Persevera

AL ALCANCE DE QUIEN ESTUDIA

BLOQUE VI · INFORMÁTICA BÁSICA Y OFIMÁTICA

Tema 8

Internet y navegadores web

Cuerpo General Administrativo de la Administración del Estado

INGRESO LIBRE · EDICIÓN 2026

perseveraoposiciones.com

AL ALCANCE DE QUIEN ESTUDIA

Estudiar una oposición ya cuesta bastante. Dinero, tiempo, esfuerzo. Lo que se ofrece habitualmente añade fricción: temarios caros y no redistribuibles, academias con horarios fijos y mensualidades que no todos pueden pagar.

Persevera publica los temarios enteros, en abierto. Lees, copias, imprimes y compartes con quien quieras.

Esta es la primera entrega. Los siguientes cuerpos los decidiremos contigo: nos cuentas qué oposición te interesa.

El temario es un producto vivo: hay erratas, hay matices que pueden afinarse, hay decisiones de redacción que pueden discutirse. Si encuentras algo que pueda mejorar, escríbenos. Lo leemos todo y publicamos las correcciones.

ÍNDICE

TEMA 8

Epígrafe 1 — La Red Internet: origen, evolución y estado actual

1. Concepto de Internet

Internet es una **red de redes**: una infraestructura global de comunicación formada por millones de redes independientes, de distintas tecnologías y titularidades, que se interconectan utilizando un conjunto común de protocolos (la familia **TCP/IP**). El nombre procede del término inglés *internet*, contracción de *internetwork* o *interconnected network* (red de redes interconectadas).

Ninguna organización, empresa o Estado posee ni controla la totalidad de Internet: funciona de forma **descentralizada** y su gestión técnica se articula a través de organismos internacionales abiertos (ICANN para los dominios y direcciones, IETF para los protocolos, W3C para los estándares web).

La comunicación en Internet sigue el **modelo cliente-servidor**: el cliente (un navegador, una app de correo u otro programa) formula peticiones de recursos concretos; el servidor es el equipo que almacena y entrega esos recursos. Un mismo equipo puede actuar como cliente para unos servicios y como servidor para otros según el contexto.

FIGURA

Diagrama cliente-servidor. Dispositivos cliente (ordenador, móvil, tableta) conectados con flechas hacia un servidor central a través de una nube etiquetada «Internet». Flechas de ida con la etiqueta «Solicitud» y flechas de vuelta con la etiqueta «Respuesta».

2. Historia: de ARPANET a la web actual

La historia de Internet arranca en el contexto de la **Guerra Fría**. El **7 de febrero de 1958**, en respuesta al lanzamiento del satélite soviético Sputnik (1957), el Departamento de Defensa de los Estados Unidos creó la **ARPA** *(Advanced Research Projects Agency, Agencia de Proyectos de Investigación Avanzados)*. La agencia cambió su denominación a **DARPA** en 1972, volvió a ARPA en 1993 y de nuevo a DARPA en 1996; ésta última es la denominación vigente.

Durante los años sesenta, ARPA diseñó una red de comunicación **descentralizada** con múltiples rutas entre nodos, capaz de seguir operando aunque algunos de sus puntos quedaran destruidos. La primera conexión efectiva se realizó el **29 de octubre de 1969, a las 22:30 PST**, entre **UCLA** (Universidad de California en Los Ángeles, sede del *Network Measurement Center* dirigido por Leonard Kleinrock) y el **SRI** *(Stanford Research Institute, hoy SRI International)*. El primer intento de transmitir la palabra *login* falló: solo llegaron las dos primeras letras, «**lo**». Antes de que terminara 1969, los cuatro nodos iniciales de **ARPANET** estaban operativos: UCLA, SRI, **UCSB** (UC Santa Barbara) y la **Universidad de Utah**. El protocolo de comunicación de ARPANET era **NCP** *(Network Control Program)*.

> **RECUERDA**
>
> El segundo nodo de ARPANET no era la Universidad de Stanford, sino el **SRI** (*Stanford Research Institute*), un instituto de investigación independiente afiliado a Stanford pero institucionalmente distinto. Es un matiz que algunos manuales clásicos resumen incorrectamente como «UCLA-Stanford».

En **1971** Ray Tomlinson envió el **primer correo electrónico** entre dos máquinas distintas de ARPANET. En **1972** la red conectaba ya unas cincuenta universidades. En **1973** se establecieron los primeros enlaces internacionales: **Reino Unido** (University College London) y **Noruega** (NORSAR).

Durante los años setenta se desarrolló la familia de protocolos **TCP/IP**. El **1 de enero de 1983** —el llamado *flag day*— ARPANET adoptó TCP/IP como estándar único, sustituyendo a NCP. Esta fecha se considera el **nacimiento técnico de Internet**. En **1986** la NSF *(National Science Foundation)* creó la **NSFNET**, sucesora de ARPANET, que extendió la

conectividad a instituciones educativas y usuarios domésticos. ARPANET fue desactivada el **28 de febrero de 1990** la NSFNET fue red troncal hasta el **30 de abril de 1995**, fecha en que la estructura se descentralizó por completo.

En **marzo de 1989**, **Tim Berners-Lee**, trabajando en el **CERN** (Organización Europea para la Investigación Nuclear, Ginebra), presentó la propuesta «*Information Management: A Proposal*» que daría lugar a la **World Wide Web** (WWW): un sistema de hipertexto navegable a través de Internet. La WWW es uno de los servicios que operan sobre Internet, no Internet en sí.

Fecha	Hito clave
1958	Fundación de ARPA (Departamento de Defensa de EE.UU.).
1969	Primera conexión ARPANET (UCLA ↔ SRI, 29/10/1969). Cuatro nodos iniciales con protocolo NCP.
1971	Primer correo electrónico (Ray Tomlinson, vía ARPANET).
1983	ARPANET adopta TCP/IP como estándar (*flag day* 1 enero). Nacimiento técnico de Internet.
1986	NSF crea la NSFNET (sucesora de ARPANET).
1989	Tim Berners-Lee propone la WWW en el CERN (Ginebra).
1990	Primer navegador web (WorldWideWeb, de Berners-Lee). ARPANET desactivada.
1993	Lanzamiento de **Mosaic**: primer navegador gráfico masivo.
1994	Tim Berners-Lee funda el **W3C** en el MIT.
1998	Fundación de **Google**.
2004-2006	Auge de la **Web 2.0**: Facebook (2004), YouTube (2005), Twitter (2006).
2011	IANA agota el pool central de direcciones IPv4 (3 de febrero).
2019	RIPE NCC asigna el último bloque IPv4 europeo (25 de noviembre).

RECUERDA

Tres fechas imprescindibles: **1969** (ARPANET con 4 nodos, NCP) · **1983** (TCP/IP estándar, nacimiento técnico de Internet) · **1989** (propuesta de la WWW por Berners-Lee en el CERN). Tim Berners-Lee inventó la World Wide Web en 1989, **no** Internet: Internet existía desde 1969.

3. Estado actual: usuarios y jerarquía de operadores

Internet alcanza hoy a la **mayoría de la población mundial**: los informes globales de referencia (*Digital Global Overview Report* de DataReportal, We Are Social y Meltwater, publicados con periodicidad anual y semestral) sitúan los usuarios de Internet, los usuarios de redes sociales y los suscriptores móviles únicos en el entorno de los **varios miles de millones** cada uno, con incrementos sostenidos año tras año. Las cifras concretas se actualizan cada pocos meses; lo estable es la tendencia: penetración alta y creciente, fuerte peso de la conexión móvil y predominio del acceso por dispositivos personales.

Entre los servicios de mayor uso se encuentran la **web**, las **redes sociales**, el **comercio electrónico**, la **mensajería instantánea** y el **vídeo en línea**.

La estructura física de Internet se organiza de forma jerárquica en tres niveles denominados ***tiers***:

Tier	Quién	Cómo conecta
Tier 1	Grandes empresas con infraestructuras troncales intercontinentales (cables submarinos, grandes IXP).	Se interconectan entre sí mediante acuerdos de ***peering*** **gratuito** y alcanzan cualquier punto de Internet sin pagar tránsito a nadie.
Tier 2	Operadores nacionales o regionales.	Peering limitado con otros Tier 2; pagan **tránsito** a un Tier 1 para zonas no cubiertas.
Tier 3	ISP locales que contratan los usuarios domésticos y empresas.	Sin red de alcance global; pagan tránsito a Tier 1 o Tier 2 por la totalidad del tráfico.

Una conexión cotidiana atraviesa habitualmente los tres niveles antes de llegar a su destino.

4. El W3C y la accesibilidad web

El **W3C** *(World Wide Web Consortium)* es el principal organismo internacional de estandarización de la web. Fue fundado el **1 de octubre de 1994 en el MIT** por **Tim Berners-Lee**. Desarrolla estándares abiertos llamados *Recomendaciones*: **HTML** (estructura), **CSS** (estilo), **XML** (intercambio de datos) y las **WCAG** *(Web Content Accessibility Guidelines)*. En la práctica, los estándares web favorecen páginas **usables** (intuitivas), **accesibles** (utilizables por cualquier persona y dispositivo) y **adaptables** (que se ajustan al tamaño de pantalla y al hardware del usuario).

