Redes de ordenadores e Internet

AUTORES: Manuel Antelo Majado, Álvaro Añón Dosil y David Fernández Varela.

ÍNDICE:

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 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.

Procesos de comunicación

Desde siempre, el ser humano 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.

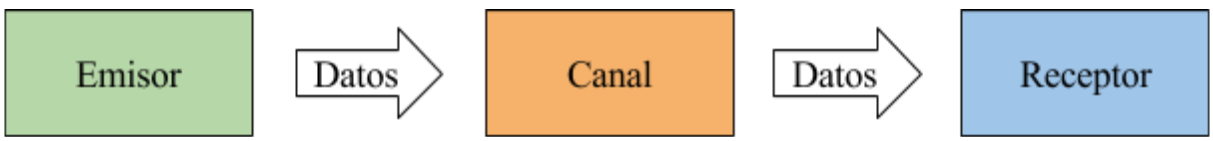


Figura 1. Elementos de la comunicación.

Redes de ordenadores

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

La principal finalidad de una red de computadoras es enlazar dos o más dispositivos para que exista comunicación entre ellos o para compartir información, recursos y ofrecer servicios a distancia, tales como la transmisión de voz, sonido, imágenes o vídeo 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.

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. De la misma forma en que las personas que no hablan un mismo

idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de conexiones propietarias. Una tecnología es llamada "propietaria" cuando está sujeta a un copyright. Esto supone que una empresa controla esta tecnología y las empresas que quieran utilizarla en sus sistemas tienen que pagar derechos por su uso. Las tecnologías de conexión que respetaban reglas propietarias de forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes o incluso con las que usaban reglas de conexión copyleft.

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.

Método 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).

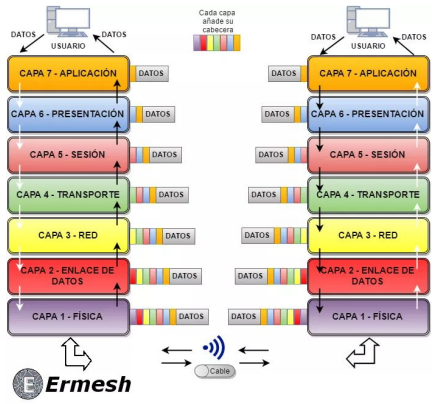


Figura 2 Capas del modelo OSI. Recuperado de: http://www.ermesh.com/modelo-osi-parte-1-aspectos-generales/

A continuación se especifican los diferentes niveles:

Capa	Nivel	Función
7	Aplicación	Suministra servicios de red a las aplicaciones de usuario. Algunos ejemplos son los navegadores de Internet, correo electrónico...
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 calidad del servicio.
3	Red	Selecciona la ruta por la que se enviarán los datos por la red entre dos sistemas.
2	Enlace de datos	Controla el flujo de datos y los distribuye de forma ordenada. Topología, acceso a la red, notificación de errores, etc.
1	Capa física	Define las especificaciones eléctricas, ópticas, mecánicas y funcionales para realizar la conexión física entre los sistemas finales. Secuencias de bits a través del medio.

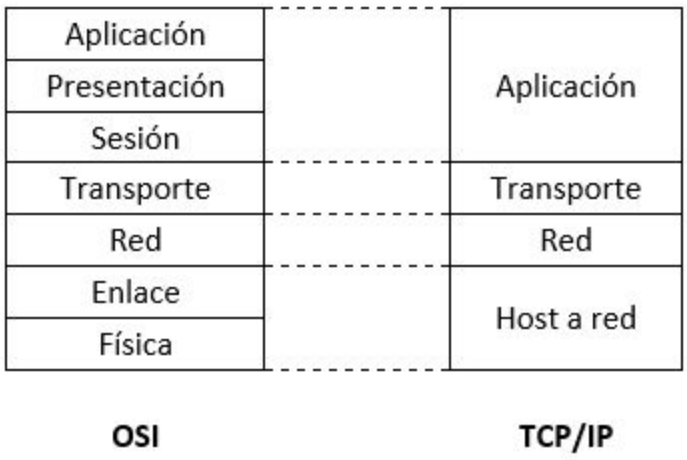
Tabla 1. Capas del modelo OSI.

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 rede 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 dos de 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.



Protocolo IP

Direcciones IP

IP (*Internet Protocol*) es el protocolo de comunicación de datos de la capa de Red del modelo OSI, que se corresponde a la capa Internet en el modelo TCP/IP, la cual es la más estandarizada en las redes.

