

Internet



Operaciones auxiliares con TIC

Contenidos

- ¿Qué es Internet?
- **World Wide Web** → WWW
- Navegación por la Web
- Buscadores
- Certificados y firmas digitales
- Protección del sistema operativo.



Objetivos

- Conocer las características de la red Internet.
- Distinguir los conceptos Internet e Intranet.
- Conocer las características del servicio **WWW**.
- Utilizar distintos navegadores para navegar por la red.
- Realizar búsquedas en Internet.
- Identificar páginas seguras y no seguras.
- Utilizar certificados y firmas digitales.

Comenzamos diciendo que ...

- En una red de área local, los ordenadores se comunican entre sí en un área geográfica reducida, típicamente un edificio, mientras que en la red de internet el área geográfica de comunicación se amplía, interconectándose los ordenadores entre sí a nivel mundial.
- Internet es una inmensa red de comunicación e intercambio de información, de forma que todos los ordenadores conectados a la red van a poder intercambiar cualquier información entre sí, sin importar su localización física.
- La red de internet surge a finales del siglo XX convirtiéndose en muy poco tiempo en un nuevo canal de comunicación y en una nueva forma de trabajar y hacer negocios.
- Buscadores como **Google** o la plataforma de redes sociales como **Facebook** o de vídeos **YouTube** aglutinan un gran porcentaje de conexión de usuarios a diario a nivel mundial.

¿Qué es Internet?



Hoy día, **Internet** es la herramienta más utilizada en todo el mundo para la búsqueda de **información** y la **comunicación** (mediante email, chats, foros, blogs, etc.).



Internet y las TICs

Pero Internet va aun más allá: con el uso de las *Tecnologías de la Información y la Comunicación (TIC)*, Internet también es un mundo virtual donde se ofrecen recursos y herramientas de **servicios** administrativos y comerciales (compras, transferencias bancarias, matriculaciones en cursos, gestiones burocráticas, etc.), **entretenimiento y ocio** (juegos on-line, etc.), el **aprendizaje** (tutoriales on-line, plataformas educativas) y la difusión del conocimiento en general

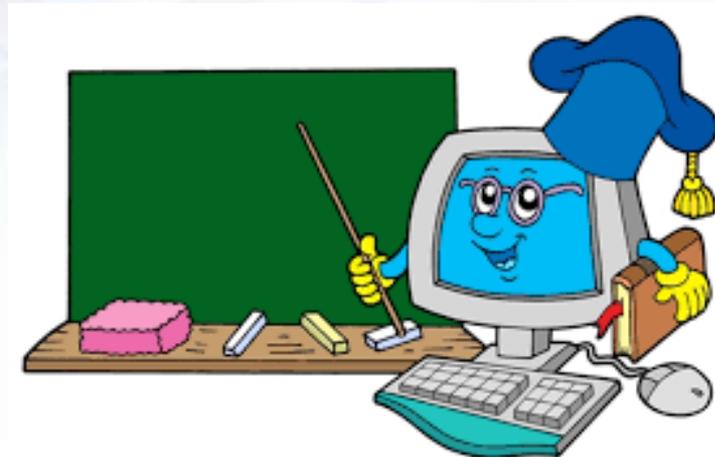


Internet



Internet y las TIC

- Las **TIC** se basan en el empleo de programas y medios electrónicos y telemáticos para conservar, gestionar, encontrar, transmitir y proteger información, favoreciendo la conexión instantánea entre personas, entidades y organismos que se encuentran distantes entre sí geográficamente, utilizando los canales denominados *autopistas de la información*.



Historia de Internet

- Los orígenes de Internet se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como **ARPANET**, entre tres universidades en California y una en Utah, Estados Unidos. ARPANET era un proyecto encargado por el ejército norteamericano para la comunicación de sus organismos en el país.



Historia de Internet

- En 1974 se cambió el protocolo de comunicación original de ARPANET por el protocolo **TCP/IP**.
- En 1983 se estandarizó el protocolo TCP/IP siendo un protocolo utilizado por la mayoría de las redes.
- En 1990 desaparece ARPANET por otras redes con velocidades más elevadas.
- En los años 90 Internet se consolida como una red de redes utilizándose con fines comerciales.
- En 1994 existían tres millones de host distribuidos por 146 países uniendo más de 25.000 redes.
- A comienzos del siglo XXI Internet ha supuesto una revolución social, al permitir nuevas formas de trabajar, comerciar, comunicarnos, entretenernos, aprender, etc.

Red de Redes

- **Internet** es un conjunto de redes interconectadas a nivel mundial con la particularidad de que cada red que conecta es independiente y autónoma.
- Es **universal**, extendiéndose, prácticamente, por todo el mundo.
- Es fácil de usar, a través de los navegadores, no hace falta tener profundos conocimientos de informática.
- Contiene gran cantidad de información a la que se puede acceder de forma libre.



Internet



Identificación en la red

- Todos los ordenadores conectados a Internet tienen que estar identificados de forma unívoca mediante una **dirección IP**.
- La información que los ordenadores clientes solicitan a los servidores, puede ser: páginas web, correos electrónicos, vídeos, imágenes, etc.
- El ordenador cliente tiene que tener instalado un programa cliente en su ordenador para poder solicitar el servicio deseado.
- Estos programas se ocupan de gestionar la comunicación con el servidor y de presentar al usuario una interfaz para poder introducir comandos y para mostrar los datos en pantalla.

