

**IFCD0210 DESARROLLO DE APLICACIONES CON TECNOLOGÍA WEB**  
**Módulo formativo: MF0493\_3 IMPLANTACIÓN DE APLICACIONES WEB EN ENTORNOS DE INTERNET, INTRANET Y EXTRANET**

**Unidad 1. Internet.**

**FORMACIÓN PROFESIONAL PARA EL EMPLEO.**

**CIPP VIRGEN DE GRACIA**



CIPP VIRGEN DE GRACIA



Castilla-La Mancha



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE TRABAJO  
Y ECONOMÍA SOCIAL



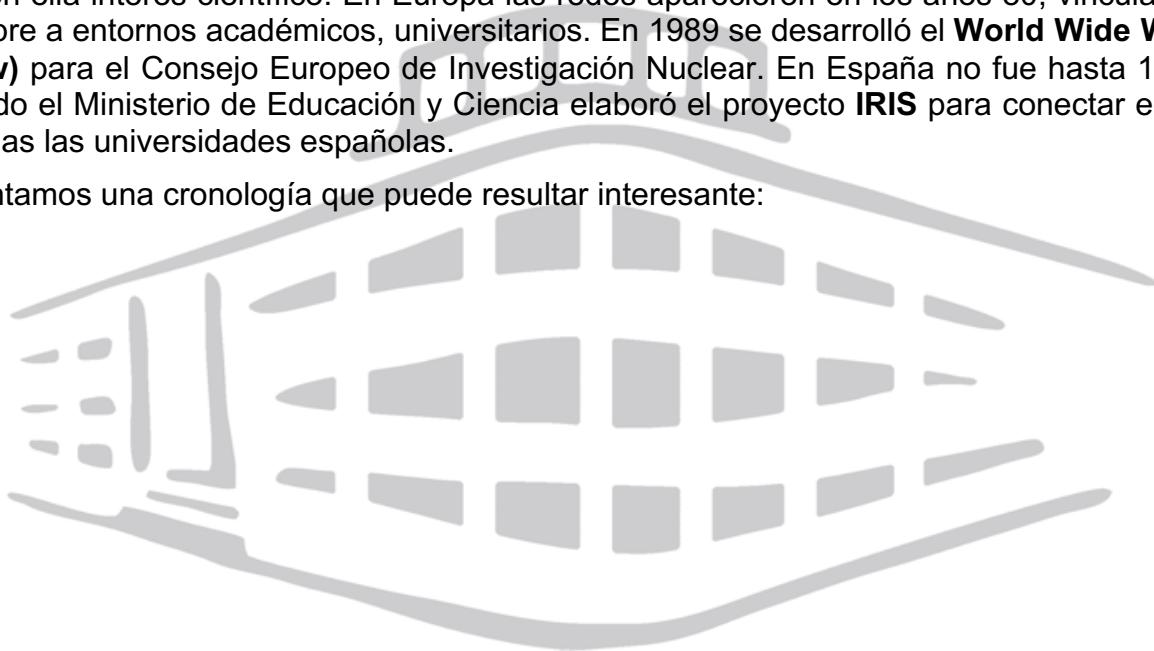
1. Breve historia y origen de Internet.....	2
2. Principales servicios ofrecidos por Internet.....	3
3. La tecnología de Internet.....	7
4. Redes TCP/IP.....	15
12. Bibliografía.....	28

## 1. Breve historia y origen de Internet

**Internet** se inició en torno al año 1969, cuando el Departamento de Defensa de los EEUU desarrolló **ARPANET**, una red de ordenadores creada durante la Guerra Fría cuyo objetivo era eliminar la dependencia de un Ordenador Central y así hacer mucho menos vulnerables las comunicaciones militares norteamericanas.

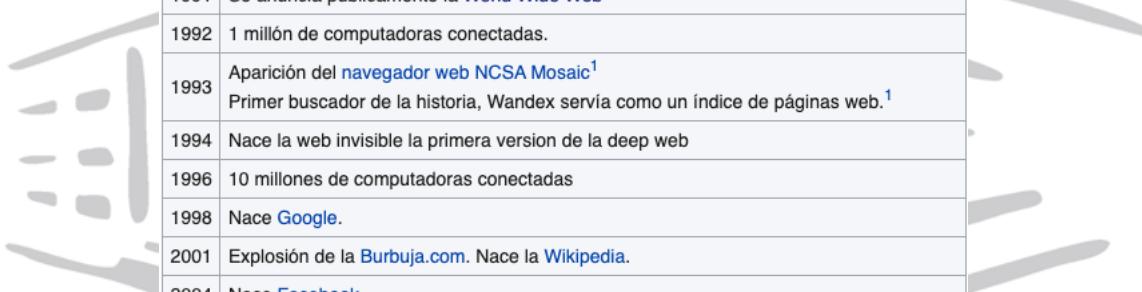
Cuando en los años 1980 la red dejó de tener interés militar, pasó a otras agencias que ven en ella interés científico. En Europa las redes aparecieron en los años 80, vinculadas siempre a entornos académicos, universitarios. En 1989 se desarrolló el **World Wide Web (www)** para el Consejo Europeo de Investigación Nuclear. En España no fue hasta 1985 cuando el Ministerio de Educación y Ciencia elaboró el proyecto **IRIS** para conectar entre sí todas las universidades españolas.

Adjuntamos una cronología que puede resultar interesante:



**CIFP VIRGEN DE GRACIA**

Año	Evento
1958	La compañía BELL crea el primer módem que permitía transmitir datos binarios sobre una línea telefónica simple.
1962	Inicio de investigaciones por parte de ARPA, una agencia del ministerio estadounidense de defensa, donde J. C. R. Licklider defiende exitosamente sus ideas relativas a una red global de computadoras.
1967	Primera conferencia sobre ARPANET
1969	Conexión de las primeras computadoras entre 4 universidades estadounidenses a través de la Interface Message Processor de Leonard Kleinrock
1971	23 computadoras son conectadas a ARPANET. Envío del primer correo electrónico por Ray Tomlinson.
1972	Nacimiento del InterNetworking Working Group, organización encargada de administrar Internet.
1973	Reino Unido y Noruega se adhieren a Internet, cada una con una computadora.
1979	Creación de los NewsGroups (foros de discusión) por estudiantes estadounidenses.
1981	Definición del protocolo TCP/IP y de la palabra «Internet»
1983	Primer servidor de nombres de sitios.
1984	1000 computadoras conectadas.
1987	10000 computadoras conectadas.
1989	100000 computadoras conectadas.
1990	Desaparición de ARPANET. Se crea el primer navegador web.
1991	Se anuncia públicamente la World Wide Web
1992	1 millón de computadoras conectadas.
1993	Aparición del navegador web NCSA Mosaic <sup>1</sup> Primer buscador de la historia, Wandex servía como un índice de páginas web. <sup>1</sup>
1994	Nace la web invisible la primera versión de la deep web
1996	10 millones de computadoras conectadas
1998	Nace Google.
2001	Explosión de la Burbuja.com. Nace la Wikipedia.
2004	Nace Facebook.
2005	Internet alcanza 1000 millones de usuarios.
2007	La aparición del iPhone populariza la web móvil.
2009	Comienzos de la mensajería instantánea en teléfonos móviles. Nace WhatsApp.



# CIFP VIRGEN DE GRACIA

## 2. Principales servicios ofrecidos por Internet

Internet está compuesta por una gran multitud de servicios que permiten a las personas estar comunicadas entre sí. No sólo es una increíble fuente de información al alcance de la mano y a la que se accede en cuestión de segundos, sino que también se compone de multitud de servicios indispensables para entender cómo funciona la sociedad a día de hoy.

### WORLD WIDE WEB

La red informática mundial, también conocida como World Wide Web, se utiliza para transmitir distintos tipos de datos a través de HTTP (protocolo de transferencia de hipertextos).

Esta red tuvo su nacimiento a finales de los 80 y fue desarrollada por el inglés Tim Berners-Lee y el belga Robert Cailliau en el CERN (The European Organization for Nuclear Research), en Ginebra (Suiza). En la actualidad se estima que existen más de 1200 millones de páginas web, aunque sólo 189 millones se encuentran activas, según un informe de la empresa [Netcraft](#).

## CORREO ELECTRÓNICO.

El correo electrónico se remonta a la década de los 70. El Instituto Tecnológico de Massachusetts (MIT, EEUU) compró un ordenador de tiempo compartido IBM 7090 que permitía a los usuarios **iniciar sesión desde terminales remotos**. Este sistema pronto se utilizó para enviar mensajes.

El primer correo contenía el texto 'QWERTYUIOP' y se envió a través de una red en 1971. Eso sí, los ordenadores estaban uno al lado del otro. Ray Tomlinson desarrolló la idea del **correo sobre redes** y fue quien usó la arroba por primera vez para establecer un destinatario.

Internet llegó y, a medida que iba creciendo, el correo electrónico se iba asentando como una forma habitual de comunicación. **Hotmail** nació en 1996 y tres años después 40 millones de personas tenían un correo electrónico en el mundo. El 1 de abril de 2004 Google presentó Gmail, su propio servicio. 14 años después contaba con 1500 millones de usuarios activos.

## BUSCADORES

El primer buscador que tuvo gran relevancia fue Yahoo. Fue creado por David Filo y Jerry Yang en 1994, dos estudiantes de ingeniería eléctrica en Standford (EEUU) que querían recopilar sus páginas web favoritas en un directorio principal. Como eran tantas, tuvieron que reorganizarlas y clasificarlas.

La gran novedad que implementó Yahoo en relación con otros navegadores primitivos era que colocaban una pequeña **descripción del contenido** de la página junto a su URL.