Las redes basadas en IP utilizan la tecnología de conmutación de paquetes, que consiste en enviar dividida en bloques la información a la dirección IP del equipo destinatario.

La configuración de red se basa en el uso de direcciones IP y algún que otro parámetro adicional como la máscara de subred, puerta de enlace y/o DNS.

Direcciones IPv4. Están formadas por 4 bytes (32 bits). Estas direcciones acostumbran escribirse con 4 números comprendidos entre 0 y 255, pero nunca acaban en estos, ya que el 0 es la dirección de red y el 255 la de broadcast. Las direcciones se clasifican en función del tamaño de la red donde se van a asignar, yendo desde la clase A hasta la clase E. La clase A es para redes muy grandes, la B para medianas y la C para, por ejemplo, comercios pequeños. En cuanto a la D, es utilizada para los multicast, mientras que la E se utiliza únicamente para propósitos experimentales.

Direcciones IPv6. Están formadas por 16 bytes (128 bits). Su razón principal de existencia es la de reemplazar a las IPv4, pues ya no dispone de direcciones suficientes para albergar al número constantemente creciente de dispositivos que se van sumando a Internet.

Estas direcciones se escriben como ocho grupos de cuatro dígitos hexadecimales separados por dos puntos. Cada bloque va desde 0000, hasta FFFF. En este tipo de direcciones los 0 iniciales se pueden obviar, por ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> 2001:123:4:ab:cde:3403:1:63 También se pueden comprimir los bloques contiguos de 0 usando ":", por ejemplo: 2001:0:0:0:0:0:0:4 -> 2001::4.

Existen dos modos de configuración IP:

IP Estática. Los equipos son configurados con una IP fija, con la que siempre acceden a la red. Los servidores de Internet emplean direcciones IP públicas y estáticas. Mucha gente confunde IP fija con IP pública, pero una IP puede ser pública o privada independientemente de si es estática o dinámica.

IP Dinámica. La IP dinámica consiste en el cambio de IP cada vez que el equipo se conecta a la red, variando en cada sesión. Generalmente este tipo de IP son privadas y están restringidas por un servidor DHCP (Dynamic Host Configuration Protocol) que automáticamente envía a cada equipo los parámetros de red.

Es recomendable tener una IP dinámica, ya que tener una IP fija hace que seamos un mejor blanco para los piratas informáticos, pues estos sabrán que el equipo se encuentra en una dirección precisa y les permite tener más tiempo para preparar un posible ataque.

Direcciones Privadas. Son un conjunto de direcciones que prácticamente solo se usan para redes locales. Estas son usadas por los hosts que utilizan NAT (Network Adress Translation) o traducción de dirección de red conectándose a una red pública. También pueden usarse por hosts que utilizan una conexión local. Las direcciones privadas son las siguientes:

Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).

Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.

Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet.

Direcciones Públicas. Es la asignada a cualquier dispositivo o equipo conectado directamente a Internet, permitiendo identificar cada dispositivo conectado a la red. Las direcciones públicas son irrepetibles, es decir, únicas. En cambio dos equipos con IP de este tipo pueden conectarse directamente entre sí, como por ejemplo tu router con un servidor web.

Subredes

Es posible dividir una red en subredes para poder gestionar su seguridad, controlar el acceso de usuarios, mejorar su tráfico de datos etc y así hacer la red más manejable. En el caso de, por ejemplo, un instituto que únicamente tiene solo un router, se puede crear una subred para el aula de profesores, otra para la de informática y otra para el aula de plástica.

Una dirección IP por sí sola no es suficiente para identificarnos en la red, si no que es necesario acompañarla con la máscara de subred, que a efectos prácticos es otra dirección IP, con la diferencia de que su numeración va a estar casi siempre compuesta por 0 y 255. Por ejemplo: Si en casa tenemos tres dispositivos conectados a Internet y sus IP son 191.167.2.3, 191.167.2.4 y 191.167.2.5 vemos que los 3 primeros números son iguales, pero el último cambia. Pues es con la máscara de subred como identificamos esa parte fija de la IP, marcando la parte que no varía con 255 y la variable con 0. Siguiendo el ejemplo anterior, la máscara de subred de esta IP sería 255.255.255.0.

