática o manual.** Los datos de red (IP, máscara, DNS, etc.) son configurados manualmente.

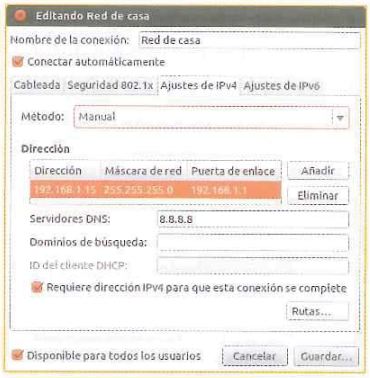


Fig. 20. Configuración de red en Linux.

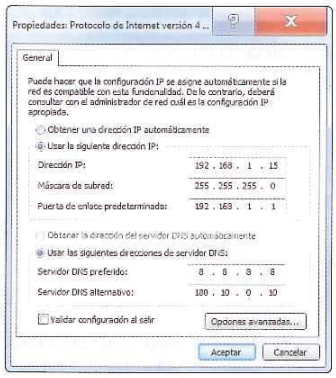


Fig. 21. Configuración de red en Windows

Actividades

Conexión a la WLAN con un dispositivo móvil

1 A continuación se muestran los pasos que se deben seguir para acceder con un teléfono inteligente a una red WLAN. Investiga cómo se puede acceder a una red que está oculta.

Fig. 22. Abre los ajustes Wi-Fi del teléfono.

Fig. 23. Elige la red a la que deseas conectarte.

Fig. 24. Elige DHCP y revisa los parámetros.

Fig. 25. Comprueba la conexión a Internet.

7.3. Router

Un router es el dispositivo que conecta redes de comunicaciones y proporciona acceso a Internet.

El proveedor de Internet (ISP) suele facilitar un router configurado para funcionar, aunque es interesante conocer algunos aspectos básicos para personalizar algunos ajustes de seguridad.

La configuración es diferente en cada modelo de router; no obstante, los pasos suelen ser bastante similares en todos ellos. El cambio de cualquier parámetro se ha de realizar con mucha precaución y previa consulta de un manual, ya que una configuración errónea podría provocar fallos en la conexión de Internet.

Acceder al router

Para acceder a la configuración del router, los pasos son:

1. Abrir el navegador de Internet y escribir la dirección IP del router.

2. Introducir el nombre de usuario y la contraseña de administración.

Configurar el servidor DHCP

El servidor DHCP asigna los datos de la configuración de red (entre ellos, la dirección IP) a los dispositivos que se conectan a la red utilizando la configuración **Automática.** Para ello, hay que especificar el rango de direcciones IP que pueden ser asignadas.

Si se deshabilita el servidor DHCP, los datos de red deben configurarse manualmente en cada dispositivo, especificando una dirección IP estática.

Cambiar el nombre de la red Wi-Fi y ocultarlo

El primer paso para poder acceder a una red es localizar su nombre. Este nombre se puede personalizar e incluso ocultar, para proteger la red de intrusos. Para ello:

1. Abrir la configuración referida a la WLAN.
2. Escribir el nuevo nombre de la red Wi-Fi en el campo **SSID.**
3. Activar la opción **Ocultar SSID,** si se desea ocultar. A partir de este momento no se muestra públicamente y solamente se podrán conectar a ella los usuarios que conozcan el SSID y configuren la conexión manualmente, utilizando la opción **Añadir red Wi-Fi.**

Encriptar la red

La red inalámbrica se puede configurar como abierta a cualquier usuario o protegida, siendo necesario introducir una clave si se desea acceder a ella.

1. Abrir la configuración referida a la **WLAN.**
2. Elegir el tipo de encriptación **WEP, WPA** o **WPA2.** Cada uno de estos protocolos estándares incrementa el nivel de seguridad.
3. Establecer la clave deseada en el campo **Key.** Es recomendable utilizar una combinación que incluya letras mayúsculas, minúsculas, números y símbolos para dificultar que pueda ser pirateada.