En la actualidad, la cosa ha cambiado. Google domina el mercado con su buscador y en 2000 se convirtió en el más usado en todo el mundo. Su éxito puede rastrearse, entre otras características, en la manera que tienen de posicionar las páginas web, **colocando las más relevantes para el usuario en primer lugar**.

## GRUPOS DE NOTICIAS Y NNTP

Hay servicios en Internet que han quedado obsoletos o que han sido sustituidos por otros más prácticos y optimizados. Es el caso del NNTP o Network New Transfer Protocol, protocolo creado para la publicación de noticias en la red Usenet, acrónimo de "Users Network" (red de usuarios). En ella, los internautas pueden leer o enviar mensajes a grupos de noticias que están ordenados de manera jerárquica.

La Usenet evolucionó hacia lo que se conocía como 'foros' de Internet, que, a su vez, han acabado siendo sustituidos por redes sociales. Aunque no del todo, ya que sitios como [Reddit](#) son pura Usenet. Un dato curioso es que esta red fue creada antes que la World Wide Web y fue concebida como un foro para resolver problemas del sistema Unix.

## LISTAS DE DISTRIBUCIÓN

Una lista de distribución permite enviar un mismo correo electrónico a una gran multitud de personas sin necesidad de escribir todas las direcciones de correo. En su lugar, aquella va dirigida a una sola dirección, la de la lista de distribución.

## FOROS

Hubo un tiempo en el que los foros constituían el principal punto de encuentro y discusión de millones de personas en Internet. Un foro solía ser un añadido de la página web para que los usuarios pudieran discutir los temas principales de los que aquella se ocupaba. Estos eran coordinados por un administrador y se clasificaban en categorías bien definidas. A pesar de que ya no se usan tanto, a día de hoy hay foros que sobreviven al paso del tiempo, como **Forocoches**...

## BLOGS

Un blog, en su acepción más canónica, es una página web donde el autor, ya sea una persona individual, grupo o empresa, escribe contenidos de su interés que suelen estar enfocados en una temática. El blog fue una evolución de los diarios en línea.

El blog tuvo sus propios subgéneros como el Fotolog, lugar en el que la impresa ocupaba un lugar primordial; el vlog, acrónimo de ‘videolog’ y precedente de uno de los contenidos más habituales de YouTube; y microblogging, sistema de publicación de caracteres limitados en el que se basa Twitter.

## TRANSFERENCIA DE ARCHIVOS FTP

En pocas palabras, un protocolo de transferencia de archivos (FTP) es un método para **enviar archivos de una ubicación en la red a otra**. Gracias a esta herramienta, podremos conectarnos con un servidor para subir o descargar archivos. También se usa para su intercambio entre servidores distintos.

En la actualidad, este sistema de transferencia ha sido sustituido en parte por el **almacenamiento en la nube**. La cloud ofrece numerosas ventajas como olvidarse de la limitación del espacio físico, mayor seguridad y fácil acceso desde cualquier dispositivo, incluyendo móviles y tablets.

## INTERCAMBIO DE ARCHIVOS P2P

La red de intercambio de archivos P2P o ‘peer to peer’ (entre pares) nació en 1999 con la creación de **Napster**, un programa que facilitaba la compartición de archivos MP3 entre usuarios sin que existieran intermediarios. Una red P2P no tiene ni clientes ni servidores fijos, sólo un conjunto de nodos que son, a la vez, clientes y servidores de los otros.

Napster y su sistema de intercambio de archivos entre usuarios fue el germen del nacimiento de la piratería digital. Programas como eMule y Soulseek utilizan la tecnología P2P para el intercambio de archivos de poco o gran tamaño, como películas completas.

## CHATS Y MENSAJERÍA INSTANTÁNEA

El IRC (Internet Relay Chat) apareció en 1988 como la primera forma de mensajería instantánea de la mano del finlandés Jarkko Oikarinen, conocido con el Nick de 'Wiz'. Para desarrollarlo se inspiró en el Bitnet Relay Chat, configuración de red de chat creada sobre notos [Bitnet](#).

El IRC adquirió una importancia vital en los albores de la comunicación de internet. Millones de personas lo utilizaban para establecer relaciones personales, además de para comunicar eventos y librarse de la censura. Por ejemplo, fue utilizado durante el intento de golpe de estado de la Unión Soviética de 1991 y por Kuwait durante la primera Guerra del Golfo.

Hoy en día sigue vivo con servidores que cuentan con entre 4000 y 9000 usuarios, aunque está lejos de sus días de gloria. Ahora han sido plenamente sustituidos por las redes sociales y los distintos servicios de mensajería instantánea que hay disponibles como Whatsapp o Telegram

## REDES SOCIALES

Una de las grandes protagonistas de Internet y punto de encuentro de internautas de diverso pelaje. Para encontrar la primera, **SixDegrees**, tenemos que remontarnos a 1997. Era una red en la que podíamos buscar a otros miembros. Su nombre se debía a la teoría de los 'seis grados de separación' que afirma que todas las personas en el mundo están conectadas en sólo seis pasos.

Sixdegrees cerró en 2001 y aparecieron otras nuevas como Friendster, para gamers, y MySpace, dedicada a músicos y fans. Tres años después apareció **Facebook** y cambiaría la historia de internet para siempre. Tras 17 años, sigue siendo la red social más usada. Y en TikTok vemos su evolución natural, donde el vídeo prima sobre la imagen. Por supuesto, no podemos olvidar Instagram, el Fotolog de la Generación Z, ni Twitter, que incorporó el sistema de microblogging.

## WIKIS

Muy pronto, Internet reunió a su alrededor a grupos de personas con intereses comunes. Estas creaban páginas y los usuarios podían editarlas desde el navegador. A esta comunidad virtual se la conoce como 'wiki', término que proviene del hawaiano y se traduce como 'rápido'.

Entre algunas de las wikis más famosas se encuentran 'Commons', dedicada a la difusión de **imágenes sin derechos** de propiedad o de licencia abierta; 'Wikiquote', colección de citas célebres y 'Wikipedia', enciclopedia abierta con una colección de más de 56 millones de artículos traducidos a 321 idiomas distintos.

## RSS

No confundir con RRSS (redes sociales). RSS corresponde a las siglas de **Really Simple Syndication**, formato XML para la difusión de contenido web sin necesidad de que esté en una página. Para verlo sólo se necesitan unos programas llamados 'agregadores' de noticias.

En un archivo RSS se encuentran los datos de las novedades del sitio en particular. Es el agregador el que se encarga de darle estilo y forma para que puedan leerse correctamente. En 2013, este tipo de archivo sufrió un enorme varapalo: Google cerró su propio agregador de noticias, Reader, ya que descubrió que los usuarios **preferían las redes sociales** para informarse. No obstante, en la actualidad existen agregadores como Freedly que son buenas alternativas.

## COMERCIO ELECTRÓNICO

El comercio electrónico es el proceso de compra y venta de artículos exclusivamente **a través de internet**. Y aunque parezca una transacción novedosa, la primera operación de este tipo data de 1984: Jane Snowball, inglesa de 72 años, realizó el primer pedido a través de un sistema inventado por Michael Aldrich.

Consistía en un **televisor conectado a un ordenador** que permitía transacciones en tiempo real a través de la línea telefónica. Snowball pudo seleccionar productos del supermercado Tesco mediante un menú en la televisión que ofrecía en pantalla un listado de los mismos.

Ahora, y sobre todo debido a la pandemia, el ecommerce va ocupando un lugar cada vez más relevante en el cómputo global de compras. Durante el segundo trimestre de 2020 el volumen de facturación del comercio electrónico alcanzó los 12020 millones de euros, según los datos de la Comisión Nacional de los Mercados y la Competencia.

## E-LEARNING

Si se puede comprar a través de Internet, también se pueden **impartir clases y recibirlas**. La enseñanza online está intrínsecamente relacionada con la propia naturaleza de la red: instruir y aprender. Fue en 1996 cuando nació el concepto de e-learning y un año después la California Virtual University creó una asociación de universidades con un catálogo de más de 1000 cursos online.

La educación digital no deja de crecer. Un estudio realizado por la Universidad Internacional de La Rioja afirma que la educación a distancia ha aumentado un **900% en el mundo desde el año 2000**.

### 3. La tecnología de Internet.

Internet es un conjunto descentralizado de redes de comunicaciones interconectadas que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyen una red lógica única de alcance mundial.