Puerta de enlace o Gateway

Una Gateway es un dispositivo que habilita la interconexión de redes con arquitecturas y protocolos diferentes. El ejemplo más claro es el router, pues es la "puerta" de acceso a internet, ya que suele enlazar redes de área local con la red de Internet. El router, al igual que el resto de dispositivos, posee una IP interna, la cual debemos conocer para configurar nuestros ordenadores, móviles etc. Así cada vez que nos pidan la Gateway tendremos que poner la IP de nuestro router para indicarle a nuestro ordenador a dónde tiene que ir para conectarse a internet.

DNS

El sistema DNS (*Domain Name System*) o sistema de nombre de dominios es una tecnología basada en una base de datos cuya función principal es para la dirección IP de la máquina donde está alojado el dominio al que queremos acceder. Cuando un equipo está conectado a una red con pocos ordenadores es sencillo tener memorizadas las direcciones IP

de cada uno, pero en el caso de que haya millones de dispositivos, cada uno con una IP diferente, sería imposible. Por esta razón existen los dominios y las DNS para traducirlos. Por ejemplo, si la IP de google es 209.85.195.104, la mayoría de la gente no llega a este sitio utilizando dicha IP, si no especificando www.google.es. A parte de que el nombre es más fácil de recordar que la IP, también es más fiable, ya que la dirección numérica puede cambiar.

A la hora de hablar de DNS debemos diferenciar las 3 partes por las que está compuesto:

Cliente DNS. Realiza peticiones de resolución de nombres a los servidores DNS. Está instalado en el cliente, es decir, nosotros.

Servidor DNS. Contesta la petición de los clientes. Algunos servidores tienen la capacidad de reenviar la petición a otro servidor en el caso de no disponer la solicitada.

Zona de autoridad. Son servidores o grupos de ellos que resuelven un conjunto de dominios determinado, pudiendo tener autoridad en varias zonas. Por ejemplo .org, .net, etc.

Dirección MAC

La dirección MAC (*Media Acces Control*) es un identificador único de 6 bytes asignado por el fabricante a una pieza de hardware de red. Se conoce también como dirección física y es única para cada dispositivo. Los últimos 24 bits están determinados y configurados por fabricante utilizando el OUI (Identificador Único de Organización), mientras que los primeros 24, por el IEEE. Un ejemplo de dirección MAC es 2C:3F:32:AC:5F:B2 (cada bloque hexadecimal son 8 dígitos binarios).

Tipos de redes

Las redes pueden ser clasificadas de diferentes maneras si atendemos a diversos factores como son: la área de cobertura, la tipología, el nivel de acceso o privacidad, la relación funcional, la tecnología física de conexión o las redes inalámbricas.

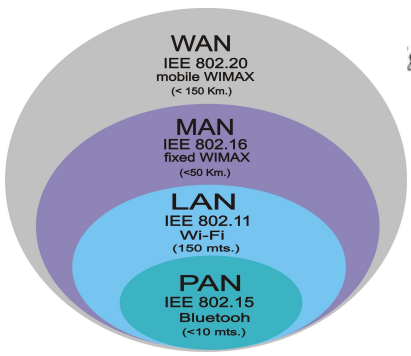
Según su área de cobertura

Red de área extensa, WAN. Tiene una gran capacidad geográfica (como pueden ser distintos continentes). Al comprender distancias tan grandes, la velocidad es menor que la de las otras redes pero, la información que maneja es mucho mayor. La conexión es realizada a través de fibra óptica o satélites. La WAN más conocida es Internet.

Red de área metropolitana, MAN. Red que conecta equipos situados a varios kilómetros o incluso regiones a alta velocidad. Un ejemplo de MAN es la WiMax, que da cobertura a varios equipos de un municipio.

Red de área local, LAN. Red que conecta equipos de una área geográfica limitada como pueden ser una casa o una oficina. Esta conexión es rápida y sin inconvenientes. Estas conexiones suelen ser realizadas a través de cableado o Wi-Fi.

Red de área personal, PAN. Red conformada por una pequeña cantidad de equipos situados a unos pocos metros de velocidad. Utilizan conexiones inalámbricas variadas como puede ser las periféricas (Bluetooth, infrarrojos, etc), las de uso domótico (ZigBee, HomeRF, etc), para microdispositivos (Wibree, RFID,etc)...



gura 3. Redes según su área de cobertura

Según su tipología

Bus. Red en desuso que se caracteriza por estar conectada a un mismo canal de comunicación. Esta razón la convierte en una red lenta y con una gran inestabilidad ya que si rompe el cable principal puede quedarse sin conexión .