Recuerda

Apagar el router cuando no se utiliza. De esta forma se reducen las probabilidades de ataque contra la red inalámbrica y, por lo tanto, de su uso fraudulento.

Realizar auditorías. La revisión periódica de la actividad del router ayuda a identificar la conexión de usuarios no autorizados. Es posible ver los equipos que se han conectado a la red, la fecha y duración, etc.

Fig. 26. Barra de direcciones del navegador.

Fig. 27. Configuración DHCP.

Fig. 28. Ocultar nombre de la red y establecer nivel de seguridad.

Activar el filtrado MAC

La red puede ser protegida limitando el acceso a los equipos con una dirección MAC determinada. El proceso a seguir es:

1. Habilitar el filtrado MAC, dentro de las opciones de WLAN.
2. Escribir la dirección MAC de los adaptadores de red que pueden acceder a la red Wi-Fi, evitando así el acceso de equipos ajenos.
3. La dirección MAC suele aparecer en los ajustes del dispositivo. También se puede consultar en el terminal, utilizando los comandos ***ipconfig –all*** (Windows) o ***ifconfig -a*** (Linux).

Fig. 29. Filtrado MAC de dispositivos que pueden acceder al router.

Gestionar los puertos

Con algunos programas (especialmente clientes de descargas y juegos) es necesario abrir algunos puertos para que se establezca una conexión directa entre el ordenador y el servidor de Internet. La apertura de estos puertos puede poner en riesgo la seguridad del ordenador puesto que permiten ser utilizados por intrusos para infiltrarse en el equipo. Por esta razón es importante dejar abiertos solo los imprescindibles. Los pasos a seguir son:

1. Localizar la opción del menú adecuada para configurar los puertos del router.
2. En cada fila hay que especificar el puerto de inicio, el puerto final, el protocolo y el dispositivo en que se desea abrir el puerto.

Fig. 30. Router con los puertos 85 (TCP) y 1985 (UDP) abiertos.

Actividades

1. Comprueba la conexión de tu equipo con el router, con el equipo de algún compañero y con Google.
   a) ¿Cuál es la dirección MAC de tu tarjeta de red? ¿Qué parte de la dirección es común con la de tus compañeros?
   b) Averigua el camino que siguen los datos desde tu equipo hasta la web www.anaya.es.

Comprobar el funcionamiento de la red

Para comprobar que la configuración es correcta o, en su caso, diagnosticar problemas de conexión, es muy útil el uso de los siguientes comandos que se pueden ejecutar desde el terminal o símbolo del sistema.

Windows	Linux	Para qué sirven
ping <IP>	ping <IP>	Ping es un comando que envía paquetes de datos al dispositivo especificado y devuelve estadísticas sobre la recepción de los paquetes. Presionando Ctrl+C se detiene el envío.
ipconfig ipconfig /all	ifconfig ifconfig -a	Muestra la configuración básica de una red TCP/IP (IP, DNS, puerta de enlace, máscara de subred...).
tracert <IP>	traceroute <IP>	Indica la ruta que siguen los paquetes que salen del equipo hasta llegar al equipo de destino.

8 Compartir recursos

8.1. Compartir archivos y carpetas en Windows

En Windows, los archivos y las carpetas se pueden compartir con otros usuarios utilizando las opciones siguientes:

Carpetas públicas

La información que se copia en estas carpetas es accesible a todos los usuarios de la red. Para acceder a ellas, hay que:

1. Abrir el explorador de Windows y hacer clic en **Bibliotecas** del panel de navegación.
2. Hacer clic en la flechita que hay a la izquierda de cada biblioteca hasta ver las carpetas: *Documentos públicos, Música pública,* etc.

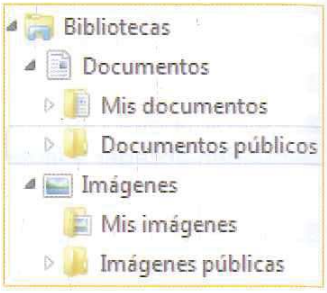


Fig. 31. Detalle del panel lateral del explorador de Windows.