Modelo cliente-servidor

- Internet utiliza el modelo cliente-servidor:

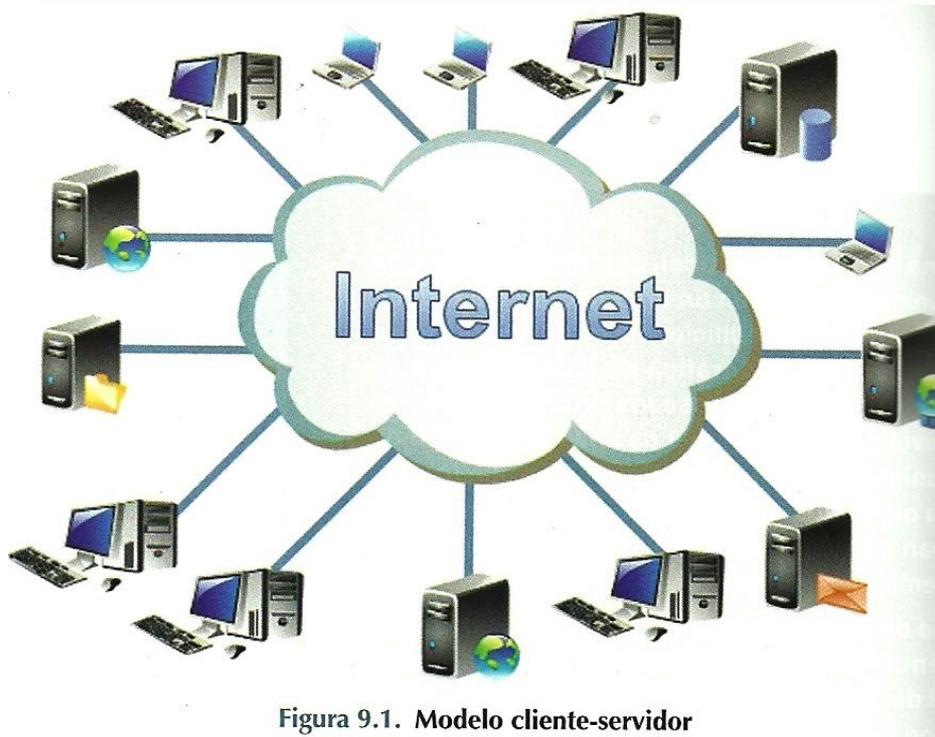


Figura 9.1. Modelo cliente-servidor

- **Ordenadores clientes:** son los que acceden a Internet como ordenadores portátiles, dispositivos móviles, etc.
- **Ordenadores servidores:** son los que ofrecen los servicios y la información que comparten con los ordenadores clientes. Servidores web, de correos, DNS, FTP, etc.

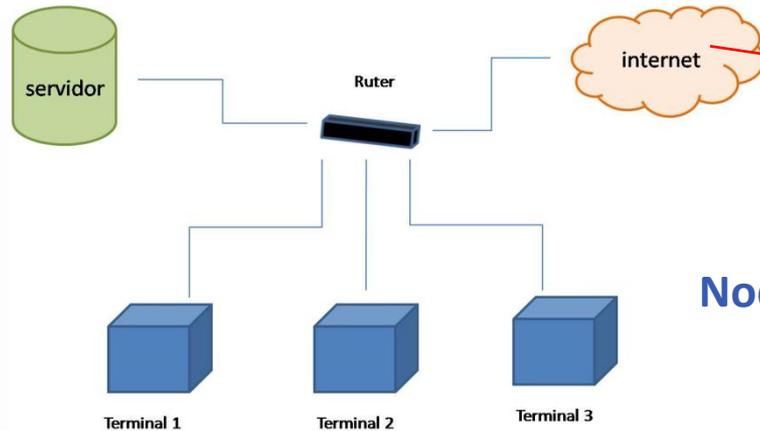
Componentes de Internet

- **Nodos o dispositivos de red:** ordenadores y enrutadores capaces de procesar y distribuir la información por toda la red.
- **Infraestructura:** líneas de comunicación que interconectan los ordenadores que forman internet salvando las distancias físicas que existen entre ellos.
- **Direcciones IP y nombres DNS (*Domain Name System*):** cada nodo de internet tendrá una dirección única, una forma de ser identificado dentro de la red mundial y un nombre de dominio DNS que asocia esa dirección a un nombre fácil de recordar.

Componentes de Internet

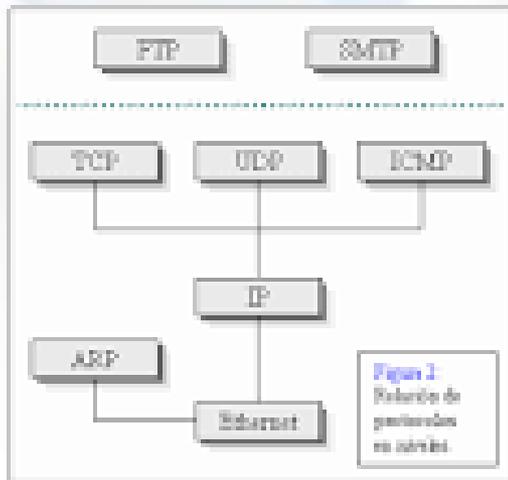
- **Reglas y normas:** dictan el funcionamiento de toda la red y de los ordenadores que forman parte de Internet y están recogidas en unos documentos llamados **RFC**, *Request for Comments* (Petición de Comentarios).
- **Protocolos:** Conjunto de reglas usadas por los ordenadores para comunicarse a través de una red. Destaca el protocolo de red (*Internet Protocol*, IP) y el de transporte (*Transmission Control Protocol*, TCP).
- **Aplicaciones:** conjunto de herramientas que permiten al usuario utilizar las capacidades de Internet de forma sencilla, como telnet, ftp, mail, www, http, etc.

Componentes de Internet



Nodos

Infraestructura



Protocolos



Aplicaciones

Tipos de conexión a Internet

- **RTC:** Red Telefónica Conmutada, Mediante Modem, con una velocidad máxima de 56Kbps. No se puede transmitir a la misma vez voz y datos.
- **ADSL:** Línea de Abonado Digital Asimétrica. Permite transmitir voz y datos simultáneamente sin que exista interferencia. Posee una velocidades de bajada de información superiores a las de subida de datos. La evolución de la tecnología ADSL se denomina VDLS, especialmente para transmisión señales TV HD por la red.

Para que un usuario se conecte mediante ADSL a Internet necesita contratar una línea ADSL con algún ISP.