Anillo. Red donde todos los equipos están conectados a la misma red cerrada. La información circula en forma de anillo y va pasando por todos los ordenadores hasta llegar al adecuado. Si algún equipo deja de funcionar, el anillo acaba fallando.

Estrella. Red donde los equipos están conectados a un mismo nodo, a través del cual puede ser un hub, un switch o un router. La ruptura de uno no influye en el resto. Esta es la tipología habitual de las LAN.

Árbol. Red parecida a la de estrella con la diferencia de que no tiene un nodo central. Tiene varios switch o hubs que imparten información a cada red en forma de estrella. Suele usarse en sistemas de control los cuales tienen varios sistemas jerárquicos.

Híbrida. Red heterogénea formada por la combinación de distintas topologías. Un ejemplo característico es Internet.

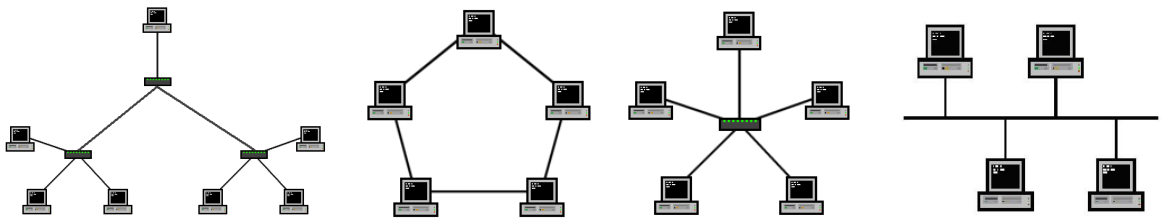


Figura 4. Redes según su tipología: Bus, Anillo, Estrella, Híbrida.

Según su nivel de acceso o privacidad

Red pública. Red de acceso público y que permite a cualquier persona comunicarse y compartir información. Un ejemplo es Internet, que permite a cualquiera persona del mundo conectarse.

Red privada. Red de acceso restringido ya que solo la pueden usarla aquellas personas que lo forman , como una oficina. Cuando se utiliza Internet se denomina Intranet.

VPN (red privada virtual). Red que usa Internet para acceder de forma segura a una red privada. Se usa para administrar equipos, para comunicar empresas, para teletrabajo, etc.

Según su relación funcional

Cliente-servidor. Redes que se basan en la distribución de tareas. Se distinguen dos:

Servidor: equipo de red sirve servicios a los demás equipos denominados clientes. La conexión a Internet, la impresión, la telefonía o el correo electrónico son algunos ejemplos.

Cliente: equipos que dependen totalmente de un servidor a los que se conectan a través de la red.

Redes entre iguales (P2P, Peer to Peer). Red de ordenadores que funcionan sin clientes ni servidores sino que funcionan con una serie de nodos que se comportan de formas iguales. Es decir, actúan simultáneamente como servidores y clientes respecto a los nodos de la red. Estas redes permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados. Algunos de estos son:

Intercambio de archivos: envío y recepción de documentos entre ordenadores conectados a Internet. Se utiliza de intercambio entre todo tipo de documentos: música, vídeos, etc. Este

sistema se basa en compartir información para que los usuarios tengan que descargar aplicaciones (Ares). Lo malo de este sistema es que a veces se comparten documentos a fuera de las leyes como fotos con derechos de autor.

***VolP*:** sistema de telefonía IP que permite enviar voz digitalmente, abaratando o incluso volviendo gratis las llamadas telefónicas. En esta llamada, la señal analógica de voz se convierte en digital y son traducidas en paquetes IP enviadas por Internet. El dispositivo que recibe la llamada hace la tarea inversa. Los mods más utilizados son:

Teléfono IP: conectado a Internet y teniendo activado el servicio VolP.

Móvil 4G o superior: teniendo acceso a voz LTE.

Una aplicación o app: permite hablar a través de internet como Skype, Hangouts, etc.

Según su tecnología física de conexión

Redes cableadas. Conectan ordenadores y dispositivos mediante cables. Existen varios estándares de redes cableadas pero el más conocido es Ethernet, que utiliza una topología en estrella y diferencia en varios tipos de redes según su velocidad:

Fast Ethernet o 100 BASE-T: su tasa de transferencia es de 100 Mbps.