En el plano normativo europeo, la **Directiva (UE) 2016/2102, de 26 de octubre de 2016**, establece los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público. En España fue traspuesta por el **Real Decreto 1112/2018, de 7 de septiembre**, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

> **MATIZ**
>
> La Directiva (UE) 2016/2102 se aplica **exclusivamente al sector público**, no a los sitios web privados. La norma española que la traspone es el **RD 1112/2018, de 7 de septiembre**. No confundir el número de la Directiva (2016/2102) con el del Real Decreto español (1112/2018).

5. Surface Web, Deep Web y Dark Web

El contenido **indexado** por los buscadores convencionales (Google, Bing, etc.) se denomina **Surface Web** o web superficial. El resto, mucho más voluminoso, es la **Deep Web** o web profunda: contenido **no indexado por los buscadores**, en su inmensa mayoría legítimo —bases de datos privadas, intranets corporativas, correos electrónicos, expedientes administrativos, historiales clínicos, registros bancarios—. Las estimaciones cuantitativas

de la proporción Surface/Deep varían mucho entre estudios y se consideran orientativas: lo relevante es la distinción cualitativa, no la cifra concreta.

La **Dark Web** es un **subconjunto muy reducido** de la Deep Web que requiere software especializado, típicamente el navegador **Tor**, y sí puede albergar contenidos y actividades ilícitas, aunque también tiene usos legítimos (anonimato para periodistas, disidentes, denuncias).

> **MATIZ**
>
> Deep Web y Dark Web **no son sinónimos**. La Deep Web es la parte **no indexada** de la red e incluye contenido **legítimo** (intranets, expedientes, bases de datos privadas, correo electrónico). La Dark Web es un subconjunto pequeño que requiere Tor u otras herramientas específicas. Identificar la Deep Web con «contenido ilegal» es un error frecuente: los expedientes administrativos son Deep Web.

6. El protocolo TCP/IP

TCP/IP es la familia de protocolos que regula la transmisión y recepción de datos en Internet. Cuando un dispositivo envía información, esta se divide en **paquetes**:

- El **protocolo IP** *(Internet Protocol)* asigna a cada paquete la dirección de destino y determina la ruta. Los paquetes pueden llegar al destino por **caminos distintos**.
- El **protocolo TCP** *(Transmission Control Protocol)* controla que todos los paquetes lleguen correctamente al destino, solicitando el reenvío de los perdidos y entregándolos en orden.
- El **protocolo UDP** *(User Datagram Protocol)* prescinde de las confirmaciones de entrega para ganar velocidad. Es habitual en **comunicaciones en tiempo real** (videollamadas, voz sobre IP, videojuegos en línea), donde la latencia importa más que la pérdida ocasional de un paquete.

Protocolo	Garantía de entrega	Velocidad	Uso típico

TCP	Sí: reenvío de paquetes perdidos y entrega ordenada.	Más lento (confirmaciones).	Web (HTTP/HTTPS), correo (SMTP/IMAP/POP3), FTP, *streaming* de vídeo bajo demanda (HLS, MPEG-DASH).
UDP	No: los paquetes perdidos se descartan.	Más rápido (sin confirmaciones).	Videollamadas, voz sobre IP, videojuegos en línea, retransmisiones en vivo de baja latencia.

RECUERDA

TCP = fiabilidad garantizada. **UDP** = velocidad sin garantías. Mnemónico clásico: TCP = Todo Con Paciencia · UDP = Ultra rápido, Da igual si se Pierde.

7. Direcciones IP: IPv4 e IPv6

Cada dispositivo conectado a Internet necesita una **dirección IP** que lo identifique de forma única. Existen dos versiones del protocolo en uso simultáneo:

Característica	IPv4	IPv6
Longitud	32 bits	128 bits
Notación	4 octetos decimales (0-255) separados por punto: `192.168.1.1`	8 grupos hexadecimales separados por dos puntos: `2001:0db8::1`
Combinaciones	2^{32} = **4.294.967.296** (4.300 millones)	340 sextillones
Estado	**AGOTADO** – RIPE NCC asignó el último bloque /22 europeo el **25/11/2019**. Solución transitoria: **CG-NAT**.	Implantación progresiva en curso.

La **IP pública** es la que el ISP asigna al router cuando se conecta a Internet (visible desde el exterior). La **IP privada** es la que el router asigna internamente a cada dispositivo de la red local mediante **DHCP** los rangos privados reservados (RFC 1918) son `10.0.0.0/8`, `172.16.0.0/12` y `192.168.0.0/16`.

Una dirección IP puede ser **dinámica** (reasignada por DHCP en cada conexión, habitual en hogares) o **estática** (fija, para servidores y servicios que deben ser siempre localizables).

MATIZ

32 bits = IPv4 · 128 bits = IPv6. IPv6 usa dígitos hexadecimales (con letras A-F); las letras en una dirección indican IPv6, **nunca** IPv4. El agotamiento de IPv4 en Europa lo declaró el **RIPE NCC** en noviembre de 2019; **IANA** (registro global) había agotado su pool central ya en febrero de 2011.

8. El sistema DNS y los dominios

El **DNS** *(Domain Name System, Sistema de Nombres de Dominio)* es un sistema distribuido de bases de datos que **traduce los nombres de dominio** legibles para las personas (`www.boe.es`) en las **direcciones IP** numéricas que los routers necesitan para enrutar paquetes. El proceso típico es:

1. El usuario escribe una URL en el navegador.
2. El equipo consulta al servidor DNS del ISP.
3. El servidor DNS devuelve la IP correspondiente.
4. El navegador establece la conexión con esa IP.

Ejemplos de DNS público: **8.8.8.8** y **8.8.4.4** (Google), **1.1.1.1** (Cloudflare).

FIGURA

Diagrama de resolución DNS en 4 pasos: (1) usuario escribe nombre en el navegador; (2) consulta al servidor DNS del ISP; (3) el servidor devuelve la IP; (4) el navegador conecta directamente a esa IP.

Un nombre de dominio se organiza **jerárquicamente de derecha a izquierda**. En `www.agenciatributaria.gob.es`:

- `.es` es el **TLD** *(Top-Level Domain, dominio de primer nivel)*.
- `gob` es el dominio de **segundo nivel**.

- `agenciatributaria` es el dominio de **tercer nivel**.
- `www` es el **subdominio** (cuarto nivel).

Los TLD se clasifican en:

Tipo	Significado	Ejemplos
gTLD	*Generic TLD* – uso genérico mundial.	`.com`, `.org`, `.net`, `.info`, `.app`
ccTLD	*Country Code TLD* – código de país de dos letras (ISO 3166-1).	`.es`, `.fr`, `.uk`, `.de`. Excepción histórica: `.co.uk` (dos niveles).
sTLD	*Sponsored TLD* – patrocinado por una entidad específica.	`.gov`, `.edu`, `.mil`, `.museum`, `.aero`
Reservados	RFC 2606: dominios reservados para pruebas y documentación.	`.test`, `.example`, `.invalid`, `.localhost`

La supervisión global del DNS y la asignación de dominios corresponde a la **ICANN** *(Internet Corporation for Assigned Names and Numbers)*. La gestión del `.es` corresponde en España a **Red.es**, entidad pública empresarial.

> **MATIZ**
>
> **ICANN** = supervisión global de todos los dominios. **Red.es** = administra exclusivamente el `.es` en España. El subdominio `www` es **tercer o cuarto nivel** según el dominio, **NO** parte del nombre de dominio principal: hoy la mayoría de sitios funcionan igual con o sin `www`.

9. La URL y los protocolos HTTP/HTTPS

Una **URL** *(Uniform Resource Locator)* es la **dirección completa y única** de cualquier recurso en Internet. Puede tener hasta siete componentes:

N°	Componente	Ejemplo	Obligatorio
1	**Esquema** (protocolo)	`https://`	Sí
2	**Subdominio**	`www.`	No
3 + 4	**Dominio y TLD**	`hacienda.gob.es`	Sí

5	**Ruta**	`/modelos/303/`	No
6	**Parámetros de consulta** (empiezan con `?`, múltiples separados por `&`)	`?ejercicio=2024`	No
7	**Fragmento** (empieza con `#`, ancla dentro de la página)	`#seccion3`	No

El protocolo **HTTP** *(Hypertext Transfer Protocol)* define cómo se solicitan y entregan los recursos web. Transmite los datos **en texto claro, sin cifrado**.

El protocolo **HTTPS** añade una capa de cifrado mediante **TLS** *(Transport Layer Security)* que garantiza tres propiedades:

- **Confidencialidad**: los datos viajan cifrados; un tercero que intercepte el tráfico no puede leerlos.
- **Integridad**: los datos no pueden alterarse en tránsito sin que el receptor lo detecte.
- **Autenticación**: el servidor acredita su identidad mediante un **certificado digital** emitido por una autoridad de certificación.