Grupo en el hogar

Para compartir archivos o carpetas en la red doméstica, hay que:

1. Seleccionar el elemento que se va a compartir.
2. Hacer clic en el vínculo **Compartir con,** que aparece en la barra de herramientas de la ventana o en el menú contextual.

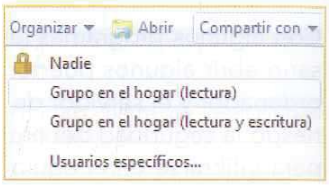


Fig. 32. Opciones del vínculo *Compartir con.*

Carpetas individuales compartidas

Para tener control sobre quién puede tener acceso a un archivo o carpeta en particular, se seguirán estos pasos:

1. Hacer clic con el botón derecho del ratón sobre el elemento a compartir y elegir la opción **Propiedades.**
2. Hacer clic en la pestaña **Compartir** y presionar el botón **Uso compartido avanzado.**
3. Seleccionar la casilla **Compartir esta carpeta** y hacer clic en **Permisos,** para permitir o denegar el control a los diferentes usuarios.

Para ver los equipos que hay en la red y qué recursos se están compartiendo en cada uno de ellos, se puede:

1. Abrir el explorador de Windows.
2. Hacer clic en el icono 

, del panel de navegación.

Actividad guiada: Compartir una impresora en la red

1. Abre el menú **Inicio** y haz clic en **Dispositivos e impresoras.**
2. Haz clic con el botón derecho del ratón sobre la impresora que deseas compartir y elige la opción **Propiedades de la impresora.**
3. Activa la pestaña **Compartir** y selecciona la casilla de verificación **Compartir esta impresora.**
4. Haz clic en **Aceptar** y comprueba que se puede utilizar la impresora desde cualquier equipo de la red.

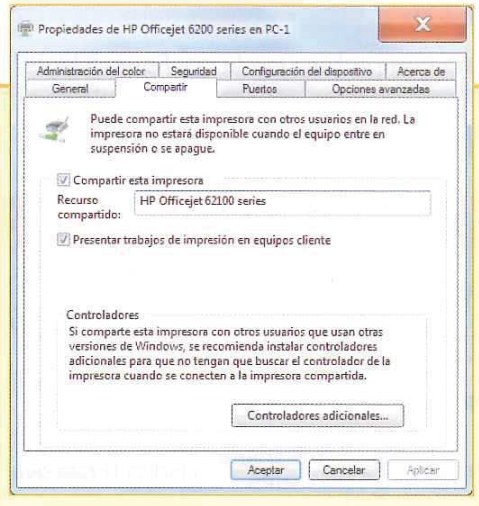


Fig. 33. Propiedades de la impresora.

8.2. Compartir recursos en distribuciones Linux

El sistema operativo asigna a cada cuenta de usuario una carpeta personal que contiene todos sus documentos, imágenes, vídeos, descargas, etc. Esta carpeta está dentro del directorio **/home**, junto con las del resto de cuentas.

Cada usuario Linux puede acceder a todos sus documentos y a los documentos compartidos por otros usuarios para los que se disponga de permiso.

Los recursos compartidos tienen asignados varios permisos: para el **Propietario** del recurso, para los usuarios que pertenecen al mismo **Grupo** del propietario y para **Otros** usuarios.

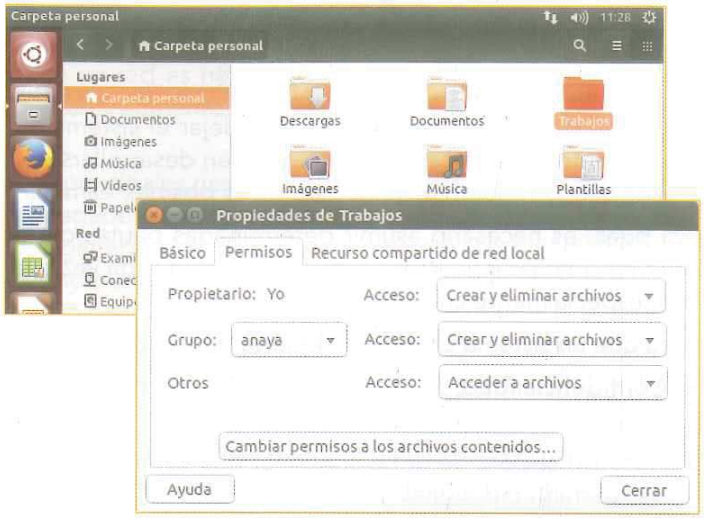


Fig. 34. Permisos que tiene atribuidos la carpeta **Trabajos**.