Gigabit Ethernet 0 1000 BASE-T: su tasa de transferencia es de 1 Gbp.

10 Gigabit Ethernet: la más utilizada, su tasa de transferencia es de 10 Gbps.

Figura 5. Redes según su tecnología física de conexión: Redes cableadas

Redes inalámbricas. Aquellas que no necesitan cables para establecer conexiones sino que se realiza a través de ondas. Las más utilizadas son.

Wi-fi: tecnología de transmisión inalámbrica por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m). Se encuentra estandarizado por la IEEE, la cual define las reglas de operación de ciertas tecnologías.

Bluetooth: tecnología de transmisión inalámbrica por medio de ondas de radio de corto alcance (1, 20 y 100 m a la redonda dependiendo la versión). Se utiliza en teclados, ordenadores, cámaras, etc.

Infrarrojos: tecnología de transmisión inalámbrica por medio de ondas de calor a corta distancia (hasta 1 m), capaces de traspasar cristales. Se usa diariamente en aparatos como mandos a distancia, móviles, etc.

Figura 6. Redes según su tecnología física de conexión: Redes inalámbricas

La red Internet

Orígenes de Internet

El origen de Internet se data en 1969, cuando la agencia DARPA estableció la primera conexión entre ordenadores que se denominó ARPANET. El supuesto fin de esta red era descentralizar la información militar duplicándola estratégicamente, de tal manera que si cualquiera de los nodos dejaba de funcionar, el resto seguiría totalmente funcionales. Posteriormente, su uso es vinculado a sectores académicos, científicos y gubernamentales y a inicios de los años 90, con el auge de las nuevas tecnologías se inicia el desarrollo de la actual red Internet.

Servicios de Internet

Internet es una fuente de servicios infinita que controla todo tipo de información (música, arte, cultura, medicina, deporte, etc) por medio de todo tipo de recursos (audio, vídeo, texto, imágenes, etc) y que permite al usuario informarse, entretenerse, crear, interactuar, etc. Internet es una red que proporciona servicios iguales a todos tipo de personas independientemente de la diferencias sociales o de la distancia . Por lo tanto Internet es un servicio que está al alcance de todas las personas y ha pasado a convertirse en la base de la sociedad del conocimiento en la que vivimos.

Figura 7. Servicios de Internet.

La web

La web está constituída por un conjunto de aplicaciones y tecnologías diseñadas para que los usuarios puedan interactuar y publicar sus contenidos con el resto del mundo.

Un sitio web es, en cambio, un espacio virtual en Internet que se trata de un conjunto de páginas webs agrupadas en un mismo dominio o subdominio. La navegación a través de estas se realiza a través de enlaces o hipervínculos.

Y, por último, las aplicaciones web son aplicaciones contenidas en la web y su finalidad es ofrecer diferentes servicios. No requiere instalación ya que están alojados en servidores de Internet.

Algunas similitudes entre los sitios y las aplicaciones web son que intercambian información, dotan la red de significado, etc.

Evolución de la web

El gran uso que tiene la web, junto con los avances tecnológicos provocaron que Internet siguiera progresando y evolucionando produciéndose unos cambios significativos:

Web 1.0 o web estática. Se limitaba a mostrar información y el usuario tenía un papel meramente observativo. Lo publicado no solía ser modificado

Web 2.0 o web social. Grandes avances respecto a la 1. Los usuarios toman un papel totalmente participativo y colaborativo dado a que estos ahora son los que crean, interactúan, se relacionan, etc. Gran uso de blogs, redes sociales, etc.

Web 3.0 o web semántica. Web donde ya no solo se conecta desde el ordenador si no que desde todo tipo de dispositivos. Es la llamada web inteligente, permite el acceso y la interacción de forma más eficiente y, encuentra respuestas con mucha más rapidez y acierto.