Los navegadores muestran un **candado** junto a la URL cuando la conexión es HTTPS.

> **MATIZ**
>
> **HTTPS no garantiza que el sitio sea legítimo**: solo garantiza que la comunicación está cifrada. Un sitio de *phishing* puede tener HTTPS y mostrar candado, porque los certificados son fáciles de obtener. Candado = cifrado en tránsito, **NO** honestidad del titular del sitio. La distinción entre `?` (parámetros de consulta) y `#` (fragmento) es un error frecuente al leer una URL.

10. Lenguajes de la web: HTML, CSS, XML y JavaScript

Lenguaje	Función	Naturaleza
HTML *(HyperText Markup Language)*	Define la **estructura** del contenido de la página mediante etiquetas. El hipertexto es texto	Lenguaje de marcado.

	que contiene **enlaces** a otros recursos.	
CSS *(Cascading Style Sheets)*	Reglas visuales: tipografía, colores, maquetación, animaciones.	Lenguaje de **estilo**.
XML *(eXtensible Markup Language)*	Formato de **intercambio de datos estructurados** entre sistemas.	Lenguaje de marcado para datos.
JavaScript	Añade interactividad y lógica del lado del cliente. Lenguaje de programación.	Lenguaje de programación.

Para funcionalidades más complejas del lado del servidor se emplean Java, Python, C#, PHP, entre otros.

11. Protocolos adicionales

Además de TCP/IP y HTTP/HTTPS, Internet se apoya en un conjunto de protocolos especializados:

Protocolo	Nombre completo	Función principal
ARP	*Address Resolution Protocol*	Resuelve una dirección IP conocida en la dirección **MAC** del adaptador de red correspondiente en la red local (capa 3 → capa 2).
RARP	*Reverse ARP*	Proceso inverso: MAC → IP. Hoy reemplazado por **DHCP**.
DHCP	*Dynamic Host Configuration Protocol*	Asigna automáticamente IP, máscara, puerta de enlace y servidor DNS a cada dispositivo que se conecta a la red.
ICMP	*Internet Control Message Protocol*	Protocolo de control y diagnóstico. Lo usan los comandos `ping` (prueba de conectividad) y `tracert`/`traceroute` (traza la ruta de los paquetes).
VoIP	*Voice over IP*	Transmite voz a través de Internet en lugar de la red telefónica

		conmutada. Ejemplos: Skype, Teams, WhatsApp voz.
IPTV	*Internet Protocol Television*	Distribuye señal de televisión a través del protocolo IP en lugar del cable o satélite.
IRC	*Internet Relay Chat*	Protocolo basado en texto para conversaciones en tiempo real. Precursor de la mensajería instantánea.
Telnet	*Teletype Network*	Permite acceder a un equipo remoto por línea de comandos. Transmite en **texto claro** sustituido por **SSH**.

RECUERDA

`tracert` (Windows) / `traceroute` (Linux) usan **ICMP** para mostrar la ruta nodo a nodo de un paquete hasta el destino. Complementan a `ping`, que solo verifica si el destino responde. **DHCP** asigna automáticamente IP, máscara, *gateway* y DNS al conectar: sin DHCP habría que configurarlos a mano en cada equipo. **ARP** hace el salto IP (capa 3) → MAC (capa 2); imprescindible para la entrega final en la red local.

TEMA 8

Epígrafe 2 — Conceptos elementales sobre protocolos y servicios en Internet

1. Hardware de red: elementos físicos

Para que los datos circulen desde el ISP hasta los dispositivos del usuario, es necesaria una cadena de elementos físicos de red. Cada uno opera a un nivel distinto del modelo OSI y cumple una función específica.

1.1. Módem y router

El **módem** *(modulador-demodulador)* convierte la señal digital del ordenador en la señal adecuada para el medio físico de transmisión (eléctrica, óptica o de radiofrecuencia) y viceversa. Es el punto de entrada de la señal del ISP en el hogar u oficina.

El **router** o **enrutador** recibe la conexión del módem, determina el camino óptimo para los paquetes y los distribuye a los dispositivos de la red local, asignándoles una **IP privada** mediante DHCP. Hoy, módem y router suelen venir integrados en un único dispositivo, el ***router doméstico*** o ***gateway***.

> **FIGURA**
>
> Imagen de un router doméstico moderno (router de fibra óptica del ISP) con sus puertos etiquetados: puerto WAN (entrada del ISP), cuatro puertos LAN Ethernet (RJ-45) y antenas Wi-Fi.

1.2. Hub y switch

Tanto el **hub** *(concentrador)* como el **switch** *(conmutador)* interconectan varios equipos dentro de una red local (LAN). La diferencia fundamental está en cómo gestionan el tráfico:

Dispositivo	Cómo distribuye el tráfico	Capa OSI	Eficiencia

Hub	Replica el paquete a **todos** los puertos (broadcast).	Capa 1 (Física)	Baja: genera colisiones.
Switch	Aprende la dirección **MAC** de cada dispositivo y envía el paquete **solo** al puerto del destinatario (unicast).	Capa 2 (Enlace de datos)	Alta: sin colisiones.

Ninguno de los dos, por sí solo, da acceso a Internet: para eso se necesita un **router**. El hub está prácticamente obsoleto en redes modernas.

1.3. Bridge, gateway y proxy

- **Bridge** *(puente)*: conecta dos segmentos de red local y actúa como filtro de tráfico entre ambos.
- **Gateway** *(puerta de enlace)*: conecta redes con **arquitecturas o protocolos distintos** realizando la conversión necesaria. En una red doméstica, el router actúa como *gateway* entre la LAN del hogar e Internet.
- **Proxy**: servidor intermediario que actúa **en nombre del cliente** ante los servidores de Internet. El cliente envía la petición al proxy, el proxy la reenvía al servidor real y devuelve la respuesta al cliente; el servidor solo ve la IP del proxy, no la del cliente real.

Funciones típicas del proxy:

Función	Descripción
Filtrado de contenido	Restringe el acceso a sitios o servicios concretos. Uso habitual en entornos corporativos y educativos.
Control de accesos	Limita qué usuarios pueden acceder a qué recursos de Internet.
Caché web	Almacena copias de las páginas más visitadas, reduciendo las peticiones a servidores externos y acelerando la carga.
Acceso a contenido geográfico	Al presentar la IP del proxy, permite acceder a contenido disponible solo en el país del proxy.

MATIZ

Hub ≠ Switch: el hub inunda todos los puertos (capa 1); el switch aprende MACs y envía solo al destinatario (capa 2). **Router ≠ Switch**: el router interconecta **redes distintas** y enruta por IP (capa 3); el switch interconecta dispositivos dentro de la **misma red** y trabaja por MAC (capa 2). **Proxy ≠ VPN**: el proxy redirige peticiones de aplicaciones concretas (normalmente el navegador); la VPN cifra **todo el tráfico** del dispositivo y lo tuneliza extremo a extremo.

2. El ISP: proveedor de servicios de Internet

Para conectarse a Internet, todo dispositivo debe hacerlo a través de un **ISP** *(Internet Service Provider, Proveedor de Servicios de Internet)*. Los ISP son las compañías que despliegan infraestructuras de telecomunicación y ofrecen acceso a Internet a hogares, empresas e instituciones.

A través del protocolo **DHCP**, el ISP asigna automáticamente al router del abonado su **dirección IP pública**, su máscara de red, la puerta de enlace y los servidores DNS; el router del abonado, a su vez, asigna **IPs privadas** a cada dispositivo de la red local.

En España, el mercado de los ISP está dominado a fecha actual por cuatro operadores con red propia:

Operador	Origen	Notas
Movistar	Telefónica.	Operador histórico, mayor cuota de fibra en España.
MasOrange	Fusión Orange España + MásMóvil, constituida el **26/03/2024**.	Aprobada por la Comisión Europea el 20/02/2024 y por el Consejo de Ministros el 12/03/2024. Opera con cuatro marcas integradas: **Orange**, **MásMóvil**, **Yoigo** y **Jazztel**.
Vodafone España	Adquirida por el fondo británico **Zegona** en mayo de 2024.	Mantiene la marca Vodafone bajo licencia.

Digi	Operador de origen rumano.	Cuarto operador con red propia; ha crecido tras la cesión de espectro impuesta por la Comisión Europea como condición a la fusión de MasOrange.

Las Administraciones Públicas españolas se sirven adicionalmente de la **Red SARA** *(Sistemas de Aplicaciones y Redes para las Administraciones)*: una intranet administrativa que interconecta los sistemas de información de la **Administración General del Estado**, las **Comunidades Autónomas** y las **Entidades Locales**, con acceso a Internet bajo niveles de seguridad reforzados. Está gestionada por la Secretaría General de Administración Digital.

3. Conexiones fijas a Internet

Las conexiones fijas requieren una infraestructura física permanente hasta el punto de acceso del abonado.