## ARQUITECTURA TCP/IP.

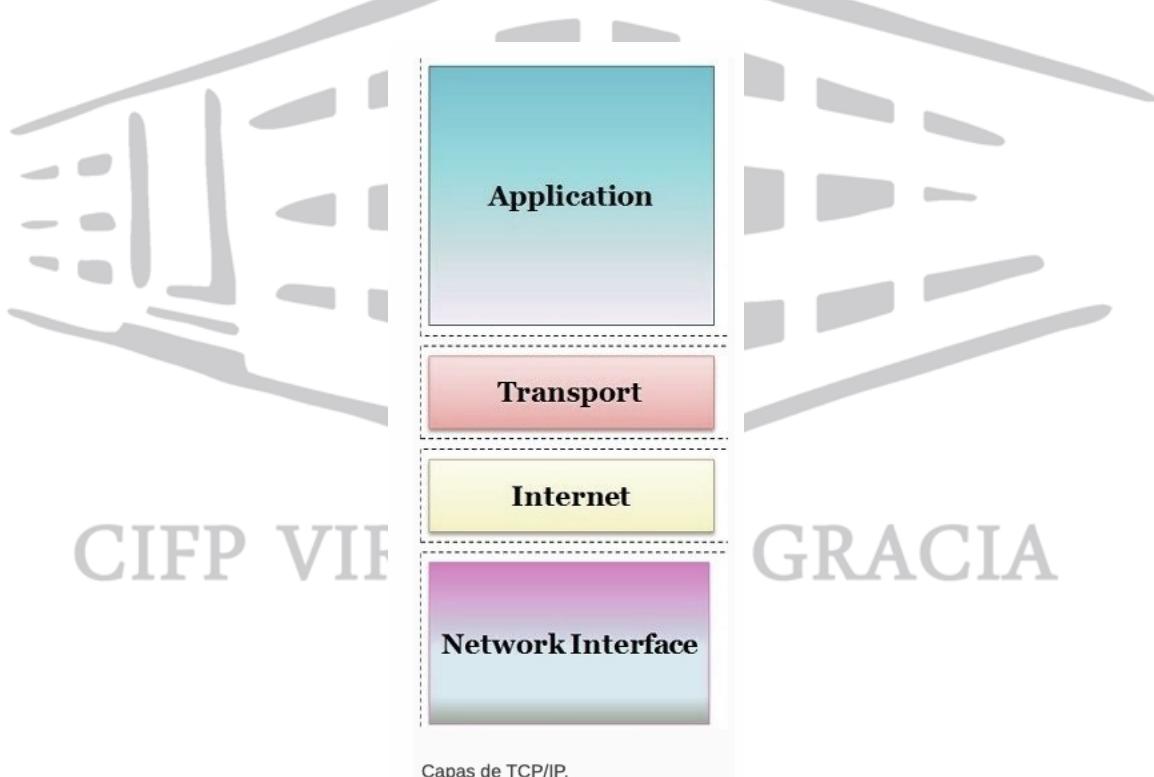
**TCP/IP** (Protocolo de Control de Transmisión / Protocolo de Internet) fue desarrollado por la agencia de proyectos del Departamento de Defensa (DoD). Consta de cuatro capas, cada una con sus protocolos.

Los protocolos de internet son el conjunto de reglas definidas para la comunicación a través de la red. TCP/IP se considera como el modelo de protocolo estándar para la creación de redes. TCP maneja la transmisión de datos e IP maneja las direcciones.

La suite TCP/IP es un conjunto de protocolos que incluye TCP, UDP, ARP, DNS, HTTP, ICMP... Sus características son robustez y flexibilidad. Se utiliza principalmente para interconectar ordenadores a través de Internet.

Las capas de TCP/IP son:

- **Capa de interfaz de red:** también llamada capa de enlace de datos o capa física, es la que maneja las partes físicas del envío y recepción de datos mediante el cable Ethernet, la red inalámbrica, la tarjeta de interfaz de red, el controlador del dispositivo en el equipo...
- **Capa de Internet:** también llamada capa de red, controla el movimiento de los paquetes alrededor de la red.
- **Capa de transporte:** es la que proporciona una conexión de datos fiable entre dos dispositivos. Divide los datos en paquetes, hace acuse de recibo de los paquetes que recibe del otro dispositivo y se asegura de que el otro dispositivo haga acuse de recibo de los paquetes que recibe a su vez.
- **Capa de aplicación:** es el grupo de aplicaciones que requiere comunicación de red. Es con lo que el usuario suele interactuar, como el correo electrónico y la mensajería. Como la capa inferior gestiona los detalles de la comunicación, las aplicaciones no tienen que preocuparse por ello.

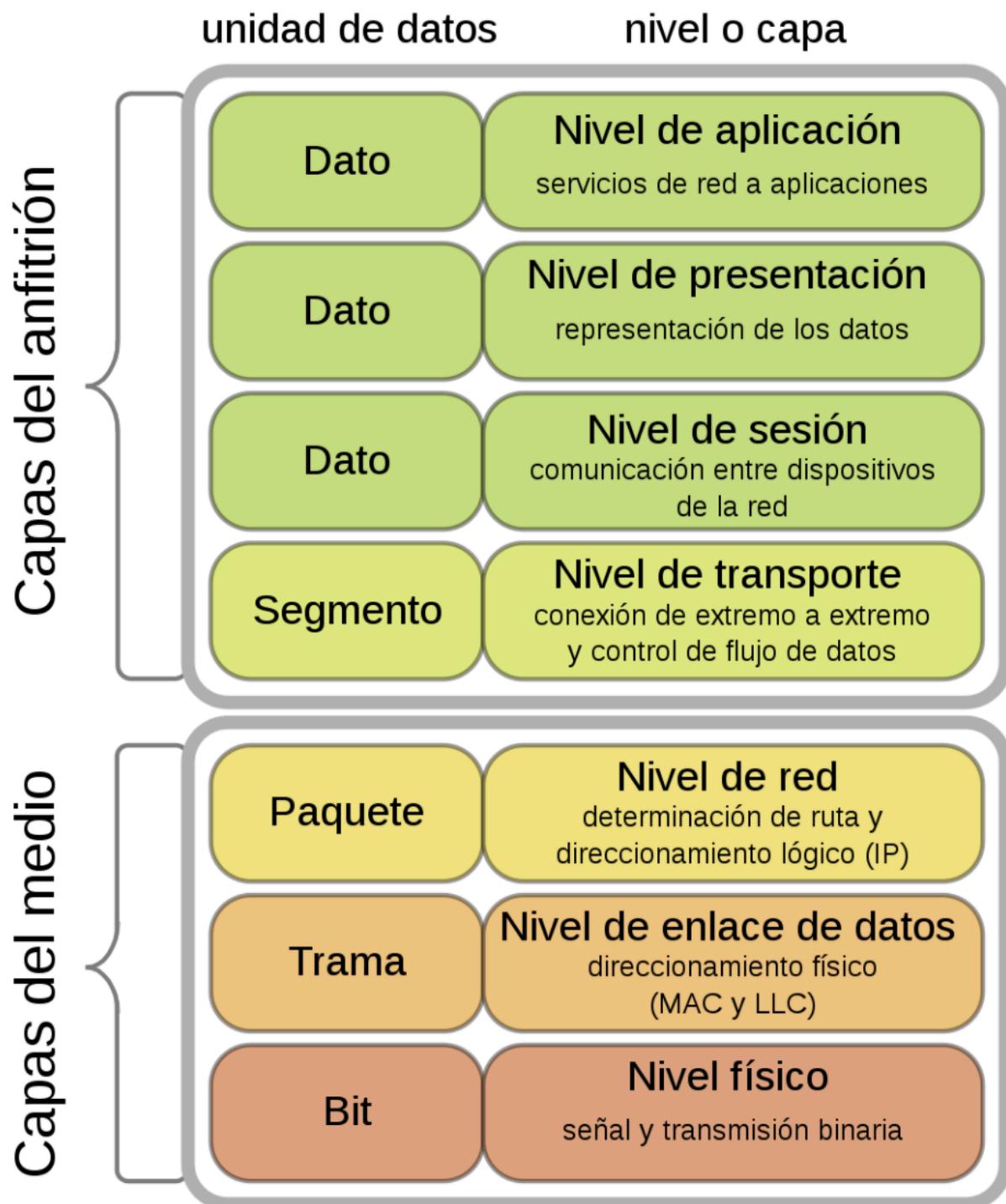


## MODELO OSI

El modelo de interconexión de sistemas abiertos, conocido como **OSI** (Open Systems Interconnection) es un modelo de referencia para los protocolos de la red (no es una arquitectura de red), creado en 1980 por la Organización Internacional de la Normalización (ISO).

El modelo OSI está formado por 7 capas o niveles de abstracción. Cada uno de estos niveles tendrá sus propias funciones para que en conjunto sean capaces de poder

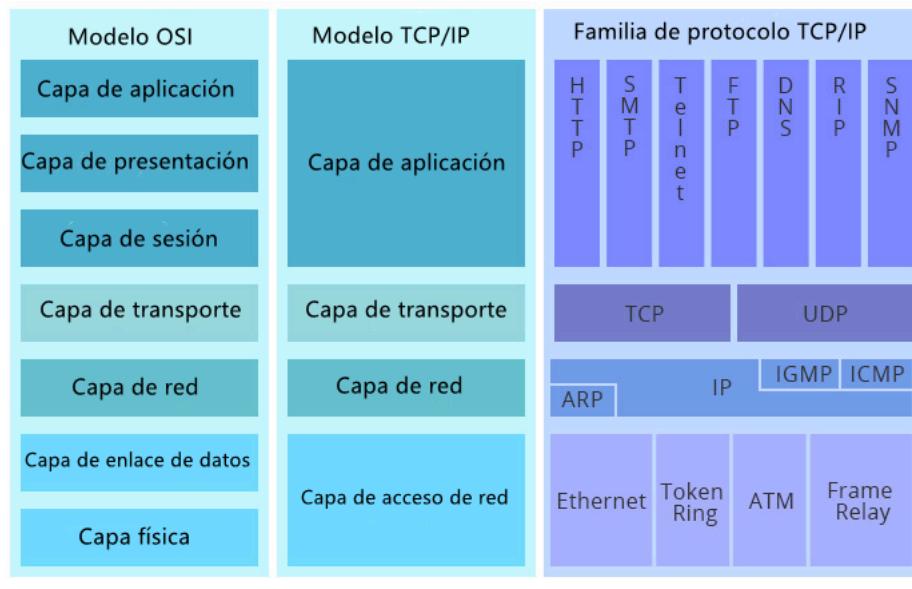
alcanzar su objetivo final. Precisamente esta separación de niveles hace posible la intercomunicación de protocolos distintos al concentrar funciones específicas en cada nivel de operación.



## DIFERENCIAS ENTRE EL MODELO OSI Y EL MODELO TCP/IP

Considerando los significados de los dos modelos de referencia, el modelo OSI es sólo un modelo conceptual. Se utiliza principalmente para describir, discutir y comprender funciones de red individuales. Sin embargo, TCP/IP está diseñado para resolver un conjunto específico de problemas, no para funcionar como una descripción general para todas las comunicaciones de red como modelo OSI. El modelo OSI es genérico, independiente del protocolo, pero la mayoría de los protocolos y sistemas se adhieren a

él, mientras que el modelo TCP/IP se basa en protocolos estándar que Internet ha desarrollado.