Recursos en la red

Los pasos para compartir una carpeta en la red son:

1. Hacer clic con el botón derecho del ratón sobre la carpeta que se desea compartir y elegir **Opciones de compartición.**
2. Presionar el botón **Instalar el servicio** que se muestra en el cuadro de diálogo si el servicio para compartir SAMBA no está previamente instalado.

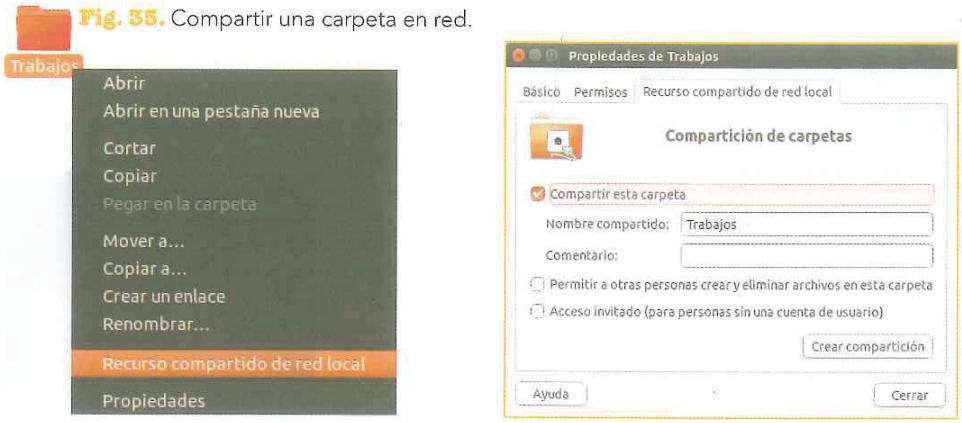


Fig. 35. Compartir una carpeta en red.

Fig. 36. Icono que identifica una carpeta compartida.

3. Activar la casilla de verificación **Compartir esta carpeta** y hacer clic en **Crear compartición.** La carpeta muestra dos flechas sobre ella, para señalizar que está compartida.

Actividad guiada: Acceder a los recursos compartidos

Para ver los equipos que hay en la red y qué recursos se están compartiendo en cada uno de ellos, realiza los siguientes pasos:

1. Abre el explorador de archivos.
2. Elige **Red** en el panel de navegación de la izquierda.
3. Haz doble clic sobre un equipo, para ver los recursos que comparte.
4. Seleccionar **Red de Windows** si se desea acceder a los equipos de la red que utilizan Windows.

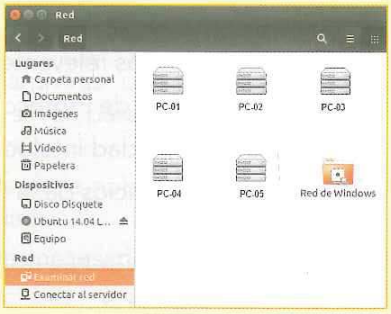


Fig. 37. Equipos en la red.

9 Seguridad en la red

Las redes de ordenadores constituyen el principal soporte de la comunicación entre usuarios, administraciones y empresas. Dada la enorme cantidad de información que circula por ellas, es necesario garantizar la protección de los datos y recursos.

El problema es que los sistemas informáticos son susceptibles de virus, accesos no autorizados, averías, etc. que pueden dejar el sistema inconsistente. Para poder hacer frente a todos estos factores, deben desarrollarse planes de seguridad integrales que permitan, en la medida de lo posible, eliminar los riesgos potenciales.