Tecnología	Soporte físico	Velocidad orientativa
RTB/RTC *(obsoleta)*	Cable telefónico de cobre. Señal analógica (módem). No permite voz y datos simultáneos.	Máx. 56 Kbps.
ADSL *(Asymmetric Digital Subscriber Line)*	Cable de cobre. Señal digital. **Asimétrica**: bajada > subida. Voz y datos simultáneos.	Hasta 20 Mbps (bajada). VDSL2 hasta 100 Mbps.
Cable coaxial / HFC	Red de televisión por cable (estándar **DOCSIS**).	2 Mbps – 1 Gbps.
Fibra óptica (FTTH/FTTB)	Fibra de vidrio o plástico: pulsos de luz. Dominante en España.	50 Mbps – 1 Gbps+.
Satélite	Señal vía satélite geoestacionario o constelaciones LEO (Starlink, OneWeb).	Variable; latencia elevada en geoestacionario, baja en LEO.
WiMAX	Ondas de radio inalámbricas con cobertura metropolitana.	Hasta 70 Mbps.
PLC *(Power Line Communications)*	Red eléctrica del hogar como medio de transmisión.	Variable; distribución local.

MATIZ

El **Wi-Fi NO es una tecnología de acceso a Internet**, sino de **distribución local**: canaliza la conexión del router a los dispositivos dentro del domicilio. El acceso a Internet lo proporciona el **ISP** mediante una de las tecnologías de la tabla (fibra, ADSL, cable, etc.). El nombre **ADSL** significa *Asymmetric Digital Subscriber Line*: la asimetría se refiere a que la velocidad de **bajada es mayor que la de subida**, no a una limitación accidental.

4. Conexiones móviles a Internet

Las conexiones móviles utilizan ondas de radio transmitidas desde estaciones base (antenas) que cubren áreas geográficas llamadas **celdas**.

Generación	Nombre / Característica	Velocidad orientativa
Pre-2G / WAP	Acceso WAP a Internet en móvil, solo texto.	10 Kbps
2.5G / GPRS	*General Packet Radio Service*. Primera transmisión de datos en paquetes.	114 Kbps
3G / UMTS	*Universal Mobile Telecommunications System*. Móvil multimedia.	Hasta 2 Mbps
3G+ / HSPA	*High Speed Packet Access*. Permite vídeo en móvil.	Hasta 14 Mbps
4G / LTE	*Long Term Evolution*. Móvil de banda ancha.	Hasta 100 Mbps
5G	Quinta generación. Baja latencia y alta densidad de dispositivos (IoT).	Hasta 1 Gbps+

RECUERDA

Secuencia ascendente: **WAP → GPRS (2.5G) → UMTS (3G) → HSPA (3G+) → LTE (4G) → 5G**. La novedad clave de **5G** no es solo la velocidad, sino la **baja latencia** (1 ms) y la **capacidad de conexión simultánea** de gran densidad de dispositivos — clave para el **IoT**, los vehículos conectados y la automatización industrial.

5. Clasificación de redes

Las redes informáticas se clasifican según cuatro criterios: jerarquía, extensión geográfica, topología y modo de transferencia de datos.

5.1. Según jerarquía

- Redes **P2P** *(peer to peer)* o **Workgroups**: redes **sin jerarquía** para grupos pequeños (hasta 10 equipos). No hay servidores especializados; todos los equipos actúan a la vez como cliente y servidor.
- Redes **cliente-servidor**: propias de entornos más grandes. Uno o varios servidores especializados proveen servicios concretos (datos, impresión, correo) a los clientes (estaciones de trabajo) que los solicitan.

5.2. Según extensión

Tipo	Extensión	Descripción
PAN *(Personal Area Network)*	Entorno personal del usuario	Dispositivos que el usuario manipula: móvil, tableta, smartwatch, auriculares.
LAN *(Local Area Network)*	Edificio / oficina / hogar	Red de área local. Mínimo dos dispositivos. Versión inalámbrica: **WLAN**.
MAN *(Metropolitan Area Network)*	Ciudad o municipio	Red de área metropolitana.
WAN *(Wide Area Network)*	Países o continentes (100-1.000 km+)	Red de área amplia. Despliegue habitual por los ISP.

FIGURA

Diagrama comparativo de los tipos de red por extensión. Cuatro zonas concéntricas: PAN (interior, entorno personal), LAN (oficina u hogar), MAN (ciudad), WAN (mapa de países o continentes).

5.3. Según topología

La topología describe **cómo están dispuestas físicamente** las estaciones de trabajo y los enlaces entre ellas.

Topología	Descripción	Ventaja	Inconveniente
Bus	Todos los equipos se conectan a un canal central común.	Simple y económica.	Si falla el canal central, cae toda la red.
Anillo	Equipos en cadena formando un anillo cerrado; la información pasa de equipo en equipo.	Buena para distancias medias.	Si cae un equipo, puede caer toda la red.
Estrella	Cada equipo tiene su propio canal y se conecta a un switch o hub central.	Si cae un equipo, no afecta al resto.	Si cae el switch central, cae toda la red.
Malla	Cada equipo conectado con todos los demás.	Múltiples rutas: máxima redundancia y fiabilidad.	Cara y compleja.
Árbol	Modelo jerárquico que combina estrella y bus. Parte de un dispositivo raíz.	Escalable y estructurada.	Si falla el nodo raíz, cae la rama afectada.
Híbrida	Combinación de dos o más topologías.	Flexible y adaptable.	Mayor complejidad de gestión.

FIGURA

Seis diagramas de topologías de red (bus, anillo, estrella, malla, árbol, híbrida) con los nodos representados como círculos y los enlaces como líneas. Cada diagrama etiquetado con su nombre.

RECUERDA

Estrella: si cae un equipo, la red sigue; si cae el **switch central**, cae toda la red. **Bus**: si falla un equipo individual, la red sigue; si falla el **canal central**, cae toda la red. **Malla**: la más resistente a fallos (múltiples rutas) pero también la más cara.

5.4. Según modo de transferencia

Modo	Descripción	Ejemplo
Simplex (unidireccional)	La información viaja en una sola dirección. Un dispositivo transmite, el otro solo recibe.	Televisión, radio.
Half-duplex (bidireccional no simultáneo)	Bidireccional, pero no en ambas direcciones al mismo tiempo.	Walkie-talkie.
Full-duplex (bidireccional simultáneo)	Transmisión y recepción simultáneas a través del mismo canal.	Telefonía, conexión a Internet.

6. Internet, Intranet y Extranet

Red	Acceso	Usuarios
Internet	Abierta. Sin restricciones (salvo contenidos ilegales).	Cualquier persona con conexión.
Intranet	**Cerrada**. Red interna de una organización con tecnologías de Internet (TCP/IP, navegadores), pero acceso restringido a sus miembros.	Empleados internos.

Extranet	**Semi-cerrada**. Extensión de la intranet hacia usuarios externos autorizados mediante usuario y contraseña. Accesible desde cualquier punto del mundo.	Miembros internos + usuarios externos autorizados (clientes, proveedores).

MATIZ

Intranet = red interna **cerrada**, solo accesible para los miembros de la organización. **Extranet** = intranet **ampliada** a usuarios externos autorizados mediante credenciales. **Internet** = red pública abierta. La intranet utiliza las mismas tecnologías que Internet (TCP/IP, navegadores), pero no es accesible desde fuera de la organización.

7. Herramientas de diagnóstico: `ipconfig`, `ping` y `tracert`

En Windows, el comando `ipconfig` muestra la configuración de red del equipo local: dirección IP privada, máscara de subred y puerta de enlace predeterminada. Con el modificador `/all` añade la **dirección MAC** de cada adaptador y el servidor DNS configurado. Es una herramienta de diagnóstico **local**: no genera tráfico de red hacia el exterior.

Comando	Función
`ipconfig`	Configuración IP local básica.
`ipconfig /all`	Añade MAC, DHCP y DNS detallado.
`ipconfig /release`	Libera la IP asignada por DHCP.
`ipconfig /renew`	Solicita nueva IP al DHCP.

El comando `ping` utiliza el protocolo **ICMP** para verificar si un equipo remoto es accesible y medir la **latencia**. Envía paquetes ICMP *Echo Request* al destino y aguarda las respuestas *Echo Reply*, mostrando el tiempo de ida y vuelta.

Variante	Para qué sirve
`ping 127.0.0.1`	Prueba la pila TCP/IP local (*loopback*). Si falla, el problema está en el software de red del propio equipo.

`ping 8.8.8.8`	Prueba la conectividad con Internet (DNS público de Google).
`ping www.google.es`	Combina **resolución DNS** + **conectividad**.

El comando `tracert` (Windows) o `traceroute` (Linux/macOS) traza la **ruta nodo a nodo** que recorre un paquete desde el equipo hasta el destino, mostrando cada salto y su latencia.