## PROTOCOLOS DE INTERNET: TCP, UDP, SMNP, SMTP, etc.

Los protocolos de red son un conjunto de reglas que gobiernan la comunicación entre dispositivos que están conectados a una red. Dichas reglas se constituyen de instrucciones que permiten a los dispositivos identificarse y conectarse entre sí, además de aplicar reglas de formateo, para que los mensajes viajen de la forma adecuada de principio a fin. Dichas reglas de formateo determinan si los datos son recibidos correctamente o si son rechazados o ha habido algún tipo de problema en la transferencia de la información.

Cuando se lleva a cabo la comunicación entre ordenadores conectados a una misma red, los datos se parten en paquetes de datos más pequeños, normalmente tienen una longitud de 1500 bytes, ya que es el típico MTU (Maximum Transfer Unit) que se suele utilizar en las redes. No obstante, las redes locales profesionales utilizan un MTU de 9000 bytes o superior, son los conocidos como Jumbo Frames, esto permite optimizar el máximo de transferencia de datos ya que se van a transferir menos cabeceras que también tienen un cierto tamaño. Por supuesto, una vez que hemos partido los datos en paquetes más pequeños, al llegar al destinatario, es necesario reensamblarlos para posteriormente pasarlo a la capa de aplicación.

### Protocolos de la capa de acceso al medio

#### ARP (Address Resolution Protocol)

El protocolo ARP para redes IPv4 es uno de los protocolos fundamentales de Internet y de las redes locales. Este protocolo también trabaja junto con el protocolo IP para mapear direcciones IP en relación a las direcciones de hardware utilizados por un protocolo de enlace de datos. A estas direcciones de hardware se las denominan **direcciones MAC**. Estas direcciones sirven de código de identificación para cada una de las interfaces de red de los dispositivos. ARP opera en el medio de la capa de red y la capa de acceso al medio.

(Si consideramos modelo TCP/IP o modelo OSI). Este protocolo se aplica cuando se utiliza el protocolo IP sobre Ethernet.

## Protocolos de la capa de red

### IP (Internet Protocol)

Los protocolos de Internet son un conjunto de reglas que determinan la manera en la que se transmiten los datos a través de la red. El protocolo de IP es un estándar con especificaciones respecto a cómo deben funcionar los dispositivos conectados que se encuentran en Internet. Por un par de razones: el **direcccionamiento** y el **routing**.

El **direcccionamiento** consiste en asegurar que cualquier dispositivo conectado a una determinada red cuente con una **dirección IP** única. Así se podrá conocer el origen y el destino de los datos en tránsito.

Por otro lado, el **routing** determina el camino por el cual el tráfico debe transitar teniendo como base la dirección IP. La tarea de routing es realizada mediante los routers, no solamente el que tenemos en nuestro hogar, sino los routers de los operadores. A su vez, varios protocolos interactúan con IP para posibilitar la comunicación en cualquier red.

### Internet Control Message Protocol (ICMP)

Este protocolo apoya al proceso de control de errores. Esto es así ya que el protocolo IP, por defecto, no cuenta con un mecanismo para la gestión de errores en general. ICMP es utilizado para el reporte de errores y consultas de gestión. Es un protocolo utilizado por dispositivos como routers para enviar mensajes de errores e información relacionada a las operaciones. Por ejemplo, puede informar que el servicio solicitado no se encuentra disponible o que un host o router no pudo ser alcanzado/localizado. Este protocolo se encuentra justo por encima del protocolo IP en la capa de protocolos TCP/IP.

## Protocolos de la capa de transporte

### TCP (Transmission Control Protocol)

TCP es el aliado de IP para garantizar que los datos se transmiten de manera adecuada a través de Internet.

Su función principal es asegurar que el tráfico llegue a destino de una manera confiable. Esta característica de confiabilidad no es posible lograrla únicamente mediante IP. Otras funciones de TCP son:

- Que no se pierdan los paquetes de datos.
- Control del orden de los paquetes de datos.
- Control de una posible saturación que se lleve a experimentar.
- Prevención de duplicado de paquetes

### UDP (User Datagram Protocol)

A diferencia de TCP, UDP no es tan confiable. Este no cuenta con posibilidad de realizar revisiones en búsqueda de errores o correcciones de transmisiones de datos. Sin embargo, hay ciertas aplicaciones en donde UDP es más fácil de utilizar que TCP. Un ejemplo de esto es una sesión de juegos en línea, donde UDP permite que los paquetes de datos se descarten sin posibilidad de reintentos.

Lo malo es que este protocolo no es recomendado para realizar transferencia de datos. Ya que si algunos paquetes se pierden durante el proceso de transferencia, el resultado final es que el archivo se corrompe, y las capas superiores (capa de aplicación) es quien debe realizar la solicitud para que se vuelva a enviar el datagrama de nuevo. Un archivo corrupto no puede ser utilizado para el fin por el cual fue enviado. Igualmente, para este escenario de juegos en línea o sesiones de streaming de vídeos, UDP es el protocolo recomendado porque es más rápido al no tener que realizar el típico handshake.

## Protocolos de la capa de aplicación

### HTTP (Hypertext Transfer Protocol)

Es el protocolo que permite que los navegadores y servidores web se comuniquen adecuadamente. Este es utilizado por navegadores web para solicitar archivos HTML de parte de los servidores remotos. Así, los usuarios podrán interactuar con dichos archivos mediante la visualización de las páginas web que cuentan con imágenes, música, vídeos, texto, etc.

El protocolo HTTP tiene como base a TCP, el cual implementa un modelo de comunicación cliente-servidor. Existen tres tipos de mensajes que HTTP utiliza:

- **HTTP GET:** Se envía un mensaje al servidor que contiene una URL con o sin parámetros. El servidor responde retornando una página web al navegador, el cual es visible por el usuario solicitante.
- **HTTP POST:** Se envía un mensaje al servidor que contiene datos en la sección «body» de la solicitud. Esto es hecho para evitar el envío de datos a través de la propia URL. Así como sucede con el HTTP GET.
- **HTTP HEAD:** Aquí se hace énfasis en la respuesta por parte del servidor. Este mensaje restringe lo que el servidor responde para que solamente responda con la información de la cabecera.

No debemos olvidar el protocolo HTTPS, el cual nos proporciona seguridad punto a punto (entre el cliente y el servidor web). El protocolo HTTPS utiliza el protocolo TLS (Transport Layer Security) que también utiliza TCP por encima.

### DNS (Domain Name System)

Es el servicio encargado de **traducir/interpretar nombres de dominio** a direcciones IP. Recordemos que los nombres de dominio se constituyen en base a caracteres alfabéticos (letras), los cuales son más fáciles de recordar. Para el usuario, es más fácil recordar un nombre que una serie numérica de cierta longitud. Sin embargo, Internet en general funciona en gran parte mediante las direcciones de IP. Siempre y cuando introduzcas un nombre de dominio en tu navegador, un servicio DNS recibe esa información para interpretarla y permitir la visualización de la página web deseada.

Tengamos presente que cuando contratamos un servicio de Internet, este nos provee la conectividad mediante sus propios servidores DNS. Sin embargo, es posible optar por DNS alternativos tanto para conectarnos desde el ordenador como nuestro móvil.

### FTP (File Transfer Protocol)

El **protocolo FTP** es utilizado para compartir archivos entre dos ordenadores. Así como el protocolo HTTP, FTP implementa el modelo cliente-servidor. Para que se pueda ejecutar FTP, se debe lanzar el cliente FTP y conectar a un servidor remoto que cuente con un software del mismo protocolo. Una vez que la conexión se ha establecido, se deben descargar los archivos elegidos de parte del servidor FTP.

Por otro lado, el **protocolo TFTP** fue diseñado para dispositivos con menor capacidad. Sus siglas corresponden a **Trivial File Transfer Protocol**. Este provee un uso básico que contiene solamente las operaciones elementales de FTP. Este protocolo se suele utilizar para cargar los firmwares en routers y switches gestionables, ya que es un protocolo muy simple de comunicación.

### POP3 (Post-Office Protocol Version 3)

Es un protocolo estándar de Internet es utilizado por los distintos clientes de correo electrónico. se utiliza para poder recibir correos de parte de un servidor remoto a través de una conexión TCP/IP. Haciendo un poco de historia, POP3 ha sido concebido por primera vez en el año 1984 y se ha vuelto uno de los más populares. Es utilizado por prácticamente el total de los clientes de correo electrónico conocidos, es simple de configurar, operar y mantener.

En la mayoría de los casos, los servidores de correo electrónico son ofrecidos y alojados por parte de los ISP. Si fuese así, dicho proveedor debe de facilitarte los datos para poder configurar correctamente tu cliente de correo electrónico. A parte de visualizar los mensajes, es posible descargar una copia de los mismos y mantenerlos en nuestro ordenador. Una vez que se descargan los mensajes, estos ya desaparecen de parte del servidor remoto. Sin embargo, existen casos en los que los usuarios configuran que los correos se mantengan en el servidor por un período determinado de tiempo.

El número de puerto TCP utilizado normalmente por parte de POP3 es el **110**. Si es que la comunicación cifrada está disponible, los usuarios pueden escoger conectarse mediante el comando **STLS (TLS seguro)** o bien, utilizando **POP3S (POP3 seguro)**. Este último puede valerse de **TLS** o **SSL** en el puerto **TCP 995** para conectarse al servidor de correo.