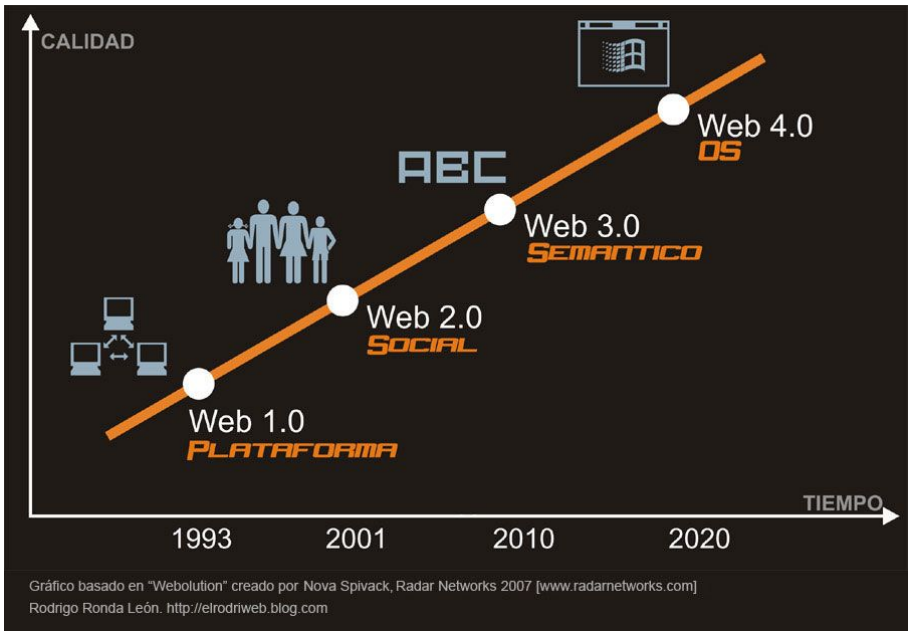


Figura 7. Evolución de la web.

Tecnologías de acceso a Internet

Los usuarios se conectan a Internet mediante proveedores de acceso a la red (ISP), que ofrecen servicios diferentes de comunicaciones y tecnologías de acceso. Este tipo de tecnologías se clasifican en tres grupos dependiendo del tipo de infraestructura que emplean para transmitir la información.

Acceso cableado. Este tipo requiere la 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. El desarrollo tecnológico experimentado en los últimos años que aprovecha la propagación de señales electromagnéticas a través del espacio libre (reflexión y refracción) ha permitido un explosivo crecimiento de los servicios de telecomunicaciones. Para que este tipo de redes inalámbricas sean útiles, el usuario debe estar dentro del radio de cobertura de la señal. Existen distintos tipos de tecnología de este tipo, como son WiMAX, LDMS, etc.

Acceso móvil. Permiten gran movilidad al usuario, pues la conexión se realiza a través de múltiples puntos de acceso a la red telefónica. Todo tipo de dispositivos móviles puede disponer de acceso por medio de una o más tecnologías, así se puede disponer, por ejemplo de tabletas que permiten el acceso vía WiFi o 3G, de forma indiferente, para proporcionarle acceso a datos.

La elección de un proveedor se realiza teniendo en cuenta factores como el tipo de tecnología que oferta, la cobertura que pueda disponer el usuario en su zona, el ancho de banda, la calidad de la señal, y, por supuesto, el coste. El ancho de banda es la cantidad de Mbps (Megabits por segundo), osea, la velocidad de la conexión.

Línea Telefónica

La finalidad de la creación de la línea telefónica fue transmitir la voz humana. Actualmente, la línea ha evolucionado utilizando los pares de cobre para la transmisión de forma digital, pero antes, al realizar una llamada, el teléfono traducía las ondas sonoras emitidas por la voz en impulsos eléctricos que eran enviados analógicamente a través de los hilos de cobre de la red de la telefonía básica (RTB).

Los primeros accesos a Internet se realizaban a través de esta línea básica, que con el tiempo evolucionó a la RDSI. Actualmente la más habitual es la popular ADSL.

RTC. Sus siglas significan Red de Telefonía Conmutada, aunque es más conocida como Red de Telefonía Básica. Se trata de la red de telefonía clásica, en la cual los terminales telefónicos se comunican con una central de conmutación a través de un solo canal compartido por la señal del micrófono y el auricular. Para enviar datos es necesario modificar la señal para que sea la adecuada al medio por el que tiene que viajar. El módem es el encargado de realizar esta función, por lo que para acceder a la red sólo necesitaremos una línea de teléfono y un módem. Debido a su obvia baja velocidad de esta tecnología y al no permitir el uso telefónico mientras se está conectado a Internet, se comenzaron a investigar nuevos métodos de conexión, lo que propició la evolución hacia la RDSI.