MATIZ

`ipconfig` = consulta **local**, sin tráfico de red — **no** puede verificar si hay conexión a Internet. `ping` = **genera tráfico ICMP**, verifica conectividad externa y latencia. `ping` usa **ICMP**, no TCP ni UDP; algunos cortafuegos bloquean ICMP, por lo que la ausencia de respuesta no implica necesariamente que el equipo esté caído.

8. Principales servicios de Internet

Internet es la infraestructura sobre la que se prestan múltiples servicios. La **World Wide Web** es el más conocido, pero no el único.

8.1. Correo electrónico

Permite enviar y recibir mensajes y adjuntos. Tres protocolos implicados:

Protocolo	Función	Puerto estándar
SMTP	Envío de mensajes (cliente → servidor y entre servidores).	25 / 465 (SMTPS) / 587 (envío autenticado).
POP3	Descarga los mensajes al dispositivo local y, por defecto, los borra del servidor.	110 / 995 (POP3S).
IMAP	Accede y gestiona los mensajes directamente en el servidor; sincronización multidispositivo.	143 / 993 (IMAPS).

RECUERDA

Para usar el correo en varios dispositivos (móvil, portátil, tableta) lo apropiado es **IMAP**: mantiene los mensajes en el servidor y los sincroniza en todos los dispositivos. **POP3** descarga el correo al equipo local y lo borra del servidor (salvo configuración explícita), por lo que solo es práctico si se consulta desde un único dispositivo.

8.2. Mensajería instantánea, foros y videoconferencia

- **Mensajería instantánea**: comunicación en tiempo real (WhatsApp, Telegram, Signal con cifrado extremo a extremo, Microsoft Teams, Slack para entorno corporativo). El precursor histórico fue **IRC**.
- **Foros**: sitios de discusión en línea donde los usuarios publican mensajes que forman un *hilo* de conversación. A diferencia de la mensajería instantánea, la conversación **no es en tiempo real**.
- **Videoconferencia**: Zoom, Microsoft Teams, Google Meet, Cisco Webex.

8.3. Transferencia de archivos: FTP, FTPS, SFTP y P2P

Protocolo	Características
FTP *(File Transfer Protocol)*	Arquitectura cliente-servidor. **Sin cifrado**. Puerto 21.
FTPS	FTP + cifrado **TLS**.
SFTP	Opera sobre **SSH**, protocolo distinto a FTP a pesar del nombre.
P2P *(peer to peer)*	Sin servidor centralizado: cada equipo actúa simultáneamente como cliente y servidor. Ejemplos: eMule, uTorrent, BitTorrent.

8.4. Almacenamiento en la nube, streaming y acceso remoto

- **Almacenamiento en la nube**: OneDrive (Microsoft), Google Drive, Dropbox, Mega, iCloud (Apple). Plataformas de infraestructura para empresas: Microsoft Azure y Amazon Web Services (AWS).
- **Streaming**: transmisión continua de contenido audiovisual sin descarga completa. El vídeo **bajo demanda** (Netflix, HBO Max, Disney+, Amazon Prime Video, YouTube)

suele emplear protocolos de **streaming adaptativo sobre HTTP**, como **HLS** *(HTTP Live Streaming)* y **MPEG-DASH**, que ajustan la calidad a la velocidad de conexión del usuario. Las **retransmisiones en vivo de baja latencia** y la **videollamada** se apoyan más en UDP, **QUIC** o **WebRTC**. El **podcast** es la versión de audio del contenido bajo demanda (Podimo, iVoox, Podium Podcast).

- **Acceso remoto**: protocolos y herramientas que permiten controlar un equipo a distancia. Microsoft usa **RDP** *(Remote Desktop Protocol)* alternativas: **VNC** *(Virtual Network Computing)*, TeamViewer, AnyDesk. **Telnet** fue el estándar histórico sin cifrado; lo sustituyó **SSH** *(Secure Shell)* con cifrado.

8.5. Comercio electrónico y sistemas de pago

El **comercio electrónico** (*e-commerce*) engloba las transacciones de bienes y servicios a través de medios electrónicos. Los **Sistemas de Pago Electrónico** (EPS, *Electronic Payment Systems*) permiten transferir dinero entre comprador y vendedor: pasarelas de pago bancarias integradas en las tiendas, **PayPal** (plataforma global independiente) y **Bizum** (pagos móviles instantáneos vinculados a la banca española).

Modalidad	Descripción	Ejemplo
B2B *(Business to Business)*	Empresa vende a empresa.	Proveedor de servicios cloud a empresa cliente.
B2C *(Business to Consumer)*	Empresa vende a consumidor final.	Amazon, AliExpress, SHEIN.
C2C *(Consumer to Consumer)*	Consumidor vende a consumidor.	Wallapop, Vinted, Airbnb.
C2B *(Consumer to Business)*	Consumidor ofrece servicio a empresa.	Marketing de *influencers*.
B2G / B2A *(Business to Government / Administration)*	Empresa vende a la Administración.	Contratos públicos, licitaciones.
C2G / C2A *(Consumer to Government / Administration)*	Ciudadano interactúa con la Administración.	Cita médica, pago de tributos online.

8.6. SEO y SEM

- **SEO** *(Search Engine Optimization)*: conjunto de técnicas para mejorar el posicionamiento **orgánico** (no pagado) de un sitio web en los buscadores.

- **SEM** *(Search Engine Marketing)*: posicionamiento mediante **anuncios pagados** que aparecen en los buscadores para determinadas palabras clave.

8.7. Otros servicios destacables

- **E-learning**: formación en línea mediante plataformas **LMS** *(Learning Management System)*. Gratuitas: Moodle, Canvas, Chamilo. De pago: Blackboard, Saba.
- **IoT** *(Internet of Things)*: conexión a Internet de dispositivos cotidianos (altavoces inteligentes, smartwatches, electrodomésticos, sensores).
- **Big Data**: tecnologías para recopilar y analizar grandes volúmenes de datos a escala.
- **Minería de datos** *(data mining)*: búsqueda automática de patrones y relaciones en grandes conjuntos de datos.
- **Hosting**: servicio que aloja el contenido de una página web para hacerlo accesible.
- **Blogs**, **wikis** y **redes sociales** (Facebook, Instagram, X/Twitter, LinkedIn, TikTok).

9. Buscadores web

Los **buscadores web** o **motores de búsqueda** son sistemas que rastrean, indexan y recuperan contenido de la Web en respuesta a consultas mediante palabras clave. El rastreo lo realizan programas automáticos llamados **robots**, **spiders** o **crawlers**.

Tipo	Funcionamiento	Ejemplo
Jerárquico (general)	Robots o *spiders* rastrean e indexan la web; resultados por relevancia.	Google, Bing, Yahoo, DuckDuckGo, Baidu (China).
Directorio	Categorías elaboradas manualmente por editores; sin rastreo automático.	DMOZ (histórico).
Vertical (especializado)	Restringido a un dominio temático o tipo de contenido específico.	Google Académico, PubMed.
Metabuscador	Lanza la consulta a varios buscadores y agrega resultados; **sin índice propio**.	MetaCrawler.

Operadores de búsqueda habituales (su funcionamiento exacto depende de cada buscador y puede variar con el tiempo):

Operador	Función	Ejemplo
`" "` (comillas)	Búsqueda de **frase exacta**.	`"seguridad informática en la AGE"`
`-` (guion)	Excluye el término que le sigue.	`malware -ransomware`
`+` (más)	Obliga a incluir el término.	`+INCIBE seguridad`
`AND / OR / NOT`	Operadores booleanos: AND incluye ambos, OR cualquiera, NOT excluye.	`SMTP AND correo NOT spam`
`site:`	Restringe la búsqueda a un sitio web concreto.	`site:boe.es accesibilidad`
`..` (dos puntos)	Búsqueda en un rango numérico.	`velocidad 100..1000 Mbps`

RECUERDA

Metabuscador ≠ buscador general: el metabuscador no tiene índice propio; **agrega resultados** de otros buscadores. **DuckDuckGo** es un buscador general orientado a la **privacidad**: no registra datos del usuario. Las **comillas** dan frase exacta, el **guion** excluye y `site:` restringe el dominio.

10. Netiqueta

La **netiqueta** es el conjunto de normas de comportamiento y cortesía aceptadas tácitamente por la comunidad de usuarios de Internet para la comunicación en foros, chats, correos, redes sociales y cualquier servicio de interacción pública. Fue sistematizada por primera vez por **Virginia Shea** en su libro **Netiquette** (1994).

Reglas básicas:

- No escribir en MAYÚSCULAS sostenidas (equivale a gritar y dificulta la lectura).
- No emplear groserías ni insultos.
- No usar espacios de diálogo para publicidad no solicitada.
- Respetar la privacidad de terceros.
- Citar la fuente de la información compartida.
- No distribuir contenido protegido por derechos de autor sin autorización.

11. Marco de referencia: Modelo OSI y Modelo TCP/IP

Para ordenar y comprender la familia de protocolos vista en este epígrafe, conviene situarlos en un marco conceptual. Existen dos modelos de referencia complementarios.