### IMAP (Internet Message Access Protocol)

Es un estándar para el acceso a correos electrónicos alojados en un servidor web, mediante un cliente de correo electrónico local. Para establecer las conexiones de comunicación, utiliza el protocolo de la capa de transporte TCP. Lo cual permite el uso de un servidor remoto de correo electrónico. Ahora bien, el puerto utilizado para IMAP es el **143**. Tiene utilidades y características similares a POP3.

Una consideración importante es que IMAP es protocolo para servidores remotos de archivos, a diferencia de aquellos que se valen del protocolo POP3, el cual permite el

almacenamiento de dichos mensajes. En otras palabras, gracias a IMAP los mensajes de correo electrónico **se mantienen en el servidor hasta que el usuario decide borrarlos**. Por otro lado, este protocolo permite la administración de una sola cuenta de correo electrónico de parte de más de un cliente.

Cuando un usuario solicita el acceso a un mensaje de correo electrónico, dicha solicitud se encamina a través de un servidor central. Algunos de los beneficios del protocolo IMAP consisten en la posibilidad de borrar los mensajes del servidor y la búsqueda mediante palabras clave entre los mensajes que se encuentran en nuestro buzón. Por tanto, se puede crear y administrar múltiples buzones y/o carpetas, y la visualización de vistas previas de los mensajes.

### **SMTP (Simple Mail Transfer Protocol)**

Este protocolo, así como los que hemos citado anteriormente, es considerado como uno de los servicios más valiosos de Internet. La mayoría de los sistemas que funcionan a través de Internet se valen de SMTP como un método para enviar/transferir correos electrónicos.

El cliente que quiere enviar un correo electrónico, establece una conexión TCP al servidor SMTP. Después, envía el mensaje a través de dicha conexión. El servidor siempre está en modo *listening*. Tan pronto se hace eco de una conexión TCP, el proceso SMTP inicia una conexión mediante su puerto asignado que es el número 25. Una vez que se haya establecido exitosamente una conexión TCP, el cliente procede al envío automático del correo electrónico.

Podemos toparnos con dos esquemas de funcionamiento SMTP:

- Método Extremo a Extremo (End-to-End)
- Método Almacenamiento y Envío (Store-and-forward)

Primeramente, el **método Extremo a Extremo** es utilizado para la comunicación entre distintas organizaciones. Por otro lado, el **método Almacenamiento y Envío** es utilizado para las comunicaciones entre los hosts que se encuentran en una misma organización. Un cliente SMTP que quiere enviar un mensaje de correo electrónico va a establecer un contacto con su destino para poder enviar el mensaje. El servidor SMTP se va a quedar con la copia del mensaje de correo hasta que el mismo haya llegado a destino.

### **SMNP (Simple Network Management Protocol)**

En español, significa **Protocolo de Gestión de Redes Simple**. Es uno de los protocolos que más tiempo lleva vigente, específicamente desde el año 1988. En un principio, los switches y routers podían ser gestionados por este protocolo, hoy en día, es posible contar con el protocolo SNMP para prácticamente cualquier dispositivo que consiga conectarse a una red. Así también, es posible realizar tanto monitorización y ajustes en la configuración de los dispositivos monitorizados de forma remota.

Este es un protocolo orientado a datagramas. Cualquiera de los dispositivos gestionados tendrá un agente que se comunica con el dispositivo central, el cual los gestiona. Dicho agente enviará información al mencionado dispositivo central, cuyo contenido será

almacenado en una base de datos que se denomina **MIB (Management Information Base)**. ¿Qué es esto? Es una manera jerárquica de organizar la información recolectada de cualquier dispositivo SNMP que se encuentra conectado a la red.

## 4. Redes TCP/IP.

### DIRECCIONAMIENTO IP. EVOLUCIÓN.

La **dirección IP** es una etiqueta numérica, *por ejemplo "192.0.10.1"* que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el Protocolo de Internet (Internet Protocol) o que corresponde al nivel de red del modelo TCP/IP.

Una dirección IP tiene dos funciones principales: identificación de la interfaz de red y direccionamiento para su ubicación.

La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.

La dirección IP puede cambiar a menudo debido a cambios en la red, o porque el dispositivo encargado dentro de la red de asignar las direcciones IP, decida asignar otra IP (*por ejemplo, con el protocolo DHCP*). A esta forma de asignación de dirección IP se le denomina también *dirección IP dinámica* (normalmente abreviado como *IP dinámica*). Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados, generalmente tienen la necesidad de una *dirección IP fija* (comúnmente, *IP fija* o *IP estática*). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, para las personas es más fácil recordar un nombre de dominio que los números de la dirección IP. Los servidores de nombres de dominio DNS, "traducen" el nombre de dominio en una dirección IP. Si la dirección IP dinámica cambia, es suficiente actualizar la información en el servidor DNS. El resto de las personas seguirán accediendo al dispositivo por el nombre de dominio.

### Direcciones IPv4

Las direcciones IPV4 se expresan mediante un número binario de 32 bits permitiendo un espacio de direcciones de hasta 4.294.967.296 ( $2^{32}$ ) direcciones posibles.

Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ". ". Cada uno de estos octetos puede estar comprendido entre 0 y 255.

- Ejemplo de representación de dirección IPv4: 10.128.1.253, 192.168.255.254/18

En las primeras etapas del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red. Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases. (classful network architecture). En esta arquitectura hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers ([ICANN](#)): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los *hosts*, de modo que la cantidad máxima de *hosts* es  $2^{24} - 2$  (se excluyen la dirección reservada para *broadcast* (últimos octetos a 1) y de red (últimos octetos a 0)), es decir, 16 777 214 *hosts*.
- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los *hosts*, de modo que la cantidad máxima de *hosts* por cada red es  $2^{16} - 2$ , o 65 534 *hosts*.
- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los *hosts*, de modo que la cantidad máxima de *hosts* por cada red es  $2^8 - 2$ , o 254 *hosts*.

Clase	Bits iniciales	Intervalo (*)	N.º de redes	N.º de direcciones por red	N.º de hosts por red(†)	Máscara de red	Dirección de broadcast
A	0	0.0.0.0 (**)- 127.255.255.255 (†)	128	16 777 216	16 777 214	255.0.0.0	x.255.255.255
B	10	128.0.0.0 - 191.255.255.255	16 382	65 536	65 534	255.255.0.0	x.x.255.255
C	110	192.0.0.0 - 223.255.255.255	2 097 150	256	254	255.255.255.0	x.x.x.255
D (Multicast)	1110	224.0.0.0 - 239.255.255.255					
E (experimental)	1111	240.0.0.0 - 255.255.255.254					

- (\*) La dirección que tiene los bits de host iguales a 0 sirve para definir la red en la que se ubica. Se denomina **dirección de red**. La dirección que tiene los bits correspondientes a *host* iguales a 1, sirve para enviar paquetes a todos los *hosts* de la red en la que se ubica. Se denomina **dirección de broadcast**.
- (\*\*) La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- (†) Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina **dirección de bucle local o loopback**.
- (‡) La primera dirección se reserva para identificar la red (p.ej. 18.0.0.0), mientras que la última dirección se emplea como dirección de difusión o *broadcast* (p.ej. 18.255.255.255). Ese es el motivo por el que el número máximo de *hosts* en una red es siempre igual al número de direcciones disponibles en un rango específico menos dos.

El diseño de redes de clases (*classful*) sirvió durante la expansión de internet, sin embargo este diseño no era escalable y frente a una gran expansión de las redes en la década de los noventa, el sistema de espacio de direcciones de clases fue reemplazado por una arquitectura de redes sin clases Classless Inter-Domain Routing (CIDR) en el año 1993. CIDR está basada en redes de longitud de máscara de subred variable (variable-length subnet masking VLSM), lo que permite asignar redes de longitud de prefijo arbitrario. Permitiendo por tanto una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y "desperdiendo" las mínimas posibles.

## Direcciones IPv6

La función de la dirección IPv6 es exactamente la misma que la de su predecesor IPv4, pero dentro del protocolo [IPv6](#). Está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos. IPv6 permite actualmente que cada persona en la Tierra tenga asignados varios millones de IP, ya que puede implementarse con  $2^{128}$  ( $3.4 \times 10^{38}$  hosts direccionables). La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

Su representación suele ser [hexadecimal](#) y para la separación de cada par de octetos se emplea el símbolo ":". Un bloque abarca desde 0000 hasta FFFF. Algunas reglas de notación acerca de la representación de direcciones IPv6 son:

- Los ceros iniciales se pueden obviar.

Ejemplo: 2001:0123:0004:00ab:0cde:3403:0001:0063 -> **2001:123:4:ab:cde:3403:1:63**

- Los bloques contiguos de ceros se pueden comprimir empleando "::". Esta operación solo se puede hacer **una** vez.

Ejemplo: 2001:0:0:0:0:0:4 -> **2001::4**.

Ejemplo no válido: 2001:0:2001::2:0:0:1 o 2001:0:0:0:2::1.

## IDENTIFICACIÓN DE SERVIDORES - DNS.

Como hemos visto, los sistemas informáticos se comunican entre sí mediante una dirección IP. Sin embargo, nosotros preferimos **utilizar nombres significativos para identificar un equipo**. Son más fáciles de recordar y ofrecen mayor flexibilidad. Podemos cambiar la dirección IP de un equipo sin que cambie su nombre.

Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del **fichero /etc/hosts de Linux** o **\Windows\system32\driver\etc\hosts de Windows** en los que se guarda cada nombre junto a su respectiva dirección IP. Todavía siguen existiendo y los podemos usar para realizar pruebas.

Sin embargo, según iba aumentaba el número de equipos conectados, mantener estos ficheros actualizados se volvió cada vez más complicado. Para paliar estos problemas se ideó el sistema de resolución de nombres, **DNS (Domain Name System)** en el que una serie de **servidores organizados de manera jerárquica** se encargan de resolver los nombres de cualquier equipo conectado a Internet. Tanto los sistemas operativos como los servidores DNS que intervienen en la resolución de nombres mantendrán una cache con las últimas consultas realizadas de manera que se pueda agilizar todo el proceso.