Tecnología	Velocidad de bajada	Velocidad de subida
ADSL	8 Mbps	0,9 Mbps
ADSL2	12 Mbps	0,9 Mbps
ADSL2+	24 Mbps	3,5 Mbps
VDSL	55 Mbps	6 Mbps

Tipos de conexión a Internet

- **Wi-Fi.** Es una conexión inalámbrica que permite tasas de velocidades de transmisión de hasta 600 Mbps del estándar 802.11 n.
- **Cable.** Utiliza cable coaxial para llegar desde el cliente al proveedor. Se realiza con fibra óptica que es un cable de transmisión a más velocidad que el de la línea telefónica y comparte Internet, TV y telefonía.
- **FTTH.** Se basa en la utilización de fibra óptica hasta los hogares para transmitir telefonía, Internet y TV. Llega hasta el edificio y se espera que remplace a las líneas ADSL.

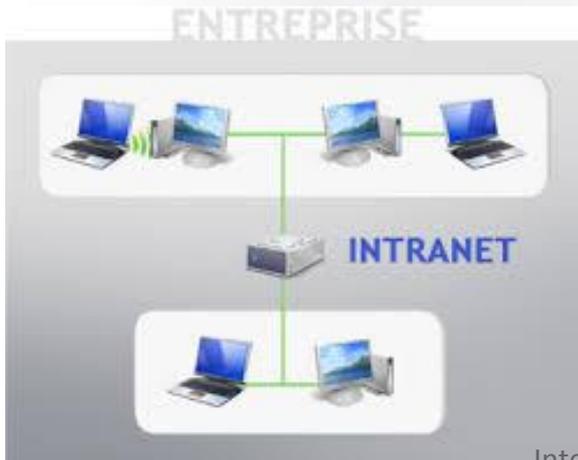
Tipos de conexión a Internet

- **Vía satélite.** Esta conexión se utiliza en lugares remotos, en el ámbito rural y las zonas de alta montaña, donde no llega el ADSL y el cable. Tiene que instalar una antena parabólica y ofrece alta velocidad y servicios de TV por satélite.
- **Módem USB móvil.** Permite acceder a Internet desde cualquier ordenador que dispongo de cobertura. Consiste en un pen drive USB con la misma tecnología 3G implementada por los móviles.
- **PLC.** (Power Line Communication) es una tecnología que ofrece conexión a Internet a través de la red eléctrica. También se utiliza para comunicar ordenadores en una LAN, en lugar de utilizar WiFi o cableado Ethernet.

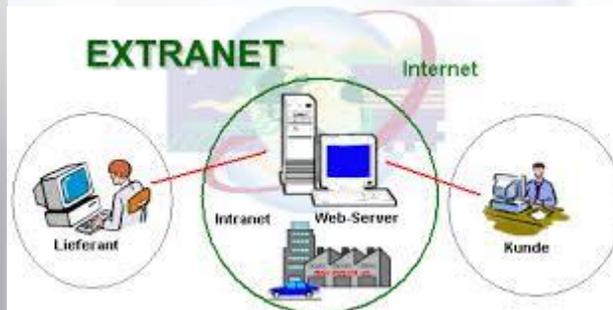
Diferencias entre Internet, Intranet y Extranet

Red	Acceso	Usuarios
Internet	Público	Cualquier persona
Intranet	Privado	Empleados de la organización
Extranet	Semipúblico	Empleados, clientes y proveedores

- **Internet** es una red de área amplia (WAN) de acceso público.
- Una **intranet** es una red de ordenadores privados que utiliza tecnología Internet para compartir de forma segura dentro de una organización parte de sus sistemas operacionales y de información. El término *intranet* se utiliza en oposición a *Internet*, red entre organizaciones, haciendo referencia, por contra, a una red comprendida en el ámbito de una organización.
- Una **Extranet** tiene recursos de una empresa disponibles a través de Internet, aunque de forma segura, utilizando un usuario y contraseña para acceder y asegurar los datos.



Internet



World Wide Web (WWW)

World Wide Web (Red global mundial), también llamado Web, es el servicio más utilizado en Internet. La Web desarrolla un medio de publicación e intercambio de información novedoso, donde los datos se almacenan en una red de nodos conectados por enlaces.



<https://www.google.es/search?client=aff-max>

¿Qué es World Wide Web (WWW)?

SABÍAS QUE: ?

La WWW junto con URL, HTML y HTTP se desarrollaron en el año 1990 por Tim Berners-Lee en el CERN en Suiza. En 1993 el CERN (Organización Europea para la Investigación Nuclear) anunció que la web sería gratuita para todos.

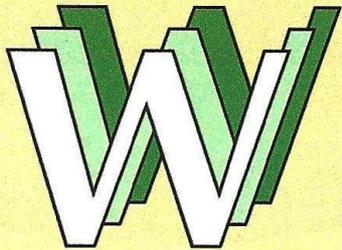


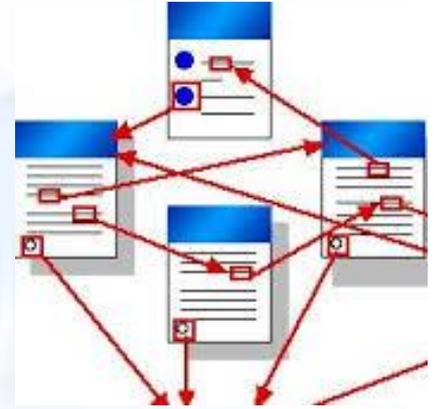
Figura 9.8. Antiguo logo diseñado por Robert Cailliau

- Se puede definir la **World Wide Web (WWW)** como un sistema de información distribuido basado en hipertextos (enlaces que permiten saltar de un lugar a otro) y en multimedia (puede manejar contenidos con texto, gráficos, video, sonido, etc.). Que se transmite por Internet.



¿Qué es el Hipertexto?

- El **hipertexto** es una forma de escritura no secuencial, que permite al lector elegir la secuencia que va a seguir y que se presenta en una pantalla interactiva facilitando la navegación. Esta navegación consiste en activar con el ratón o el teclado en ciertas zonas sensibles y destacadas llamadas **hiperenlaces**.
- La mayoría de los **navegadores** funcionan de forma parecida. Las diferencias de aspecto de las páginas Web sólo tienen que ver con su diseño de creación.
- Todos los recursos existentes en Internet, como páginas, archivos, gráficos, etc. tienen una **URL** (Localizador Uniforme de Recursos) distinta que los identifica. Es lo que se conoce habitualmente por el nombre de **dirección web**.