11.1. Modelo OSI (7 capas)

La **Organización Internacional de Normalización** (ISO) publicó en **1984** el **modelo OSI** *(Open Systems Interconnection)* como marco teórico para estandarizar la comunicación entre sistemas de distintos fabricantes. Divide el proceso de comunicación en **siete capas**, aislando las funciones de cada nivel y facilitando el diagnóstico de problemas.

Capa (de arriba a abajo)	Nombre	Función principal	Protocolos / elementos típicos
7	**Aplicación**	Interfaz entre la red y las aplicaciones del usuario.	HTTP, HTTPS, SMTP, FTP, DNS, SSH
6	**Presentación**	Traducción, cifrado y compresión de datos para que sean inteligibles entre sistemas.	SSL/TLS, JPEG, MPEG
5	**Sesión**	Establece, gestiona y cierra las sesiones de comunicación.	NetBIOS, RPC
4	**Transporte**	Segmentación, reensamblado, control de flujo y de errores extremo a extremo.	TCP, UDP
3	**Red**	Enrutamiento de paquetes entre redes; direccionamiento lógico.	IP, ICMP, ARP (*), router
2	**Enlace de datos**	Transferencia de tramas dentro de la misma red; direccionamiento físico (MAC).	Ethernet, Wi-Fi (802.11), switch

(*) **ARP** *(Address Resolution Protocol)* opera en la **frontera entre la capa de red y la de enlace**: resuelve la dirección IP de un equipo de la LAN en su dirección MAC. Los manuales lo encuadran indistintamente en capa 3 (por su función de soporte al direccionamiento

IP) o en capa 2 (porque trabaja con direcciones MAC). | 1 | **Física** | Transmisión de bits en el medio físico: cables, conectores, señales. | Cables, hub, conectores RJ-45 |

11.2. Modelo TCP/IP (4 capas)

El **modelo TCP/IP**, formalizado por la IETF en los RFC 1122 y 1123 (1989), es el modelo **práctico real** sobre el que funciona Internet. Tiene **cuatro capas** que colapsan algunas del OSI:

Capa TCP/IP	Equivalencia OSI	Función	Protocolos clave
4. **Aplicación**	Capas 5 + 6 + 7 del OSI	Interfaz con el usuario. Aplicaciones de red.	HTTP, HTTPS, SMTP, FTP, DNS, SSH, Telnet
3. **Transporte**	Capa 4 del OSI	Control del transporte extremo a extremo.	TCP, UDP
2. **Internet** (Red)	Capa 3 del OSI	Enrutamiento de paquetes entre redes.	IP, ICMP, ARP (frontera con la capa de acceso a red)
1. **Acceso a red** (Enlace)	Capas 1 + 2 del OSI	Transmisión física y en la red local.	Ethernet, Wi-Fi, cables, MAC

MATIZ

El modelo **OSI tiene 7 capas** el modelo **TCP/IP tiene 4 capas**. OSI fue creado por **ISO en 1984** como modelo teórico de referencia; **TCP/IP** es el modelo práctico real de Internet. La capa **Aplicación** del TCP/IP engloba las capas **5 (Sesión) + 6 (Presentación) + 7 (Aplicación)** del OSI. La capa **Acceso a red** del TCP/IP engloba las capas **1 (Física) + 2 (Enlace)** del OSI.

RECUERDA

Las siete capas OSI de **abajo a arriba**: **Física → Enlace → Red → Transporte → Sesión → Presentación → Aplicación**. Mnemónico ascendente: *Francisco Es Raro, Tiene Solo Pocos Amigos*. Sitúa los protocolos clave: **TCP** opera en la capa 4 (Transporte) · **IP** opera en la capa 3 (Red) · **HTTP** opera en la capa 7 (Aplicación) · **Ethernet** opera en la capa 2 (Enlace) · **switch** en la capa 2, **router** en la capa 3, **hub** en la capa 1.

TEMA 8

Epígrafe 3 — Funcionalidades básicas de los navegadores web

1. Qué es un navegador web

Un **navegador web** es una aplicación cliente que solicita recursos a servidores web mediante el protocolo **HTTP** o **HTTPS**, interpreta el código recibido (principalmente HTML, CSS y JavaScript) y lo presenta al usuario de forma visual e interactiva.

Los navegadores actuales soportan también otros protocolos (FTP, *file://*) y utilizan **motores de renderizado** propios para interpretar y mostrar el contenido:

Motor	Navegadores que lo emplean
Blink (Google, fork de WebKit en 2013)	Chrome, Edge (desde 2020), Opera, Brave, Vivaldi.
Gecko (Mozilla, 1998)	Firefox.
WebKit (Apple, derivado de KHTML de KDE en 2001)	Safari.

2. Principales navegadores web

La referencia de trabajo en este epígrafe es **Microsoft Edge**, navegador predeterminado de Windows 10 y Windows 11, aunque las funcionalidades descritas son comunes en mayor o menor medida a todos los navegadores modernos.

El ranking de cuota mundial de uso, según fuentes de seguimiento del mercado (*StatCounter Global Stats* y similares), se actualiza mes a mes; las posiciones relativas se mantienen razonablemente estables:

Posición	Navegador	Empresa / Año	Motor
1	**Google Chrome** – cuota ampliamente dominante.	Google, 2008.	Blink

2	**Safari** – segundo a distancia, propulsado por iOS y macOS.	Apple, 2003. Solo dispositivos Apple.	WebKit
3	**Microsoft Edge** – predeterminado en Windows 10/11. IA Copilot integrada. Buscador por defecto: Bing.	Microsoft, 2015 (sobre Chromium desde **15/01/2020**).	Blink
4	**Mozilla Firefox** – código abierto, orientado a privacidad.	Mozilla Foundation, 2002.	Gecko
5	**Samsung Internet** – predeterminado en dispositivos Android de Samsung.	Samsung, 2012.	Blink
6	**Opera** – pionero en pestañas. Migró a Blink tras la fusión con Chromium.	Opera Software, 1996.	Blink

MATIZ

Edge NO es Internet Explorer. Internet Explorer 11 fue retirado en Windows 10 el **15 de junio de 2022**: la app fue redirigida automáticamente a Microsoft Edge. Edge es un navegador completamente nuevo, basado en **Chromium desde el 15 de enero de 2020**. Edge integra un **«Modo IE»** para sitios heredados que aún requieran ActiveX, pero eso no lo convierte en Internet Explorer. Diferencia de motor: **Edge legacy** (2015-2019) usaba **EdgeHTML** **Edge moderno** (2020 en adelante) usa **Blink** (base Chromium). Son prácticamente dos navegadores distintos.

3. Elementos de una página web

Antes de las funciones del navegador conviene conocer los elementos que pueden aparecer en las páginas web:

- **Banner**: pieza de publicidad que combina imagen, texto y elementos interactivos, insertada en una página para dar visibilidad a una empresa o campaña. Al hacer clic redirige al usuario.
- **Pop-up** o **ventana emergente**: ventana superpuesta al contenido principal. Puede usarse con fines publicitarios, para mostrar avisos legales o para solicitar el consentimiento de cookies. Los navegadores modernos llevan un **bloqueador de pop-ups** activo por defecto.
- **CAPTCHA** *(Completely Automated Public Turing test to tell Computers and Humans Apart)*: mecanismo que verifica que la interacción la realiza un ser humano y no un *bot*. Se presenta como reto visual (texto distorsionado, identificación de imágenes, *puzzles*).
- **FAQ** *(Frequently Asked Questions, Preguntas Frecuentes)*: sección de una página con las dudas más habituales y sus respuestas, para reducir la carga de soporte.
- **Splash screen**: pantalla de presentación o bienvenida que se muestra antes de cargar el contenido principal.

Las páginas web se construyen principalmente con **HTML** (estructura mediante etiquetas), **CSS** (apariencia visual), **JavaScript** (interactividad del lado del cliente) y **XML** (intercambio de datos estructurados).

4. Interfaz del navegador: zonas principales

FIGURA

Captura esquemática de Microsoft Edge con las zonas principales etiquetadas: barra de pestañas (parte superior), botones de navegación (atrás, adelante, actualizar), barra de direcciones u *omnibar* con el icono de favoritos, barra de herramientas (extensiones, menú ···), área de contenido (página web cargada) y barra de estado en la parte inferior que muestra la URL al pasar el cursor sobre un enlace.

Zona	Función
Barra de pestañas	Parte superior; muestra las páginas abiertas como pestañas. Botón + para abrir nuevas.

Botones de navegación	Atrás (`Alt + ←`), Adelante (`Alt + →`) recorren el historial de la pestaña activa. Actualizar (`F5` o `Ctrl + R`) recarga; durante la carga, el botón se transforma en Detener (X) o `ESC`.
Barra de direcciones u *omnibar*	Campo central donde se introduce la URL **o** una consulta de búsqueda. Si el texto no es una URL válida, lanza una búsqueda en el motor predeterminado (Bing en Edge, Google en Chrome).
Área de contenido	Zona principal donde el motor de renderizado interpreta y muestra la página web.
Barra de estado	Pie de la ventana; muestra la URL de destino al pasar el cursor sobre un hipervínculo (antes de hacer clic).