El procedimiento es parecido al que se sigue a continuación para encontrar la IP de la web <http://www.debian.org/distrib/netinst>:

- Se consulta la memoria caché del sistema operativo. Si ya se ha realizado esta consulta anteriormente y está almacenada en la memoria cache, el proceso finaliza.
- Se consulta la memoria caché del servidor DNS configurado en la configuración de red del sistema operativo. Si ya existe una entrada para la dirección, el proceso termina.

- El DNS averigua la IP del servidor DNS que resuelve el dominio raíz 'org' y le pregunta por la IP del servidor DNS que gobierna el subdominio 'debian' bajo 'org'.
- Por último, una vez obtenida la IP del servidor DNS que gobierna el dominio 'debian.org', se le pregunta por la IP del equipo 'www.debian.org', y el proceso ha terminado.

Como se observa, los DNS se encargan únicamente del nombre del dominio, www.debian.org. La ruta /distrib/netinst depende del servidor direccionado y tendrá que crearse y configurarse correctamente en el servidor destino.

## Funcionamiento del DNS

La siguiente imagen presenta gráficamente el funcionamiento del DNS, tomando como ejemplo la página web www.debian.org y considerando que la información de la petición del dominio a buscar no se encuentra en tu ordenador o en un servidor DNS local existente en tu red o en tu ordenador.

1. A través de tu navegador quieres consultar la página web oficial de Debian escribiendo en la barra de direcciones la URL <http://www.debian.org>.
2. El navegador busca la información de las DNS del dominio **debian.org**.
3. Internet está ordenada en forma de árbol invertido, si no encuentra la información en tu ordenador, irá a buscarla a los servidores DNS que posees en la configuración de red de tu ordenador, típicamente los proporcionados por tu Proveedor de Servicios a Internet (ISP): DNS Primario (3a) o DNS Secundario (3b). De no estar, seguirá buscándola a niveles superiores y, en último lugar, lo encontrará en el Servidor de Nombres Raíz: DNS Raíz (3n).
4. La información buscada: las IP correspondientes al servidor DNS que gobierna el dominio **debian.org**, llega a tu ordenador: DNS1→ 206.12.19.7 y DNS2→ 128.31.0.51. Suelen ser dos porque las especificaciones de diseño de DNS recomiendan que, como mínimo, deben existir dos servidores DNS para alojar cada zona, a la que pertenece cada dominio.

Tu ordenador ahora intentará conectar con el servidor DNS1 (5a) o ante cualquier problema de conexión con éste lo intentará con el servidor DNS2 (5b). Éstos son los servidores de nombres donde se encuentra información acerca de dónde se puede buscar la página web (servidor de la web), una dirección de correo electrónico (servidor de correo), etc.

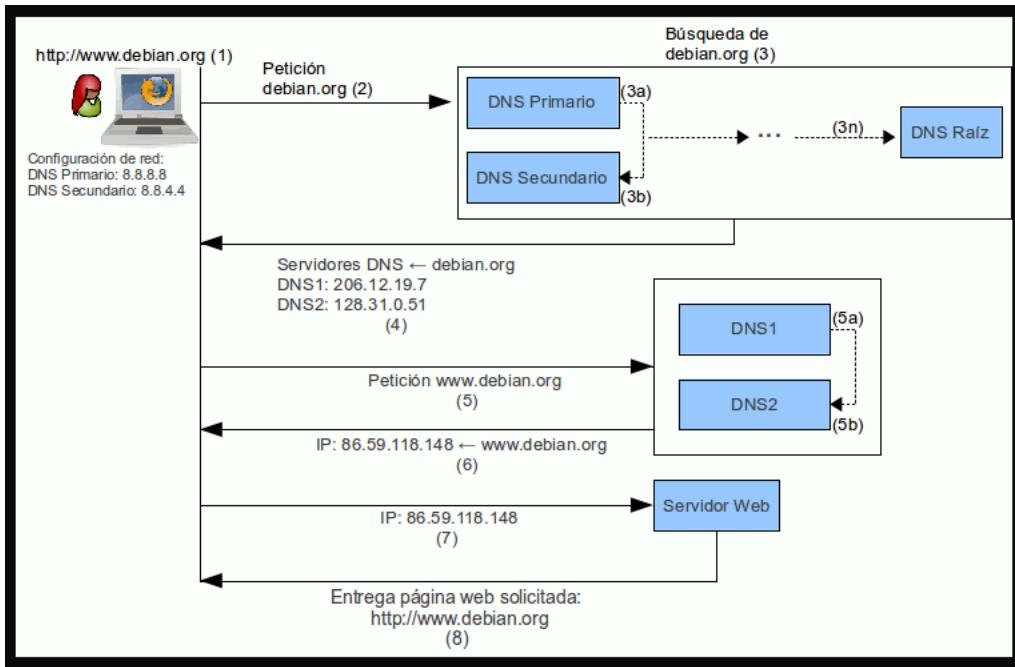
5. Tu ordenador recibirá la información acerca de la localización de la página web, o sea, la dirección IP del servidor web donde está alojada la página.
6. Tu ordenador se dirigirá luego al servidor web y buscará la página web en él.
7. Por último, el servidor web devuelve la información pedida y tú recibes la página web, visualizándola en el navegador.

Pero, y si vuelves a consultar la página web oficial de Debian escribiendo en la barra de direcciones la URL <http://www.debian.org>, ¿se repetirá de nuevo todo el proceso? Para contestar esta pregunta hay que establecer dos situaciones:

1. El host desde el que vuelves a realizar la consulta es el mismo: Si no lo es, antes de repetir todo el proceso se intentaría con lo expuesto en el siguiente punto, pero si es el mismo, al haber hecho la consulta desde este host, la resolución dominio-IP se guarda durante algún tiempo en la memoria caché del mismo, por lo cual no será necesario

repetir todo el proceso de nuevo. Si el tiempo en el que la memoria caché guarda la resolución ha expirado se volverá a repetir el proceso de nuevo.

2. Existe un servidor DNS caché en tu red o en tu host: por lo tanto, si un segundo cliente, que tiene configurado este servidor DNS, vuelve a realizar la misma petición, como este servidor tiene la respuesta almacenada en su memoria caché, responderá inmediatamente sin tener que cursar la petición a ningún servidor DNS de Internet. Si el tiempo en el que la memoria caché guarda la resolución ha expirado se volverá a repetir el proceso de nuevo.



## Nombres de dominio.

¿Qué es lo que sueles escribir en la barra de direcciones URL del navegador? Normalmente algo similar a: **www.debian.org**. Entonces, vienen siendo unos caracteres separados por puntos. ¿Qué es lo que significan esos puntos? ¿Qué dividen? Además, en el ejemplo expuesto, al escribir **www.debian.org** el navegador autocompleta esta petición a **http://www.debian.org**, ¿por qué?

Todas estas preguntas tienen respuesta, así que vamos a por ellas:

- Primero: Los puntos separan dominios y subdominios, empezando de derecha a izquierda tendrás dominios de primer nivel y dominios de segundo, tercero, ..., n-ésimo nivel, denominados subdominios. Así:
  - **org** es el dominio de primer nivel que identifica a organizaciones.
  - **debian** es un subdominio, en este caso dominio de segundo nivel bajo org, que identifica al nombre de la organización o al nombre de la empresa, sucursal, etc.
  - **www** es un subdominio, en este caso dominio de tercer nivel bajo debian, que identifica al equipo donde está colgada la página web, esto es, identifica el servidor web que aloja la página web. Es el dominio www que el servidor DNS redirecciona a la IP del servidor web.
- Segundo: **http://** es el protocolo de hipertexto que permite la correcta visualización de la página web en el navegador. Es lo que el navegador autocompleta en caso de no estipular uno propio en la barra de direcciones URL con en nombre de dominio.

Los dominios de primer nivel identifican el tipo de página web que solicitas o bien la localización de la misma, por ejemplo:

- **net** identifica redes.
- **com** identifica comercio.
- **es** identifica localización España.
- **tk** identifica localización Tokelau.

Esto suele ser lo común, más no es obligatorio, es decir, si una empresa posee un dominio **com** puede dedicarse al sector de redes de comunicaciones y no poseer el dominio **net**, así como puede ser una empresa localizada en España y no poseer el dominio **es**.

A nivel gramatical los dominios deben cumplir una serie de requisitos. Por ejemplo:

- Sólo pueden estar compuestos de letras (alfabeto inglés), números y guiones ("").
- No pueden empezar o terminar por guiones.
- Tienen que tener menos de 63 caracteres sin incluir la extensión, y más de uno o dos dependiendo del dominio de primer nivel.

Ahora bien, hoy día ya es posible registrar dominios con caracteres de otras lenguas no inglesas, como la ñ o la ç. Estos dominios se denominan **multilingües**.

### **Jerarquía de nombres de dominio**

El espacio de nombres de dominio (el universo de todos los nombres de dominio) está organizado de forma jerárquica. El nivel más alto en la jerarquía es el dominio raíz, que se representa como un punto (".") y el siguiente nivel en la jerarquía se llama dominio de nivel superior (TLD). Sólo hay un dominio raíz, pero hay muchos TLDs y cada TLD se llama dominio secundario del dominio raíz. En este contexto, el dominio raíz es el dominio principal, ya que está un nivel por encima de un TLD y cada TLD, a su vez, pueden tener muchos dominios hijos. Los hijos de los dominios de nivel superior se llaman de segundo nivel, los del segundo nivel se llaman de tercer nivel, los del tercer nivel de cuarto, y así sucesivamente.