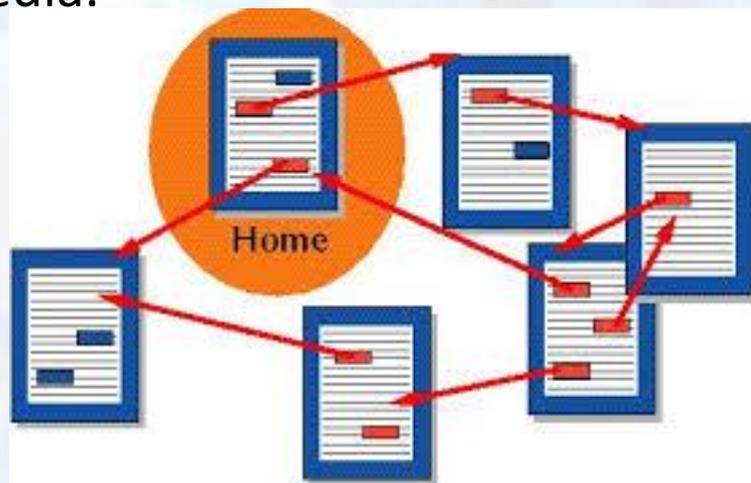


rtext

Una mano cursor blanca con un índice extendido, apuntando hacia el texto "rtext".

Recuerda

- El **hipertexto** es texto que contiene enlaces (links) a partir de los cuales se puede acceder a información ubicada en otra zona del texto, o en otra zona del mundo, permitiendo acceder a archivos multimedia.



- Los enlaces se establecen por medio de ciertas imágenes o palabras que aparecen resaltadas en la pantalla, generalmente con color azul y subrayadas.

[La Web](#) [Imágenes](#) [Vídeos](#) [Maps](#) [Noticias](#) [Libros](#) [Gmail](#) [Más](#)

Figura 9.9. Ejemplos de hipertextos en una página web

Recuerda

- El éxito de la **www** se debe a:
 - El **Hipertexto**, que permite acceder a cualquier página de Internet localizada en cualquier parte del mundo.
 - El contenido **multimedia**, ya que maneja información que combina texto, gráficos, imágenes, sonido, vídeos, etc.
 - La facilidad de la creación de páginas web mediante el lenguaje **HTML**.
- Un **dominio** de Internet es un nombre que identifica a un sitio web, creado con caracteres alfanuméricos de forma que es más fácil de recordar que los números de su dirección IP. Los dominios se registran pagando de forma periódica la exclusividad del nombre de dominio.



Página web, sitio web y portal



- La información en **WWW** se representa mediante páginas web que son documentos escritos en lenguaje **HTML**, que pueden incluir diferentes tipos de información: textos, gráficos, animaciones, audio, vídeo e hipertexto.
- Este programa emplea un protocolo llamado **HTTP**, que funciona sobre TCP/IP, y que se encarga de gestionar el aspecto de las páginas y los enlaces.

Página web, sitio web y portal

- Un nombre de dominio se compone de tres partes:
 1. El primer parámetro suele ser **www** para indicar que es un sitio web.
 2. El segundo parámetro es el **nombre del dominio**, que suele ser el nombre de la organización.
 3. Y el tercer parámetro se refiere al tipo de organización. Por ejemplo **.com**, **.org**, **.es**, etc.
- La **Web** no es Internet, sino uno de los servicios disponibles gracias a Internet.
- Las **páginas Web** son documentos de **hipertexto**.

WWW.
miSitio
.com

www.midominio.es



.COM .EU
.ES .ORG
.NET .PRO
.MOBI .INFO

Recuerda

- Todo el texto y el hipertexto está en los documentos **HTML** y el resto de contenidos (imágenes, sonidos, vídeos) se almacena en archivos separados a los que se les hace referencia. También es frecuente encontrar en las páginas Web componentes activos (escritos con otras tecnologías como **Flash, Javascript** o **PHP**) que permiten que las páginas tengan dinamismo y sean un medio de interacción con aplicaciones remotas como bases de datos, sistemas de ficheros, etc.
- La Web equivale a una **enciclopedia gigante** que abarca todo el mundo y cuyos contenidos totales se desconocen por la rapidez con la que cambia. Cualquier usuario con un servidor Web puede publicar lo que quiera, con la única limitación de su responsabilidad legal.

Portales horizontales

- Son portales dirigidos a todo tipo de público, ya que incluyen información amplia con temática variada. Ejemplo de estos portales serían: Yahoo, MSN, Terra, etc

Blogs	Foros	Autopista.es	Deportes	Móviles	Nat Geo	Tecnología	Callejero	Empleo
Chat	Comunidad	Cine	Invertia	Mujer	Noticias	Televisión	Descargas	Kedin
Correo	Pixbox	Corazón	Juegos	Música	Pressing Catch	TerraTV	El tiempo	Loterías

FOROS & CHATS



Internet



YAHOO! COMPANY INFORMATION



Portales verticales

- Son portales con contenidos especializados dirigidos a determinados públicos, por ejemplo, portales sobre empleo, educativos, inmobiliarios, deportivos, médicos, etc.



Estándares de WWW

→ URL

→ HTML

→ HTTP

URL (Identificador de recurso uniforme)

- Es la dirección utilizada en Internet para nombrar y localizar un recurso de un host (página web, imagen, fichero, etc.). El formato de una dirección URL es:

protocolo://host/directorio/archivo

- **Protocolo:** para el intercambio de páginas web es el protocolo **http**.
- **Host:** puede ser una dirección IP o un nombre de dominio.
- **Directorio:** en un host la información suele estar organizada en directorios.
- **Archivo:** es el nombre del archivo solicitado con una extensión que indica el tipo de documento del que se trata, que suele ser **html**.
- Por ejemplo, la dirección URL de la página inicial del buscador Google es <http://www.google.es>, no contiene ni directorio ni archivos en su dirección.