5. Pestañas: atajos y operaciones

La navegación por pestañas permite mantener múltiples páginas abiertas en una sola ventana del navegador. Los atajos están normalizados entre Edge, Chrome y Firefox:

Acción	Atajo
Abrir nueva pestaña	`Ctrl + T`
Cerrar pestaña activa	`Ctrl + W`
Reabrir última pestaña cerrada	`Ctrl + Mayús + T`
Pestaña siguiente / anterior	`Ctrl + Tab` / `Ctrl + Mayús + Tab`
Ir a la pestaña N (1 a 8)	`Ctrl + 1` … `Ctrl + 8`
Ir a la **última** pestaña	`Ctrl + 9`
Abrir enlace en nueva pestaña (sin cambiar)	`Ctrl + clic` sobre el enlace
Abrir enlace en nueva pestaña (y cambiar)	`Ctrl + Mayús + clic`
Nueva ventana del navegador	`Ctrl + N`
Nueva ventana InPrivate	`Ctrl + Mayús + N`
Seleccionar omnibar	`Ctrl + L` / `Alt + D` / `F6`
Completar `www.` y `.com` al nombre escrito	`Ctrl + Intro`

RECUERDA

Ctrl+T = nueva pestaña · **Ctrl+W** = cerrar · **Ctrl+Mayús+T** = reabrir la última cerrada. `Ctrl+1` a `Ctrl+8` van a las pestañas **1 a 8 en orden** `Ctrl+9` va **siempre a la última pestaña**, independientemente de cuántas haya. **Ctrl+clic** abre el enlace en nueva pestaña **sin cambiar** a ella; **Ctrl+Mayús+clic** abre y cambia.

5.1. Teclas de función

Tecla	Función
`F1`	Abre la página de soporte técnico y Ayuda.
`F3` / `Ctrl + F`	Búsqueda **dentro de la página** actual.
`F4` / `Alt + D` / `Ctrl + L`	Selecciona la URL de la barra de direcciones.
`F5` / `Ctrl + R`	Actualiza la página actual.
`F11`	Activa/desactiva el modo pantalla completa.
`ESC`	Detiene la carga de la página.

5.2. Otros atajos con `Ctrl` y `Alt`

Atajo	Función
`Ctrl + Mayús + K`	Duplica la pestaña activa.
`Ctrl + Mayús + A`	Busca entre las pestañas abiertas.
`Ctrl + Mayús + D`	Agrega todas las pestañas abiertas a favoritos.
`Ctrl + Mayús + O`	Abre el panel de favoritos.
`Ctrl + Mayús + B`	Muestra u oculta la barra de favoritos.
`Ctrl + P`	Imprime la página actual.
`Ctrl + Mayús + S`	Captura de pantalla de la página.
`Ctrl + Mayús + U`	Activa la lectura en voz alta.
`Alt + F`	Abre el menú **Configuración y más** (···).

6. Historial de navegación

El **historial de navegación** registra las páginas web visitadas. Debe distinguirse del **historial de la pestaña activa**:

Historial	Qué contiene	Acceso	Persistencia
De pestaña activa (Atrás / Adelante)	Páginas visitadas en esa pestaña durante la sesión actual.	`Alt + ←` / `Alt + →`	Solo mientras la pestaña esté abierta.
Global	Todas las páginas visitadas, agrupadas por día.	`Ctrl + H`	**Persistente entre sesiones** hasta que se borra.

Desde el historial global (`Ctrl + H`) se puede buscar por palabras clave, ver pestañas cerradas recientemente, ver pestañas de dispositivos sincronizados, filtrar por fecha y borrar datos de navegación (historial, descargas, cookies, caché).

> **MATIZ**
>
> Historial de pestaña (Atrás/Adelante) ≠ historial global (`Ctrl+H`). Son **dos funciones distintas**. El botón **Atrás** solo conoce la sesión de la pestaña activa; el **historial global** persiste entre sesiones. Borrar el historial de descargas **NO borra los archivos** del disco: solo elimina el registro. Los archivos permanecen en la carpeta de Descargas.

7. Favoritos o marcadores

Los **favoritos** (Edge) o **marcadores** (Firefox/Chrome) son accesos directos guardados a páginas web de visita frecuente.

Acción	Atajo
Guardar página actual en favoritos	`Ctrl + D`
Panel de favoritos (gestionar, crear carpetas, importar, exportar)	`Ctrl + Mayús + O`
Mostrar/ocultar barra de favoritos	`Ctrl + Mayús + B`

Al guardar (`Ctrl + D`) el navegador propone un nombre editable y permite elegir la carpeta de destino. Desde el panel (`Ctrl + Mayús + O`) se pueden crear carpetas, reorganizar marcadores, importar favoritos de otro navegador y exportarlos a un archivo HTML.

8. Descargas

El panel de descargas (`Ctrl + J`) muestra el estado y el historial de los archivos descargados. Permite pausar, reanudar o cancelar descargas en curso y acceder a la ubicación del archivo en el disco.

La carpeta de destino predeterminada en Windows es `C:\Users\[usuario]\Downloads` (Descargas del perfil del usuario).

> **MATIZ**
>
> Borrar el historial de descargas en el panel del navegador (`Ctrl + J` o `Ctrl + Mayús + Supr`) **NO elimina los archivos del disco**. Los archivos descargados permanecen en la carpeta de Descargas hasta que el usuario los borre manualmente desde el Explorador de archivos.

9. Guardar una página web

El atajo `Ctrl + S` guarda la página activa en el disco local en uno de cuatro formatos:

Formato	Extensión	Descripción
Página web completa	`.html` + carpeta de recursos	El archivo HTML y todos los recursos (imágenes, CSS, JS) en archivos separados, dentro de una carpeta adjunta.
Solo HTML	`.html`	Únicamente el código HTML. Las imágenes y estilos externos no se incluyen.
MHTML / Archivo web	`.mhtml`	Todo el contenido (HTML, imágenes, CSS) en un **único archivo autocontenido**.

Archivo de texto	`.txt`	Solo el texto visible de la página, sin formato ni imágenes.

10. Búsqueda en página y en Internet

Los navegadores ofrecen **dos tipos de búsqueda** que conviene distinguir:

- **Búsqueda en la página** (`Ctrl + F` o `F3`): localiza texto dentro del documento actualmente cargado. Resalta las coincidencias y permite navegar entre ellas. **No genera tráfico de red.**
- **Búsqueda en Internet**: se realiza escribiendo términos en la barra de direcciones (omnibar), que los reenvía al motor de búsqueda predeterminado. **Sí genera tráfico de red** al buscador.

> **MATIZ**
>
> `Ctrl + F` = búsqueda **dentro del documento cargado**, sin tráfico de red. **Omnibar** = búsqueda **en Internet**, con tráfico de red al buscador. Son funciones completamente distintas aunque ambas se denominen «búsqueda».

11. Hipervínculos e imágenes

Los **hipervínculos** son elementos de texto o imagen que, al ser clicados, dirigen al usuario a otro recurso. El texto de un hipervínculo no visitado aparece típicamente en **azul subrayado** tras visitarlo, cambia a **morado**. Al pasar el cursor sobre un hipervínculo, la **barra de estado** del navegador muestra la URL de destino antes de hacer clic, lo que permite verificar el enlace.

Las **imágenes** en la web utilizan distintos formatos según el contenido:

Formato	Características	Uso típico
JPEG (extensiones `.jpg` / `.jpeg`)	Compresión **con pérdida**. No admite transparencia.	Fotografías.
PNG	Compresión **sin pérdida**. Admite transparencia.	Gráficos, logotipos, iconos.

GIF	Máximo 256 colores. Admite **animación**.	Animaciones sencillas.
WebP	Compresión moderna eficiente. Admite transparencia y animación.	Uso web moderno; combina ventajas de JPEG y PNG.

12. Caché del navegador

La **caché del navegador** es un almacenamiento temporal en el disco local donde el navegador guarda copias de los recursos web descargados (imágenes, CSS, JavaScript, fuentes, HTML). El propósito es acelerar la carga de páginas visitadas con frecuencia: en visitas sucesivas el navegador recupera los recursos de la caché local en lugar de volver a descargarlos del servidor.

El inconveniente es que la caché puede mostrar contenido **desactualizado** si el servidor ha modificado los recursos. La **recarga forzada** (`Ctrl + Mayús + R`) obliga al navegador a descargar todos los recursos del servidor ignorando la caché. Para borrarla por completo: `Ctrl + Mayús + Supr` ⟶ marcar «**Imágenes y archivos almacenados en caché**».