Por lo tanto el DNS, organiza los nombres de máquina (hostname) en una jerarquía de dominios separados por el carácter punto '!'. Un **dominio** es una colección de nodos relacionados de alguna forma -porque están en la misma red, tal como los nodos de una empresa-. Por ejemplo:

```
rrhh.departamento.empres.org
marketing.departamento.empres.org
contabilidad.consultas.empres.org
```

Donde:

- La empresa agrupa sus nodos en el dominio de primer nivel "org". Éste es un TLD.
- La empresa tiene un subdominio, dominio de segundo nivel "empresa" bajo "org". Así "empresa" es un dominio de segundo nivel, hijo del TLD "org".

- A su vez puedes encontrar nuevos subdominios dentro, en este caso: "departamento" y "consultas". Es decir, dominios de tercer nivel, hijos a su vez del dominio de segundo nivel "empresa".
- Finalmente, un nodo que tendrá un nombre completo conocido como totalmente cualificado o FQDN, que es la concatenación de: TLD, dominio de segundo nivel, dominio de tercer nivel, etc., tal como:

`rrhh.departamento.empres.org, marketing.departamento.empres.org, contabilidad.consultas.empres.org.`

También es posible tener un dominio de cuarto nivel, dominio de quinto nivel, y así sucesivamente.

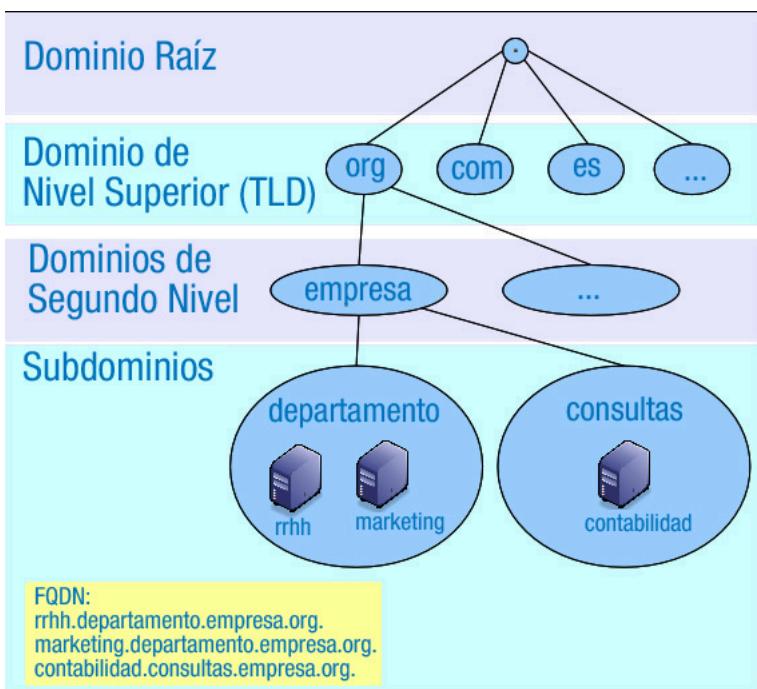
En la siguiente figura puedes ver una parte del espacio de nombres. La raíz del árbol, que se identifica con un punto sencillo, es lo que se denomina dominio raíz y es el origen de todos los dominios. Para indicar que un nombre es FQDN, a veces se termina su escritura en un punto, aunque por lo general se omite. Este punto significa que el último componente del nombre es el dominio raíz. Así, por ejemplo, en el nombre de dominio:

El símbolo del dominio raíz es el punto situado más a la derecha del nombre del dominio.

Sólo hay una raíz de dominio, pero hay más de 250 dominios de nivel superior, clasificados en los siguientes tres tipos:

- TLD de código de país (ccTLD): dominios asociados con países y territorios. Hay más de 240 ccTLD. Están formados por 2 letras, por ejemplo: es, uk, en, y jp.
- Dominios de nivel superior genéricos (gTLD): están formados por 3 o más letras. A su vez se subdividen en:
  - Dominios de internet patrocinados (sTLD): representan una comunidad de intereses, es decir, detrás existe una organización u organismo público que propone el dominio y establece las reglas para optar a dicho dominio. Por ejemplo: edu, gov, int, mil, aero, museum.
  - Dominios de internet no patrocinados (uTLD). Sin una organización detrás que establezca las reglas para optar a dicho dominio. La lista de gTLD incluye: com, net, org, biz, info.

CIFP VIRGEN DE GRACIA



## DNS dinámico

Si dispones de una conexión a Internet con IP dinámica, ¿es posible ofrecer servicios en Internet?

Parece claro que si dispones de una IP estática de conexión a Internet, previo pago de un plus por disponer siempre de una misma IP para tu conexión a Internet, simplemente deberías enrutar las peticiones de los servicios que ofreces a los hosts que esperan la conexión a esos servicios. Si además, posees nombres de dominios puedes redirigir esos nombres a las IP de tus hosts a través del servidor DNS.

Pero qué es lo que pasa si quieres hacer lo mismo y no dispones de IP estática. Cada vez que te conectas a Internet, tu IP, aunque a veces sea la misma, puede cambiar. Pues, sí, sí es posible, ¿cómo?. A priori, si lo piensas un poco, lo único que necesitarías sería:

1. Recoger la IP de tu conexión cada vez que te conectas en Internet.
2. Una vez recogida tu IP difundirla en Internet. Para difundirla, o bien lo haces de forma estática, y cada vez que la recoges te preocupas de hacer los cambios necesarios para difundirla, o bien de forma dinámica configuras un programa para que automáticamente recoja la IP y la difunda.

Está claro, que la mejor opción es difundirla de forma dinámica, para ello puedes aprovecharte de servicios ofrecidos, incluso de forma gratuita, por **DynDNS**, **No-IP** y **FreeDNS**. De hecho, hoy en día, los routers que los ISP suelen montar ya poseen la opción de configuración por DNS dinámica.

Entonces, el **DNS dinámico** es un sistema que permite la actualización en tiempo real de la información sobre nombres de dominio situados en un servidor de nombres, siendo usado, mayoritariamente, para asignar un nombre de dominio de Internet a un ordenador con dirección IP variable (dinámica).

El DNS dinámico, así, puede ofrecer servicios en Internet en hosts que posean conexión con dirección IP dinámica, la típica configuración que los ISP ofrecen para conectarse a Internet.

De todos modos, aunque existe la posibilidad de ofrecer servicios en Internet desde tu propia casa, debes tener en cuenta que, usualmente, la infraestructura técnica y la electrónica de red que poseas no se pueda comparar con los servidores ofrecidos por empresas de Hosting, así: ¿posees balanceadores de carga? ¿redundancia en caso de fallos? ¿generadores eléctricos que garanticen conexión eléctrica permanente a pesar de caída eléctrica? ¿Y, sobre todo, dispones del ancho de banda necesario para permitir múltiples conexiones concurrentes sin perjudicar el servicio ofrecido?

## ÁMBITOS: INTRANET, INTERNET Y EXTRANET. CONSIDERACIONES DE SEGURIDAD. CORTAFUEGOS.

### Internet

Esta es la parte más fácil. Se trata de la **red mundial de computadoras**. Se puede definir a internet como un conglomerado de redes locales distribuidas por el mundo, con computadoras que se conectan mediante un protocolo específico.

“Las computadoras con acceso a internet pueden llegar a páginas web, enviar y recibir emails y compartir **archivos y otras informaciones** con cualquier otra computadora alrededor del mundo”, resume Jan Axelson, autor de siete libros sobre tecnología, entre ellos *Embedded Ethernet and Internet Complete: Designing and Programming Small Devices for Networking*.

Internet, uno de los mayores **avances tecnológicos de la humanidad**, reduce la distancia entre las personas y hace posible situaciones inimaginables hace dos décadas. En otras palabras, “estamos todos conectados a internet como una neurona en un cerebro gigante”, según la famosa descripción del físico inglés Stephen Hawking.

La consultora eMarketer, especializada en estudios globales sobre el universo digital, estima que la **mitad de la población mundial** tendrá acceso a internet a partir de 2018. Hacia fines de 2014 había 2.800 millones de personas conectadas, según datos de esa empresa.

### Intranet

La intranet también es una red de computadoras, pero, mientras internet es abierta a cualquier persona con el protocolo necesario, una intranet es un espacio **destinado a determinado público**, para la distribución de informaciones de uso limitado.

En este caso, la red conecta a algunas computadoras entre sí, utilizando servidores locales, **sin acceso externo**. Esta modalidad se utiliza para reducir costos, agilizar la comunicación y garantizar más seguridad a la comunicación, ya que es necesario una identificación del usuario y contraseña para acceder en la red.

### Extranet

La Extranet tiene la misma función de una intranet, pero **permite el acceso externo**, a través de internet. ¿Confuso? Veamos: la extranet continúa siendo una red cerrada y limitada a un determinado grupo de personas, pero se puede ingresar desde cualquier lugar del mundo siempre que el usuario registrado tenga conexión a internet.

Así, es posible descentralizar y ampliar la base de conocimiento. Esta forma también **facilita la interacción** entre personas de un mismo grupo que están separadas, utilizando la seguridad ofrecida por una intranet con la libertad de internet.

### Intranet, extranet e internet en tu empresa

Internet es la **base de la comunicación en los días actuales**, permitiendo transmitir cualquier tipo de archivo con personas distantes, de manera casi instantánea.

La intranet, por su parte, permite que tu empresa cree una red propia para **distribución interna y segura**, lo que también tiende a reducir gastos. Restringes el acceso y puedes utilizar otros protocolos para la comunicación.

Por último, la extranet es útil si se desea **ampliar la relación** con clientes o si se tiene una base de empleados descentralizada, con personas que actúan en diferentes regiones y necesitan comunicarse diariamente entre sí.