HTML (Lenguaje de marcado de hipertexto)

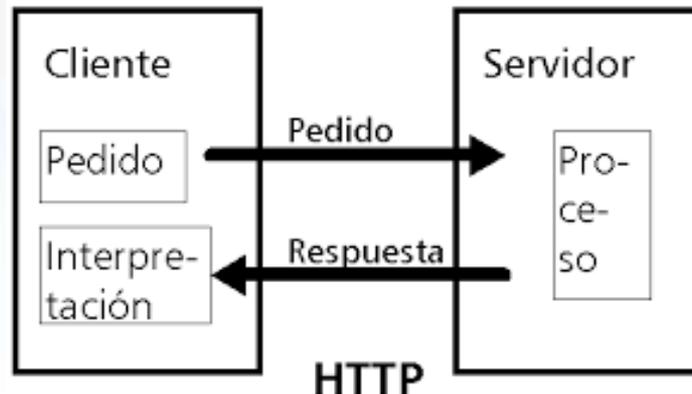


- **html** es un grupo de códigos de programación empleado para describir la forma de mostrar las páginas web en un navegador.



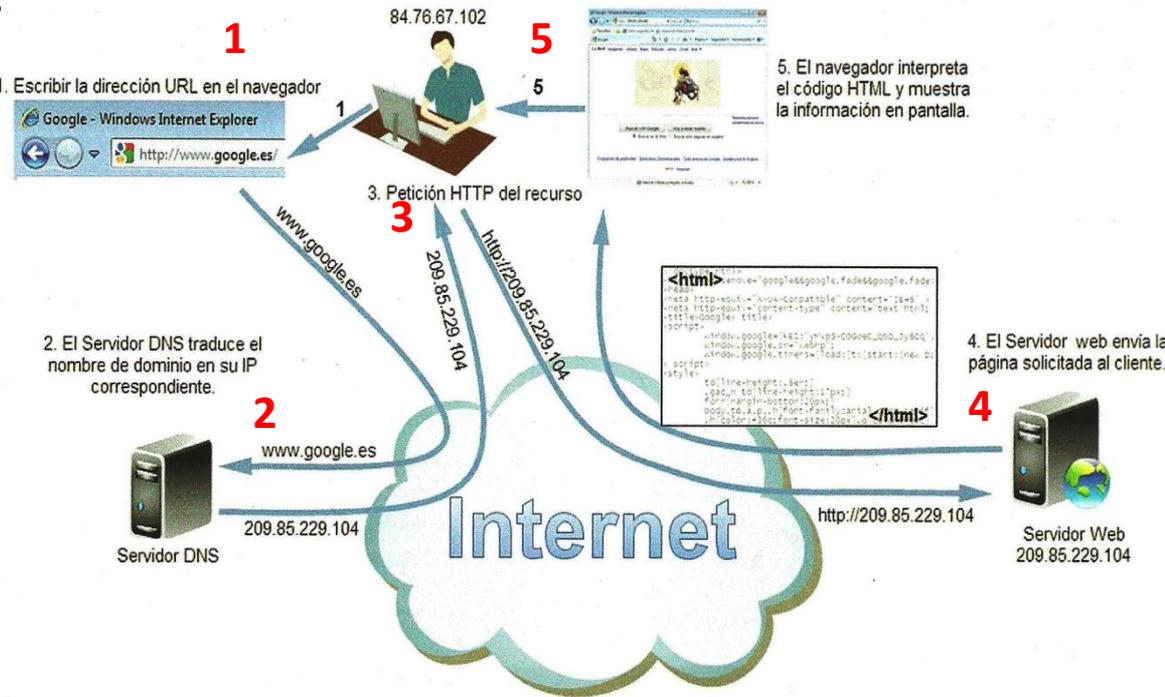
HTTP (Protocolo de transferencia de hipertexto)

- **HTTP** es el conjunto de reglas empleado para describir cómo se envían y reciben los documentos web por internet. Proporciona las reglas para que los navegadores hagan peticiones de páginas web y los servidores entreguen el código de las páginas web.



Ejemplo de funcionamiento del servicio www

1. Escribimos una dirección **URL** en nuestro navegador web.
2. El servidor **DNS** traduce el nombre del dominio del host (servidor web) solicitado en la dirección URL en su correspondiente dirección IP.
3. El ordenador envía una petición **HTTP** al servidor web a través de su IP indicando el recurso solicitado.
4. El servidor web encuentra el documento y envía el código **HTML** al navegador.
5. El navegador interpreta el código HTML y muestra la información en pantalla.



Navegación por la Web

- Para poder visualizar los documentos que proporcionan los servidores web es necesario un programa llamado **navegador web** (browser) que se encarga de interpretar las páginas **HTML** y mostrarla en pantalla. La utilidad de un navegador web es que sirve para movernos (navegar) por Internet.



Internet



Navegadores Web

SABÍAS QUE: ?

Según los datos de la empresa Net Application que monitoriza más de 40.000 sitios web, los porcentajes de cuota de mercado de los navegadores son:

Navegador	%
 Internet Explorer	62,12
 Firefox	24,43
 Chrome	5,22
 Safari	4,53
 Opera	2,97
Otros	0,68

- **Internet Explore** de Microsoft viene por defecto en todos los sistemas operativos de Microsoft Windows.
- **MozillaFirefox** es muy ligero y compite con Internet Explore. Ha sido el sustituto de Netscape.
- **GoogleChrome** se caracteriza por su sencillez y por su velocidad a la hora de iniciarse y de cargar páginas web.
- **Safari** ha sido creado por Apple para todos sus ordenadores y dispositivos móviles.
- **Opera** destaca por su reducido , por su velocidad y por su constante innovación.

Trabajando con un navegador Web

- Los dos navegadores Web más utilizados (**Internet Explore** y **Firefox**) tienen una interfaz similar basada en una ventana con barras de desplazamiento en la que se visualiza la información de las páginas Web.
- La ventana de un navegador, al igual que la mayoría de ventanas de Windows, se compone de los siguientes elementos:
 - Barra de títulos.
 - Barra de direcciones.
 - Cuadro de búsqueda.
 - Barra de menús.
 - Barra de herramientas.
 - Área de la ventana
 - Barra de estado.