MATIZ

Caché ≠ cookies. La caché almacena **recursos** de la página (imágenes, CSS, JS) para acelerar la carga. Las cookies almacenan **datos del usuario** (sesión, preferencias, seguimiento). `Ctrl + R` o `F5` = recarga normal (puede usar caché). `Ctrl + Mayús + R` = recarga **forzada** (ignora caché, descarga todo del servidor).

13. Cookies

Las **cookies** son pequeños archivos de texto que los servidores web envían al navegador del usuario para que los almacene en su equipo. En visitas posteriores el navegador devuelve automáticamente las cookies al servidor, lo que permite al sitio reconocer al usuario o recuperar su estado. Tres usos principales:

- **Gestión de sesión** e **identificación** (mantener al usuario autenticado).
- **Almacenamiento de preferencias** (idioma, configuración).

- **Analítica y publicidad** (seguimiento del comportamiento para perfiles publicitarios).

El **Reglamento General de Protección de Datos (RGPD)**, junto con el **art. 22.2 de la Ley 34/2002 LSSI-CE**, exige que los sitios web soliciten el **consentimiento informado** del usuario para instalar cookies no estrictamente necesarias. Las cookies estrictamente necesarias para el funcionamiento del sitio (gestión de sesión, carro de compra) **no requieren consentimiento** las de analítica y publicidad **sí**.

Tipo de cookie	Duración	Uso típico
De sesión	Se elimina al cerrar el navegador.	Autenticación durante la visita.
Persistente	Persiste hasta su fecha de expiración.	Preferencias, recordar usuario.
De terceros	La instala un dominio distinto al visitado.	Publicidad y seguimiento entre sitios.

14. Seguridad en el navegador

Los navegadores modernos incorporan varias capas de seguridad:

- **Indicador HTTPS / candado**: confirma que la comunicación está cifrada mediante TLS. **No garantiza** que el sitio sea legítimo (un sitio de *phishing* puede tener HTTPS).
- **Prevención de seguimiento** (en Edge: **Básico**, **Equilibrado** —predeterminado— o **Estricto**): bloquea rastreadores de terceros.
- **Bloqueador de ventanas emergentes** (pop-ups), activo por defecto.
- **Gestor de contraseñas integrado**: en Edge, Configuración → Contraseñas; permite guardar y autocompletar credenciales.
- **Filtro de sitios sospechosos**: en Edge, **Microsoft Defender SmartScreen** advierte ante descargas o sitios potencialmente maliciosos detectados por su servicio de reputación.

15. Navegación privada e invitado

La **navegación privada** (**InPrivate** en Edge, **Incognito** en Chrome, **Privada** en Firefox) abre una sesión aislada en la que el navegador no guarda localmente historial, cookies,

datos de formularios ni archivos de caché al cerrar la ventana. Los archivos descargados y los favoritos guardados durante la sesión privada **sí se conservan** en el disco.

La **navegación como invitado** (distinta de la privada) está pensada para un usuario ocasional: no guarda historial, cookies, descargas ni favoritos, y no se tiene acceso a los favoritos ni al perfil del usuario principal del equipo.

Elemento	Navegación normal	InPrivate / Incognito	Cuenta Invitado
Historial de navegación	Se guarda	No se guarda al cerrar	No se guarda
Cookies y datos de sesión	Se conservan	Se eliminan al cerrar	No se guardan
Caché y archivos temporales	Se conservan	Se eliminan al cerrar	No se guardan
Datos de formularios	Se conservan	No se guardan	No se guardan
Archivos descargados	Se guardan en disco	Se guardan en disco	Se guardan en disco
Acceso a favoritos del perfil	Sí	Sí	No
Guardar nuevos favoritos	Sí	Sí	No
Acceso a contraseñas guardadas	Sí	Sí	No
Datos asociados al usuario	Sí	No	No

Atajo de navegación privada
Edge: `Ctrl + Mayús + N`
Chrome: `Ctrl + Mayús + N`
Firefox: `Ctrl + Mayús + P`

MATIZ

La navegación privada **NO anonimiza** al usuario en Internet: el ISP, los servidores web y el administrador de red siguen viendo la dirección IP del usuario y los sitios visitados. **InPrivate** solo impide que se guarden datos de navegación en el dispositivo local. Para anonimato real frente al ISP se necesita VPN o Tor; ni siquiera estas soluciones son perfectas.

16. Extensiones

Las **extensiones** son pequeños programas que se añaden al navegador para ampliar sus funcionalidades: bloqueadores de publicidad (uBlock Origin, AdBlock), gestores de contraseñas (Bitwarden, 1Password), traductores, etc.

En Edge se gestionan desde `edge://extensions/` o desde el menú ··· → **Extensiones**. Pueden instalarse desde la **Microsoft Edge Add-ons Store** o, al ser Edge un navegador basado en Chromium, también desde la **Chrome Web Store**.

Es recomendable revisar los **permisos** que solicita cada extensión antes de instalarla: pueden acceder a los datos de las páginas visitadas, lo que las convierte en un vector de riesgo si proceden de un desarrollador desconocido.

17. Códigos de estado HTTP

Los **códigos de estado HTTP** son números de tres cifras que el servidor devuelve al navegador como respuesta a cada petición, informando del resultado de la operación. Se organizan en **cinco grupos** según el primer dígito:

Rango	Significado general	Códigos clave
1xx – Informativo	La petición se está procesando.	`100 Continue`, `102 Processing`
2xx – Éxito	La petición se ha procesado correctamente.	`200 OK`, `206 Partial Content` (descarga parcial)
3xx – Redirección	El recurso se ha movido a otra ubicación.	`301 Moved Permanently`, `302 Found` (temporal)

4xx – Error del cliente	El error está en la petición del cliente.	`400 Bad Request`, `401 Unauthorized`, `403 Forbidden`, `404 Not Found`, `408 Request Timeout`
5xx – Error del servidor	El error está en el procesamiento del servidor.	`500 Internal Server Error`, `502 Bad Gateway`, `503 Service Unavailable`

MATIZ

403 Forbidden: el recurso **existe**, pero el servidor **deniega el acceso** (sin permiso). El servidor conoce el recurso y decide no entregarlo. **404 Not Found**: el recurso **no existe** en el servidor (URL incorrecta o recurso eliminado); el servidor no lo encuentra. En 403 el servidor niega, en 404 el recurso no existe — es la distinción más frecuente del grupo 4xx.

18. Amenazas habituales en la navegación web

Aunque las nociones generales de seguridad informática se tratan en el Tema 1 del Bloque VI, conviene fijar aquí las amenazas que afectan directamente a la navegación web y que los navegadores tratan específicamente de mitigar.

18.1. Phishing

El **phishing** consiste en el envío masivo de correos electrónicos fraudulentos —y, por extensión, mensajes en redes sociales o anuncios— que imitan la identidad de una entidad de confianza (banco, Administración, empresa tecnológica) para engañar al destinatario y conseguir que proporcione sus credenciales o descargue un archivo malicioso. Los enlaces del correo llevan a sitios web falsos que reproducen la apariencia del original.

Los navegadores incorporan filtros de reputación que advierten al usuario cuando un sitio está identificado como fraudulento (en Edge, **Microsoft Defender SmartScreen** en Chrome, **Safe Browsing**). El usuario puede verificar visualmente la URL antes de introducir credenciales: dominios mal escritos, certificados emitidos a entidades distintas o ausencia de HTTPS son señales de alerta.

18.2. DNS spoofing

El **DNS spoofing** *(suplantación de DNS)* es un ataque en el que el atacante manipula las respuestas del servidor DNS para asociar un nombre de dominio legítimo a una **dirección IP fraudulenta** bajo su control. Cuando el usuario escribe la URL correcta del banco o del servicio público, el DNS comprometido devuelve la IP de una página falsa que imita a la original, permitiendo el robo de credenciales. El usuario **no percibe nada anómalo** porque ha escrito la URL correcta.

La mitigación pasa por usar servidores DNS de confianza, **DNSSEC** *(DNS Security Extensions)* que firma criptográficamente las respuestas, y **DoH** *(DNS over HTTPS)* o **DoT** *(DNS over TLS)* que cifran las consultas. Edge y Chrome admiten DoH desde sus opciones de privacidad y seguridad.

> **MATIZ**
>
> En el **phishing** el usuario es engañado para que **interactúe con un señuelo fraudulento** (un enlace, un adjunto, un formulario, una llamada): el atacante necesita su acción. En el **DNS spoofing** el usuario puede haber **escrito correctamente la URL**, pero la resolución DNS manipulada lo redirige a la IP del atacante; por eso es más difícil de detectar a simple vista, aunque el certificado del sitio, **HSTS** y las advertencias del navegador pueden delatar el fraude.

TRES FORMAS DE EMPEZAR

La app Persevera complementa este temario con las herramientas para estudiarlo:

tests · flashcards con repaso espaciado · supuestos

simulacros · mindmaps · tutor IA · planificador

Suscripción mensual sin permanencia. Cancelas cuando quieras desde la app.

WEB

perseveraoposiciones.com

IOS

iPhone / iPad

ANDROID

Google Play