Así pues, es necesario asumir determinadas pautas de conducta y utilizar herramientas que garanticen una total tranquilidad cada vez que se utiliza un sistema en red, especialmente cuando se trate de Internet.

Para que un sistema en red sea seguro, debe cumplir las siguientes características:

- **Confidencialidad.** Solo deben tener acceso a los datos los usuarios autorizados para ello.
- **Autentificación.** Se debe confirmar que cada usuario es quien dice ser a través de su identidad digital.
- **Autorización.** El acceso a los diferentes servicios debe estar condicionado por la identidad y los permisos atribuidos a cada usuario.
- **Integridad.** Los datos enviados deben ser los mismos que los recibidos, evitando la manipulación o corrupción de estos en su recorrido.
- **Disponibilidad.** La disponibilidad es la característica, cualidad o condición de la información para estar a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

9.1. Amenazas a la seguridad

La seguridad de una red está expuesta a numerosas amenazas que se pueden agrupar en los siguientes tipos:

- **Causas humanas.** Son usuarios que, intencionada o accidentalmente, pueden dañar el sistema: usuarios inexpertos, piratas informáticos, espías, ingeniería social, etc.
- **Causas lógicas.** Es el software que puede atacar al ordenador: malware, correo basura, virus, errores de programación, etc.
- **Causas físicas.** Están relacionadas con fallos en dispositivos, interrupciones de suministro eléctrico, fenómenos meteorológicos, etc., que pueden dejar inoperativa la red.

Fig. 38. Las huellas en la red.

9.2. Legislación en la red

Existe legislación específica sobre el uso de las redes y los delitos informáticos. Algunas de las leyes más relevantes son:

- **LOPD,** Ley Orgánica de Protección de Datos.
- **LPI,** Ley de la Propiedad Intelectual.
- **LSSI-CE,** Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.
- **LAECSP,** Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- **Ley de Firma Electrónica.**

Información en la red

Cada vez que se realizan actividades en la red, como enviar un e-mail, subir un vídeo o una imagen a Internet, los servidores registran automáticamente datos como la IP, el navegador utilizado y el tiempo de permanencia. Esta información, generalmente utilizada con fines estadísticos, también es útil para desvelar la identidad de personas que cometen un delito en la red.

9.3. Adopción de medidas adecuadas

Al trabajar en red, no basta con tener soluciones de seguridad, sino que, además, es fundamental utilizar el sentido común para gestionar los recursos correctamente y realizar buenas prácticas. En cualquier sistema informático en red es necesario adoptar un conjunto de medidas para evitar o reducir las diferentes amenazas y sus efectos. Algunas de ellas, a diferentes niveles, son:

- **Protección.** Tradicionalmente, los virus han sido uno de los principales riesgos de seguridad para los sistemas informáticos que se han propagado a través de las redes informáticas. En los últimos tiempos, y debido al uso generalizado de Internet, han aparecido otras amenazas de malware *(malicious software)* que pueden resultar muy dañinas, tanto por causar pérdida de datos como por pérdida de productividad. Algunas medidas de protección son el uso de contraseñas robustas, permisos de acceso, cortafuegos, antimalware, conexiones seguras, etc.
  - **Antivirus.** Un antivirus es un programa que detecta, bloquea y elimina malware. Aunque se sigue utilizando la palabra antivirus, estos programas han evolucionado y son capaces de detectar y eliminar no solo virus, sino también otros tipos de códigos maliciosos como gusanos, troyanos, espías, etc. Algunos ejemplos de antivirus son Kaspersky, McAfee, Norton, Panda, Nod32, etc.
  - **Cortafuegos.** Un cortafuegos, o *firewall* en inglés, es un programa o dispositivo hardware que se utiliza para controlar las comunicaciones e impedir accesos no autorizados a un ordenador o a una red. Para ello, filtra los datos de la conexión dejando pasar solo los que están autorizados.
- **Recuperación.** Mecanismos empleados cuando el sistema ya ha sufrido algún daño. Si un sistema informático falla, los programas y los equipos se pueden reemplazar por otros nuevos, pero la única forma de recuperar los datos es recurriendo a copias de seguridad, réplicas en la red, almacenamiento en la nube, uso de servidores remotos, etc.
  - **Copias de seguridad.** Las copias de seguridad, en inglés *backup*, son duplicados de todos los datos que permiten recuperar la información original en caso de ser necesario. Las copias de seguridad se realizan en soportes de almacenamiento, como pueden ser discos externos, discos RAID, cintas, etc.
  - **Información en la nube.** La ventaja de estas copias de seguridad es que su acceso se puede realizar desde cualquier dispositivo y lugar. Su uso ya es habitual en dispositivos móviles con aplicaciones, como Dropbox, que almacenan automáticamente una copia de seguridad online cada vez que se guarda un archivo en el dispositivo, con un historial de versiones y la capacidad de poder recuperarlos.
  - **SAN** *(Storage Area Network).* Es una red de dispositivos que proporciona alta capacidad de almacenamiento a gran velocidad. Se suele utilizar para mejorar la protección de datos en redes empresariales.