Recuerda

- La **Web** no es Internet, sino uno de los servicios disponibles gracias a Internet.
- Las **páginas Web** son documentos de **hipertexto**.
- El **hipertexto** es una forma de escritura no secuencial, que permite al lector elegir la secuencia que va a seguir y que se presenta en una pantalla interactiva facilitando la navegación. Esta navegación consiste en activar con el ratón o el teclado en ciertas zonas sensibles y destacadas llamadas **hiperenlaces**.
- La mayoría de los **navegadores** funcionan de forma parecida. Las diferencias de aspecto de las páginas Web sólo tienen que ver con su diseño de creación.
- Todos los recursos existentes en Internet, como páginas, archivos, gráficos, etc. tienen una **URL** (Localizador Uniforme de Recursos) distinta que los identifica. Es lo que se conoce habitualmente por el nombre de **dirección web**.

Buscadores

- Una de las principales características de Internet es que contienen gran cantidad de Información, es una gran biblioteca distribuida en servidores de todo el mundo. El principal inconveniente es poder encontrar rápidamente la información que se está buscando.
- Un buscador es una aplicación que a través de una página web permite al usuario buscar información sobre un tema en internet.
- El buscador consulta una base de datos en donde se relacionan las páginas web con sus contenidos y como resultado muestra al usuario un listado de enlaces (links) de páginas relacionadas con el contenido buscado.



Internet



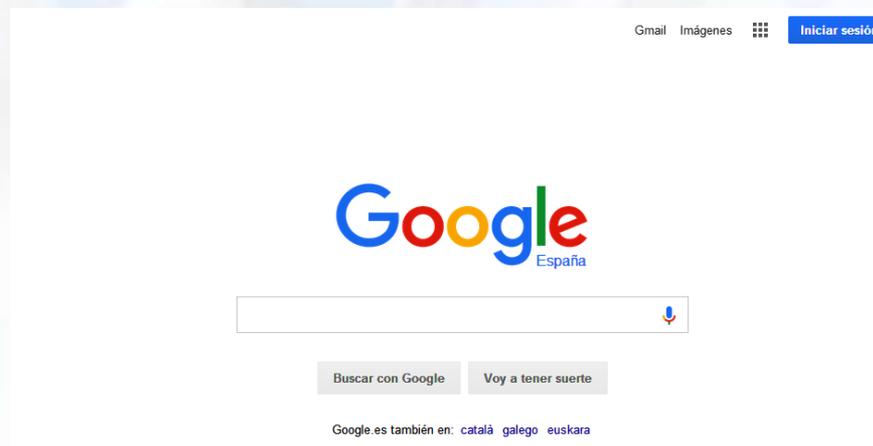
Buscadores

- Actualmente **Google** es el buscador más utilizado en el mundo con una cuota de mercado superior al 80%. Le siguen, con cuotas inferiores al 10%, los buscadores **Yahoo!**, **Bing**, **Baidu** (buscadores más utilizado en china), **Ask**, **AOL** y **AltaVista**.
- Los buscadores se clasifican en:
 - **Buscadores tipo directorio:** se realiza la búsqueda por temática o categorías jerarquizadas. El usuario accede al que le interesa y después ejecuta el buscador. El más utilizado es **Yahoo**.
 - **Motores de búsqueda tipo índice:** se realiza la búsqueda por palabras claves. La información se busca en todos los directorios indistintamente. El más utilizado es **Google**.

The Google logo, consisting of the word "Google" in its characteristic multi-colored font (blue, red, yellow, blue, green, red).

Google

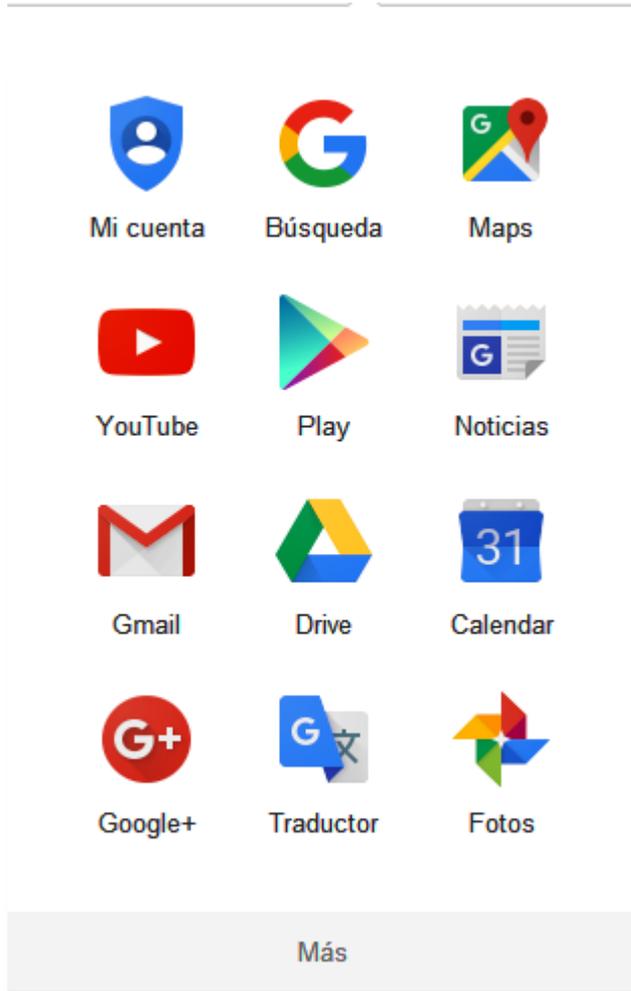
- Google es el buscador más utilizado en el mundo.
- Para realizar una búsqueda hay que teclear las palabras clave en el cuadro de texto y pulsar la tecla **Enter** o en **Buscar con Google**. Según se va escribiendo las palabras clave van apareciendo sugerencias de búsqueda.
- Si se pulsa el botón **Voy a tener suerte** no aparece un listado con los resultados de la búsqueda, sino directamente se carga en la ventana la primera página de la consulta efectuada..