RDSI. Sus siglas significan Red Digital de Servicios Integrados. Siendo la evolución de la RDI, la RDSI facilita conexiones digitales extremo a extremo para proporcionar servicios, como puede ser el de voz. Los usuarios acceden a esta red a través de un conjunto de

interfaces normalizados. Este tipo de red envía la información codificada digitalmente, dividiendo la línea en 3 canales: 2 por los que circula la información y un tercero para gestionar la conexión. Una de las ventajas más destacables de la RDSI frente a la RDI es la posibilidad de poder utilizar la línea telefónica y conectarse a Internet al mismo tiempo, o bien utilizar las dos líneas al mismo tiempo y así incrementar la velocidad de transmisión.

Para transformar la información es necesario un adaptador de red para adecuar la velocidad entre el PC y la línea.

ADSL. Sus siglas significan Línea de Abonado Digital Asimétrica. Esta tecnología, siendo la evolución de la RDSI, divide el cable de cobre convencional de la línea telefónica en 3 canales independientes: recepción de datos, envío de datos y servicio telefónico tradicional. Generalmente la recepción de datos es de mayor velocidad que el de envío, pues los dos canales de datos son asimétricos. Nuevas versiones mejoradas de esta tecnología como ADSL2 y ADSL2+ han traído consigo un aumento importante de las velocidades de transferencia que permiten servicios desde vídeo de alta calidad a televisión digital. Actualmente es uno de los tipos de conexión más utilizados.

Cable o HFC

Hybrid Fiber Coaxial o HFC es un término que define una red de fibra óptica que combina este tipo de fibra con un cable coaxial para crear una red de banda ancha. Los proveedores de servicio de cable utilizan cable coaxial para conectar el domicilio del abonado hasta un nodo zonal y fibra óptica para interconectar los nodos zonales. Una de las ventajas más destacables

de la fibra óptica es su capacidad para cubrir grandes distancias con un mínimo de amplificación y regeneración de señal. El cable coaxial proporciona una capacidad de ancho de banda razonable, utilizándose para dar servicio a muchos usuarios a la vez.

Fibra óptica hasta el hogar

FFTH (Fiber to the home) o fibra hasta el hogar, se basa únicamente en la utilización de cables de fibra óptica, ofreciendo un acceso a Internet de banda ancha, telefonía y televisión. Se trata de una de las redes más rápidas, pudiendo proporcionar hasta varios gigabytes por segundo (Gbps), ya que la fibra óptica tiene tiene una gran capacidad para transmitir datos. Poco a poco los accesos tradicionales basados de cobre están siendo sustituidos por estos modernos sistemas.

Internet por satélite

La conexión por satélite es una más entre todas las tecnologías de banda ancha que nos permiten conectarnos a Internet con alta velocidad. No es una de las conexiones más económicas, por eso su uso se suele limitar a lugares remotos, para gente que no tiene otra manera de conectarse a la red, ni siquiera con ADSL. Los datos son transmitidos en forma de ondas electromagnéticas, enviados por satélites artificiales situados en la órbita terrestre, por lo que el usuario debe tener un módem conectado a una antena parabólica para poderse conectar.

WiMAX y LDMS

Este tipo de tecnologías son inalámbricas para el acceso a internet, conectándose por ondas de radio. Se utilizan habitualmente en zonas rurales o empresariales, donde el despliegue de cable o fibra sería muy costoso para la baja densidad de población.

LDMS. Se trata de un medio de transmisión de altas frecuencias y tiene una cobertura máxima de 35 km, aunque suele cubrir distancias de hasta 5 km. Dado que las altas frecuencias no atraviesan obstáculos, se requiere visibilidad directa con la antena emisora.

WiMAX. Mediante ondas electromagnéticas es capaz de cubrir distancias de hasta 50 km, sin necesidad de visibilidad directa entre antenas, por ello es más utilizado que LDMS.

Red eléctrica

Este sistema proporciona, mediante la red eléctrica, el acceso a Internet. Su ventaja es que no requiere de ningún tipo de instalación.

Basta con colocar un adaptador PLC (Power Lines Communications), en cualquier enchufe del domicilio. Con este nuevo concepto, podremos utilizar la instalación eléctrica de nuestra casa como infraestructura de telecomunicaciones. El PLC utiliza la red eléctrica como línea digital de alta velocidad para transmitir datos, de la misma forma que el WiFi lo hace por el aire, pero sin arriesgarnos a la inestabilidad de este. Su uso permite el acceso a internet mediante banda ancha, la transmisión de vídeo de alta definición y el uso de telefonía IP.