Importancia de los datos

Los equipos y los programas se pueden reemplazar por otros nuevos, pero los datos no son sustituibles. Así pues, ante un problema grave en el ordenador los datos y la información se perderán, a no ser que se disponga de medidas de recuperación adecuadas.

Fig. 39. Teléfono inteligente protegido con el antivirus Avast.

Actividades

1. Indica qué medidas de protección y recuperación estás empleando para proteger los equipos que forman la red de tu hogar. ¿Consideras que son suficientes o deberías tener en cuenta alguna más?
2. ¿Con qué frecuencia realizas copias de seguridad de tu información? ¿Cuándo hiciste la última?
3. Enumera varios antivirus que conozcas y otras herramientas que sirvan para proteger o limpiar un equipo de malware.
4. Busca varios sitios de la nube que permitan alojar copias de seguridad.
5. ¿Consideras que es necesario proteger los móviles inteligentes?

9.4. Conexiones seguras y cifradas

La comunicación en red ofrece un amplio abanico de posibilidades tanto para ciudadanos como para empresas, ya que, además de comunicarse, permite comercializar productos y servicios.

Los usuarios se autentifican a través de su identidad digital, utilizando:

- **DNIe,** que acredita electrónicamente la identidad de la persona que lo utiliza. Para acceder a un sitio seguro con el DNIe, se inserta en el lector de tarjetas inteligentes y se introduce el PIN de seguridad.
- **Certificados digitales,** que autentifican a los usuarios, de forma similar al DNI. Los certificados suelen contener archivos que hay que instalar en el ordenador o utilizar desde una memoria USB, junto con una clave de seguridad que solamente conoce el usuario.

Por su parte, las empresas y demás organismos deben garantizar la seguridad en las comunicaciones, especialmente cuando se van a realizar transacciones relacionadas con el comercio electrónico, acceso a datos de carácter personal, gestiones administrativas, etc. Por ello, para acceder a sus sedes electrónicas, es importante verificar que se realizan conexiones cifradas **https** autentificadas con **certificados electrónicos.**

- **HTTPS** *(Hyper Text Transfer Protocol Secure).* Protocolo seguro de transferencia de hipertexto. Es la versión cifrada de HTTP y está diseñado para la transferencia de datos sensibles, resistiendo a ataques o accesos no autorizados. Hay que tener en cuenta que la información que se envía a Internet utilizando el protocolo **http** viaja en texto plano (legible para cualquier persona que lo intercepte), sin encriptar, con el riesgo que supone el envío de datos confidenciales como contraseñas, datos bancarios, mensajes, etc.
- **Certificado electrónico.** Documento digital mediante el cual una autoridad de certificación garantiza la autenticidad de la identidad del titular del documento, ya sea un usuario, una entidad, una empresa, etc. De ese modo, un certificado electrónico asegura que la entidad con la que el usuario se conecta es quien dice ser y ofrece una clave con la que se inicia una comunicación cifrada segura.