Google

- Google también tiene múltiples funciones de **búsqueda avanzada** para **refinar** las consultas. La búsqueda avanzada permite realizar consultas más complejas para localizar la información que no seamos capaces de encontrar con la búsqueda básica y permite concretar las búsquedas sin necesidad de conocer todos los operadores que ofrece Google. De esta forma se pueden seleccionar los contenidos:
 - Filtrados por palabras
 - Que estén en páginas escritas en un idioma determinado.
 - Que se encuentren en una determinada región.
 - Que se hayan actualizado en las últimas 24 horas, en la última semana, mes o año.
 - Ubicados en uno solo o en varios dominios (por ejemplo, buscar en .org o .es).
 - Que se encuentren sólo en determinadas partes del documento (título, texto, URL, enlaces, etc.).
 - [Trucos para búsqueda avanzada en Google](#)

Google



- Además del buscador, **Google** tiene muchas herramientas como **GMail**, el servicio de correo electrónico, **Google Talk** para mensajería instantánea (chat), **Google Drive** para compartir en la red documentos de los usuarios, **Google Noticias**, el servicio automatizado de recopilación de noticias, **Google Maps**, el servicio que nos permite visualizar el mundo a través de imágenes vía satélite, imágenes de mapas o combinar estas dos o **Google Calendar** para organizar la agenda del usuario.

Técnicas de búsqueda

Hay que saber cómo funciona el buscador y seguir los siguientes consejos:

- **Escribir solamente las palabras clave de la búsqueda:** en general, los buscadores desprecian preposiciones, artículos y conjunciones (a, en, el, que, y, etc.).
- **Utilizar todas las palabras clave que se pueda:** cuanto mejor describamos lo que buscamos, más fácil será encontrarlo, es decir, la búsqueda será más afinada.
- **Pensar en formas de afinar la búsqueda:** añadiendo o cambiando palabras clave.
- **Vigilar la ortografía:** una palabra equivocada suele producir resultados equivocados, aunque muchos buscadores son capaces de detectar palabras mal escritas.
- **Buscar expresiones exactas:** si se conoce alguna frase o expresión que aparece en la página que estamos buscando, debe escribirse literalmente en el buscador.

Operadores de búsqueda

Existen una serie de **operadores**, que unidos a las palabras clave, aumentan la eficacia:

- **AND:** equivale a “Y”. Obliga a que todas las palabras que lo acompañan aparezcan en la búsqueda. Por ejemplo: libros AND informática. En la mayoría de los buscadores actuales no es necesario introducirlo.
- **OR:** equivale a “O”. Es el operador por defecto, ya que equivale al espacio entre las palabras y produce una búsqueda en la que pueden aparecer alguna de las palabras que lo acompañan o ambas. Por ejemplo: Yahoo OR Google.
- **Comillas:** realiza una búsqueda exacta de las palabras que están entre las comillas, con lo que se restringen más las búsquedas. Por ejemplo: “buscador más utilizado del 2012”.

Otros buscadores

- Además de Google, existen muchos otros buscadores, desde los genéricos Yahoo, Altavista o Bing de Microsoft hasta buscadores de temas más específicos como Gennio, basado en redes sociales o WotBox, basado en búsquedas geográficas.



Internet



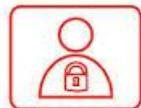
Certificados y firmas digitales

- Los certificados y firmas digitales surgen para poder realizar transacciones electrónicas seguras.
- Para que el receptor de una transacción pueda confiar en el emisor, una **Autoridad de Certificación** ha tenido que emitir un certificado digital al emisor de la transacción.
- Cuando una persona solicita un certificado digital, se genera un par de claves, una clave pública y una clave privada, que es lo que se utiliza para firmar electrónicamente.
- Con la firma digital se consigue:
 - Tener plena certeza de la identidad del autor del mensaje.
 - Verificar que el mensaje no se ha modificado desde su creación.



¿Qué es la firma digital?

- Una **firma digital** es una cadena de caracteres asociada a un mensaje digital que garantiza la **autenticidad** del origen y la **integridad** del mismo. Para generarla se utilizan métodos criptográficos que asocian la identidad de una persona o de un equipo informático, al mensaje o documento. En función del tipo de firma, se puede además asegurar la integridad del documento o mensaje. Se usan en entornos informáticos donde no hay objetos tangibles para identificar al usuario. Una firma digital debe ser auténtica, no falsificable, no alterable y no reusable.



firmas digitales

SABÍAS QUE: ?

La **firma digital** es el equivalente electrónico de la firma manuscrita. Es un número de más o menos 300 dígitos (1024 bits) dividido en:

- Una **clave pública** que conoce todo el mundo a través del certificado digital.
- Una **clave privada** que el usuario guarda en un dispositivo seguro y no se transmite nunca por la red.

Un **certificado digital** sirve para certificar que una clave pública pertenece a una persona u organización.

TEN EN CUENTA QUE:

El proceso de firma digital de un mensaje es:

1. El emisor envía un mensaje firmado electrónicamente mediante su clave privada.
2. El receptor descifra el mensaje con la clave pública del emisor teniendo la certeza de que el mensaje lo envió la persona propietaria de la clave pública y de que el mensaje no ha sufrido modificaciones durante el proceso de transmisión.

¿Qué es un certificado digital?

- Un certificado digital es un archivo electrónico de no más de 2KB de tamaño que contiene:
 - Los datos del propietario.
 - La clave pública del propietario.
 - El periodo de validez, que suele ser de 30 meses.
 - La firma digital de la Autoridad de Certificación.
- En España la **Fabrica Nacional de Monedas y Timbre** es la autoridad pública de certificación española que emite certificados digitales de forma gratuita.
- Actualmente el principal uso de la firma electrónica es realizar trámites con las diferentes administraciones públicas aunque también se puede utilizar para realizar transacciones con las siguientes empresas: eBay, Correos y Telégrafos, Renfe, Mercadona, Mapfre, etc.



Internet

SABÍAS QUE: ?