### Consideraciones de seguridad

- **La intranet**

Cualquier Intranet es vulnerable a los ataques de personas que tengan el propósito de destruir o robar datos empresariales. Los inexistentes límites de Internet y los protocolos TCP/IP exponen a una empresa a este tipo de ataques.

Las Intranets requieren varias medidas de seguridad, incluyendo las combinaciones de hardware y software que proporcionan:

- el control del tráfico
- la encriptación y las contraseñas para convalidar usuarios
- las herramientas del software para evitar y curar de virus, bloquear sitios indeseables, y controlar el tráfico.

El término genérico usado para denominar a una línea de defensa contra intrusos es *firewall*. Un *firewall* es una combinación de hardware / software que controla el tipo de servicios permitidos hacia o desde la Intranet.

Los *firewall* protegen a las intranets de los ataques iniciados contra ellas desde internet. Están diseñados para proteger una intranet del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos. También están diseñados para impedir que los usuarios internos accedan a los servicios de internet que puedan ser peligrosos, como ftp. Las computadoras de las intranets sólo tienen permiso para acceder a internet después de atravesar un *firewall*.

Un *firewall* de un servidor bastión (un servidor bastión o bastion host es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna) se configura para oponerse y evitar el acceso a los servicios no autorizados. Normalmente está aislado

del resto de la Intranet en su propia subred de perímetro. De este modo si el servidor es atacado, el resto de la Intranet no estará en peligro.

Puede prohibir a los usuarios de una Intranet la obtención de material indeseable. El software puede comprobar cualquier archivo que entra en la Intranet para asegurarse que está libre de virus.

Son muy usados los sistemas de autenticación que son una parte importante en el diseño de la seguridad de cualquier Intranet, ya que se emplean para asegurar que es la persona que dice ser. Los sistemas de autenticación normalmente utilizan nombres de usuario, contraseñas y sistemas de encriptación.

Hay varias formas de instalar la seguridad en la intranet:

#### 1. *EL ENRUTADOR PARA FILTRAR.*

Una manera de asegurarse de que las personas impropias o los datos erróneos no pueden acceder a la Intranet es usar este enrutador.

Es un tipo especial de enrutador que examina la dirección IP y la información de cabecera de cada paquete que entra en la Intranet, y sólo permite el acceso a aquellos paquetes que tengan direcciones u otros datos, como e-mail, que el administrador del sistema ha decidido previamente que pueden acceder a la Intranet.

Un administrador de Intranets establece las reglas que utilizan los enrutadores para tomar decisiones sobre qué paquetes deberían admitir o denegar.

#### 2. *LOS FIREWALLS.*

Se encargan de proteger a las Intranets de los ataques iniciados contra ellas desde Internet, del acceso no autorizado a la información de la empresa, y del daño o rechazo de los recursos y servicios informáticos.

También están diseñados para impedir que los usuarios internos accedan a los servicios de Internet que puedan ser peligrosos, como FTP.

Los administradores de sistemas deciden qué paquetes admitir y cuáles denegar.

Cuando una Intranet está protegida por un firewall, están disponibles los servicios internos usuales de la red, como el e-mail, el acceso a las bases de datos corporativas y a los servicios de la Web, y el uso de programas para el trabajo en grupo.

Las computadoras de las Intranets sólo tienen permiso para acceder a Internet después de atravesar un firewall.

Los firewall seleccionados de la subred tiene una manera más para proteger la Intranet: un enrutador exterior de selección, también denominado enrutador de acceso. Este enrutador selecciona paquetes entre Internet y la red de perímetro y puede proteger a la red incluso si el enrutador interno falla.

### 3. EL SERVIDOR SUSTITUTO.

Es un servidor sustituto software y un servidor que se coloca en un firewall y actúa como intermediario entre computadoras en una Intranet e Internet.

Cuando una computadora en la Intranet realiza una petición a Internet (como recuperar una página Web desde un servidor Web), la computadora interna se pone en contacto con el servidor Internet que envía la página Web al servidor sustituto, que después la mandará a la computadora de la Intranet. Los servidores sustitutos registran todo el tráfico entre Internet y la Intranet, por ejemplo, un servidor sustituto es Telnet, es un protocolo de red que nos permite ver lo que sucede en otra computadora sin necesidad de estar delante de ella por lo que podría seguir la pista de cada pulsación de una tecla en cada sección Telnet en la Intranet, y también podría seguir la pista de cómo reacciona al servidor externo en Internet con esas pulsaciones.

También puede ayudar a los administradores de Intranets a construir mejor acceso y servicios para los empleados. Algunos servidores sustitutos tienen que trabajar con clientes sustitutos especiales. Una tendencia más popular es usar clientes con servidores sustitutos ya configurados.

También pueden hacer efectivos los diseños de seguridad. Por ejemplo podría configurarse para permitir el envío de archivos desde Internet a una computadora de la Intranet, pero impedir que se manden archivos desde la red empresarial a Internet, o viceversa. De este modo, los administradores de Intranets pueden impedir que cualquier persona externa a la corporación reciba datos corporativos vitales. O pueden evitar que los usuarios de la Intranet reciban archivos que puedan contener virus.

### 4. EL ANFITRIÓN BASTIÓN.

Es un servidor fuertemente fortificado que se coloca dentro del firewall, y es el punto de contacto principal de la Intranet e Internet.

Así que, por ejemplo, no debería haber ninguna cuenta de usuarios en un servidor bastión, para que nadie pudiera entrar, tomar el control y después obtener acceso a la intranet.

Los servidores bastión registran todas las actividades para que los administradores de Intranets puedan decir si la red ha sido atacada. A menudo guardan dos copias de los registros del sistema por razones de seguridad: en caso de que se destruya o falsifique un registro, el otro siempre está disponible como reserva.

Los monitores automatizados son programas que comprueban con regularidad los registros del sistema del servidor bastión, y envían una alarma si encuentra un patrón sospechoso. Por ejemplo, se puede enviar una alarma si alguien intenta más de tres conexiones no exitosas. Algunos servidores bastión incluyen programas de auditoria, que examinan activamente si se ha iniciado un ataque en su contra.

Cuando un servidor bastión recibe una petición de un servidor como puede ser enviar una página Web o repartir e-mail, el servidor no administra la petición él mismo; en su lugar, envía la petición al servidor de Intranets apropiado. El servidor de Intranets maneja la

petición, y después devuelve la información al servidor bastión; y será ahora cuando envíe la información requerida al solicitarme en Internet.

#### - La extranet

La seguridad en el diseño de la extranet es fundamental para asegurar que los datos confidenciales sigan siendo confidenciales pese a viajar por la red. Que sólo las personas autorizadas tengan acceso a la información que se comunican las distintas empresas participantes en la extranet.

Las Extranet tienen una complejidad adicional, dado que no sólo están mediando entre el mundo interno de una organización y el mundo externo de Internet, sino que también están mediando entre las culturas de diversas entidades de negocios.

La seguridad es responsabilidad de todas las empresas en conjunto que están en los terminales de los túneles que enlaza a los usuarios que acceden a la red.

La extranet al comprender usuarios locales y remotos distribuidos por todo el mundo y en diversas empresas, se complica las medidas de seguridad. Hoy día, un gran número de empresas utiliza plataformas heterogéneas, lo que dificulta el despliegue de las aplicaciones y la información para todos los usuarios.

La seguridad en las Extranet debe ser rigurosa y evidente. El administrador debe “vender” constantemente a los usuarios la idea de que es un sitio seguro.

Todo esto se traduce en mayores costes para la empresa.

Es de vital importancia tener dentro de la seguridad de la extranet controlado a cada socio, cada uno tiene una dirección IP, por lo que el firewall se debe programar de modo que solo acepte paquetes de mensajes de esas direcciones específicas. Tener un sistema de rastreo y control de acceso personalizado mediante un plan de ingeniería de rastreo de aplicaciones, instalándolo en el firewall y agregándole un servidor.

Si se trata de información muy delicada se debe optar por un dispositivo en forma de tarjeta de crédito de seis dígitos que cambia cada dos minutos.

## 5. Bibliografía.

- [https://es.wikipedia.org/wiki/Historia\\_de\\_Internet](https://es.wikipedia.org/wiki/Historia_de_Internet)
- <http://www.ojosdepapel.com/Index.aspx?blog=918#:~:text=Antonio%20Gonz%C3%A1lez%20Fuentes-,Internet%20se%20inici%C3%B3%20en%20toro%20al%20a%C3%B1o%201969%2C%20cuando%20el,vulnerables%20las%20comunicaciones%20militares%20no%20americanas>
- <https://blog.orange.es/consejos-y-trucos/servicios-de-internet/>
- <https://pc-solucion.es/2018/03/27/tcp-ip/>
- [https://es.wikipedia.org/wiki/Modelo\\_OSI](https://es.wikipedia.org/wiki/Modelo_OSI)
- <https://community.fs.com/es/blog/tcip-vs-osi-whats-the-difference-between-the-two-models.html#:~:text=El%20modelo%20OSI%20es%20gen%C3%A9rico,protocolos%20est%C3%A1ndar%20desarrollados%20por%20Internet>
- <https://www.redeszone.net/tutoriales/internet/protocolos-basicos-redes/>
- [https://es.wikipedia.org/wiki/Direcci%C3%B3n\\_IP](https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP)
- [https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/DAW/DEAW/DEAW01/es DAW DEAW01 Contenidos/website\\_index.html](https://ikastaroak.birt.eus/edu/argitalpen/backupa/20200331/1920k/es/DAW/DEAW/DEAW01/es DAW DEAW01 Contenidos/website_index.html)
- <https://bautil91.wordpress.com/2015/04/23/30/>



CIFP VIRGEN DE GRACIA