Para verificar la autenticidad del protocolo https se requiere un certificado emitido por una entidad autorizada. Los detalles del certificado se pueden consultar haciendo clic sobre el botón o candado que aparece en la barra de navegación.

Fig. 40. Conexión segura a la red social Facebook.

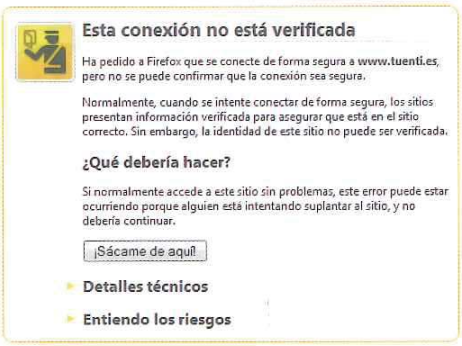


Fig. 41. Advertencia de conexión https no verificada.

Al navegar por una dirección no verificada, utilizando el protocolo https, se mostrará un mensaje de advertencia. En estos casos es recomendable no usar datos confidenciales.

9.5. Configuración segura del navegador

El navegador es una de las aplicaciones más utilizadas para acceder a multitud de servicios de Internet, pero al mismo tiempo también es uno de los principales elementos a considerar para la gestión de la privacidad o su uso seguro en la red.

Como recomendación general, aplicable a cualquier software que se encuentre instalado en el equipo, es muy importante mantener el navegador actualizado a la última versión estable (no en fase beta o de pruebas).

Los navegadores incluyen diferentes herramientas y opciones que permiten configurar el nivel de seguridad necesario para cada usuario. Algunas de estas características de seguridad y privacidad son:

- **Navegación privada.** Al elegir este modo, el navegador no guardará nada relacionado con el historial de navegación, las búsquedas, el historial de descargas, cookies o archivos temporales de Internet. Es recomendable activarla cuando se necesita un nivel de privacidad muy alto, por ejemplo al utilizar un ordenador de acceso público.
- **Filtro contra la suplantación de identidad *(Phishing)*.** Opción que se utiliza para que el navegador indique si la página que se está visualizando está intentando suplantar la identidad de otra. Un ejemplo son las páginas que imitan a las de entidades bancarias con el propósito de confundir al usuario y que este proporcione datos confidenciales para posteriormente realizar una estafa.
- **Bloqueador de elementos emergentes.** Evita que aparezcan ventanas con publicidad no deseada o *pop-ups* que, en algunas ocasiones, intentan infectar el ordenador con software malicioso.
- **Java/JavaScript.** Lenguajes que dotan a las páginas web de nuevas funciones y que, en ocasiones, pueden ser aprovechadas por los piratas informáticos para realizar alguna actividad maliciosa, robar información del equipo, etc.
- **Filtrado ActiveX.** Tecnología usada por los desarrolladores web para crear contenido interactivo en sus páginas, aunque también puede implicar un riesgo de seguridad. Es posible activar los controles ActiveX solamente para los sitios que son de confianza.
- **Configuración de las cookies.** Las cookies son pequeños archivos que se guardan en el ordenador con información sobre los usuarios para facilitarles la navegación cuando se visitan ciertas páginas de forma frecuente. El peligro es que sean utilizados con intenciones fraudulentas para conseguir información de los usuarios sin su consentimiento.

Otras de las herramientas que hay que tener configuradas adecuadamente a la hora de usar el navegador son: **Historial, Descargas, Configuración de los formularios, Gestión de contraseñas,** etc.

Actividades

6 Al acceder al sitio web de una sucursal bancaria o una tienda online, ¿cómo indica el navegador que se trata de una conexión segura?

7 Comprueba si se establece una conexión segura cuando accedes a tu correo electrónico. ¿Quién es la autoridad que lo certifica? ¿Está vigente o ha caducado?

8 Abre el navegador de Internet y localiza en qué menús se encuentran las opciones de seguridad.

Fig. 42. Configuración segura en Firefox.