Conexión por telefonía móvil

Según su orden de aparición y prestaciones, contamos con diferentes agrupaciones de generaciones de conexión por medio de telefonía móvil:

Primera Generación (1G). Estos representan el conjunto de estándares que emplean tecnologías analógicas. En su época fueron sistemas pioneros, revolucionando los servicios de comunicación de los años 80, permitiendo la movilidad.

Segunda Generación (2G). Aparece a comienzos de los años 90. Su principal diferencia con la primera generación es el cambio de protocolos de telefonía móvil analógica a digital. Su desarrollo deriva de la necesidad de poder tener un mayor manejo de llamadas en prácticamente los mismos espectros de radiofrecuencia. Por razones como estas se implementaron servicios como el SMS. En Europa el sistema estándar más destacado es GSM (*Global System for Mobile*), que mejorando sus servicios dio lugar a GPRS (*General Packet Radio Service*), que utiliza conmutación de paquetes y se considera la generación 2.5. El GPRS permite el uso del correo electrónico y la navegación web, con velocidades de hasta 114 Kbps. La evolución tecnológica facilita la aparición de nuevos estándares con un ancho de banda mayor, como EDGE (*Enhanced Data Rates for GSM*) que novedosamente implementa el uso de aplicaciones de vídeo y más servicios multimedia.

Tercera Generación (3G). Los servicios asociados con la tercera generación son los de proporcionar la posibilidad de transmitir voz, o incluso la descarga de programas e intercambio de correos electrónicos. Está basada en el uso de del sistema de comunicación UMTS (*Universal Mobile Telecommunication System*), que se caracteriza por poseer una velocidad de acceso a Internet elevada o mismo posibilidades multimedia.

Cuarta Generación (4G): La 4G está completamente basada en el protocolo IP, siendo un sistema y una red exclusivamente de paquetes de datos.Su principal diferencia con las

generaciones predecesoras es la velocidad de acceso, las cuales serán del tipo de 100 Mbits en movimiento y 1GBit en reposo. La comunicación de voz se realiza mediante VolP. Las dos variantes más conocidas de 4G sin WiMAX y LTE (*Long Term Evolution*), que es la tecnología utilizada por la mayoría de operadoras de telefonía.

Quinta Generación (5G): Actualmente se encuentra sin estandarizar, aunque se espera que su uso común sea a partir de 2020. Será construído sobre los cimientos que el 4G LTE ha dejado, ya que es la más estandarizada. Su diferencia principal con 4G será la velocidad de transferencia. La velocidad máxima alcanzada por dispositivos 4G es 1 Gigabit por segundo, aunque esta cifra se ve afectada por muchos factores (microondas, edificios…). Se espera lograr con esta tecnología 5G una velocidad de 10 Gigabits por segundo, lo que se traduce en poder descargar, por ejemplo, una película en cuestión de segundos. Aunque el 5G no está implementado en la telefonía móvil, en algunos y servicios fijos de WiFI sí que está implementado, pero sólo móviles con acceso a redes 5G podrán aprovecharlo. La utilidad de este 5G estático es debido a que cuando nos conectamos con un dispositivo a una red WiFi, no alcanzamos su totalidad de velocidad, mientras que con esta capacidad 5G, nos aproximamos bastante más.

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 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.

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.

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.

Adopción de medidas de seguridad

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 sólo 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.

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. 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. 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 auntentificadas 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.

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 en 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.

Webgrafía:

- Redes de ordenadores.
- Fundamentos de las redes
- Finalidad de las redes.
- Historia de las redes.
- Modelo de referencia OSI.
- Orígenes y modelos de referencia
- Protocolo IP
- Tipos de redes
- Tipos de redes
- Tipos de redes
- Tipos de redes
- Tipos de redes
- La red Internet
- La red Internet
- Tecnologías de acceso a Internet
- HFC
- Seguridad en la red
- Seguridad en la red
- Seguridad en la red
- Seguridad en la red

Bibliografía:

- Sáez, N. R., Bordallo, C. P., y García, J. M. R. (2015) Cultura científica: 1º Bacharelato. Madrid, España: Grupo Anaya.
- Núñez, P. G., y Martínez, A. B. (2015) Tecnologías de la Información y la Comunicación: 1º Bachillerato. Madrid, España: Grupo Anaya.