Se necesita un certificado digital para realizar a través de Internet los siguientes trámites con las administraciones públicas:

- Completar la declaración de la renta.
- Consultar los datos en la Seguridad Social de la vida laboral.
- Comprobar el saldo de puntos en el carnet de conducir.
- Inscribirse en concursos y oposiciones de la Administración General del Estado.

DNle

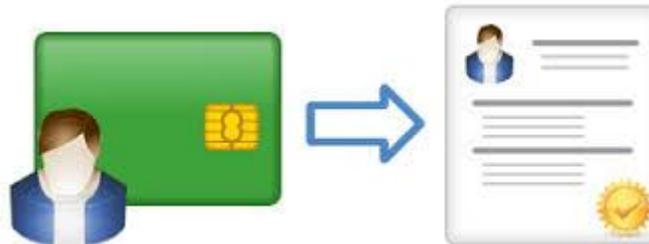


- El DNI tradicional incorpora actualmente en su formato un pequeño chip capaz de guardar de forma segura información del titular. De esta forma se amplía su uso para poder utilizarlo con las nuevas tecnologías de la información y de las comunicaciones.
- La Dirección General de la Policía es la entidad pública de certificación que emite los certificados de firma electrónica incluidos en los **DNle**.
- Para la utilización electrónica del **DNle**, se necesita un lector de tarjetas y descargar un software propio de acceso a tarjetas, disponible en la página web www.dnielectronico.es.

SABÍAS QUE: ?

El chip de DNle contiene la siguiente información:

- Datos de identificación personal.
- La fotografía digitalizada.
- La imagen digitalizada de la firma manuscrita.
- El patrón de la impresión dactilar.
- Certificado electrónico.
- Firma electrónica.



Páginas web seguras

- La información que se envía a un servidor web utilizando el protocolo http, viaja en texto, sin encriptar.
- Una conexión segura es un intercambio cifrado de información entre el sitio web y el usuario. El cifrado se ofrece a través de certificados SSL en el sitio web.
- El protocolo http transfiere hipertexto por Internet sin cifrar, mientras que el protocolo **https** es capaz de transferir hipertexto cifrado. Cuando nos conectamos a un servidor seguro el navegador avisa al usuario de que hemos cambiado de protocolo mostrando un candado.



Protección del sistema operativo

- Desde la aparición en 1988 del primer virus que colapsó toda la red de ARPANET, se ha puesto en relieve la importancia de la seguridad en las redes informáticas.
- Por ello es conveniente tener instaladas en el ordenador herramientas que nos protejan de ataques malintencionados procedentes de Internet. Estos ataques se producen por la introducción de **Malware** (*Malicious Software*, también conocido como **virus**) en nuestro ordenador.
- Existen muchos tipos, desde los gusanos y troyanos hasta los programas espías o spyware y los bots.

Amenazas y programas de detección

Amenaza	Descripción	Programas
Virus	<p>Programa informático diseñado específicamente para causar daños, alterando el funcionamiento normal de un ordenador. Su principal característica es que puede replicarse a sí mismo y propagarse a otros ordenadores.</p> <p>Los virus se adjuntan a programas y archivos, recibiendo a través de correos electrónicos, páginas web y dispositivos de almacenamiento secundario como pendrives.</p>	<p><i>Antivirus propietarios:</i></p> <ul style="list-style-type: none"> • Panda AntiVirus • Norton Antivirus • McAfee VirusScan <p><i>Antivirus gratis para uso personal:</i></p> <ul style="list-style-type: none"> • Avast Home • Avira Antivir Personal
Spam (correo basura)	<p>Correo electrónico enviado de forma masiva que contiene publicidad que no ha sido solicitada por el propietario de la cuenta de correo. También pueden incluir enlaces a un sitio web infectado o un archivo infectado.</p> <p>El spam es un correo anónimo, el remitente utiliza una dirección falsa o perteneciente a otra persona para ocultar su identidad.</p> <p>Por lo general, las direcciones de correo electrónico a las que van dirigidos los spam son robadas, compradas, recolectadas en la web o tomadas de cadenas de mail.</p>	<p><i>Antispam:</i></p> <ul style="list-style-type: none"> • MailWasher Free • CA Anti-Spam
Phishing	<p>Correo electrónico enviado de forma masiva que aparentando provenir de una fuente fiable, intenta conseguir que el usuario proporcione información confidencial.</p> <p>El término phishing proviene de la palabra inglesa "fishing" (pesca), aludiendo a que el usuario "pique el anzuelo".</p> <p>El caso más típico es el envío de emails que se hacen pasar por una entidad bancaria online, para conseguir que el usuario introduzca sus contraseñas en una página web falsa.</p>	<p>Los navegadores de Internet incluyen una barra Antiphishing que mostrará un aviso a los usuarios de los sitios web que han sido etiquetados como fraudulentos. También se pueden instalar barras de otros fabricantes.</p>
Spyware (programas espía)	<p>Son aplicaciones que se instalan ilícitamente en un ordenador y recopilan información (hábitos de navegación, programas instalados, etc) sobre una persona u organización sin su consentimiento. Son utilizados por empresas con fines comerciales.</p> <p>Se instalan a través de virus, de páginas web con controles ActiveX y de programas gratuitos (freeware o adware).</p>	<p><i>AntiSpyware:</i></p> <ul style="list-style-type: none"> • Ad-Aware de Lavasoft • Spyware Doctor de PC Tools • AVG Anti-Spyware de Grisoft

Recomendaciones para proteger el sistema operativo

1. Activar las actualizaciones automáticas.
2. Activar el firewall (cortafuegos) de Windows.
3. Instalar un antivirus o una suite de seguridad.
4. Utilizar contraseñas para acceder al ordenador.
5. Configurar el navegador de Internet.
6. Utilizar un correo electrónico con un buen filtro antispam.

En la red de una empresa el administrador del sistema se ocupará de la protección del sistema. El usuario generalmente no tiene privilegios para modificar los parámetros de seguridad.

El firewall que utilizan las empresas suelen ser un equipo, hardware, situado entre internet y la LAN. Suele utilizarse para limitar el acceso de internet a sus empleados así como para impedir el acceso de archivos con virus.

Fin del Tutorial

