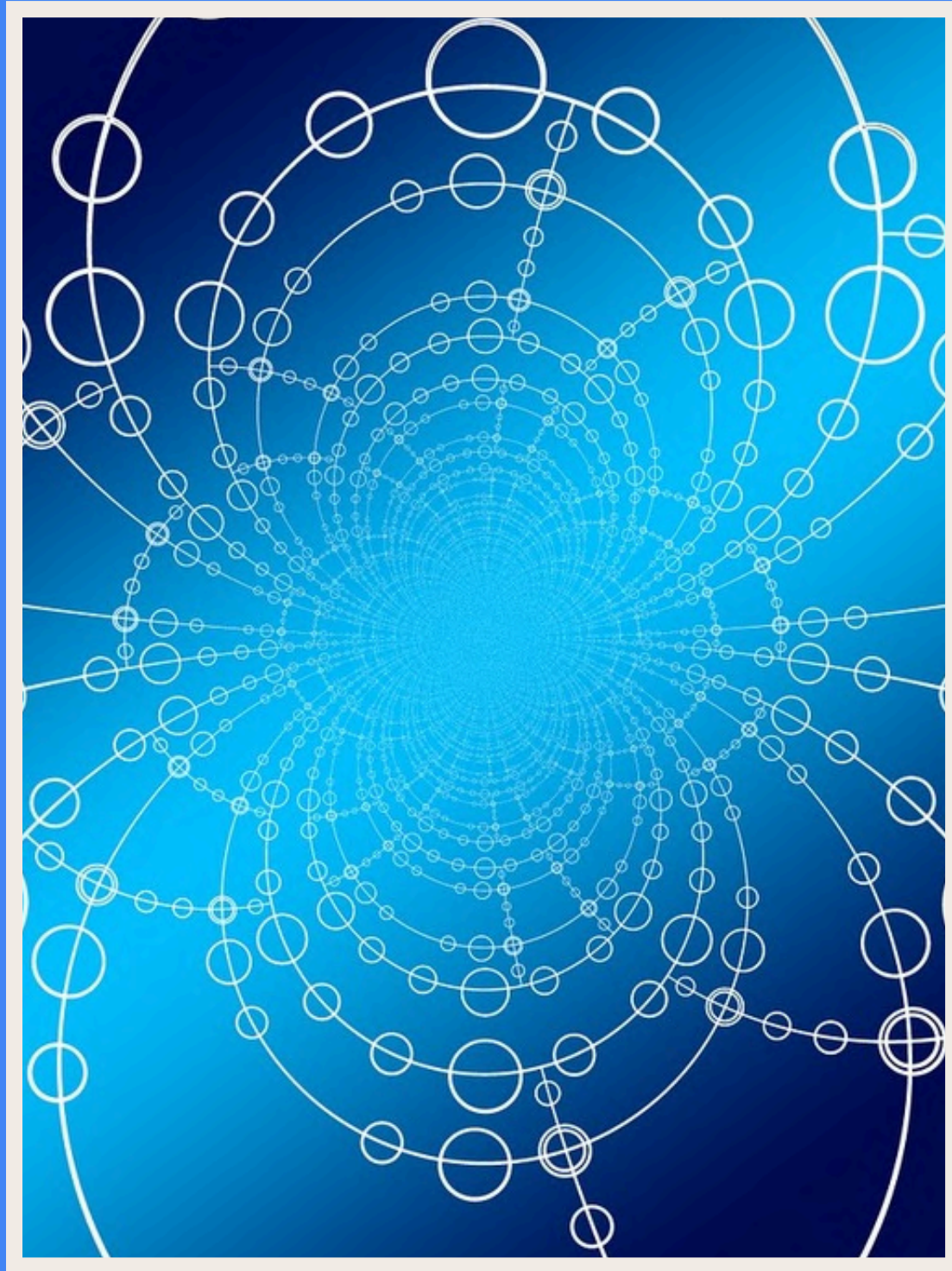


## 3.3 Tipos de redes



## 3.3 Tipos de Redes



# INTRODUCCIÓN

Dada la diversidad de características que presentan las redes informáticas, no existe un único criterio universal para su clasificación. Por esta razón, es necesario considerar múltiples enfoques para entender mejor sus distintas facetas. En los apartados siguientes, examinaremos varios de estos criterios y analizaremos cómo cada uno nos permite categorizar las redes de manera efectiva.



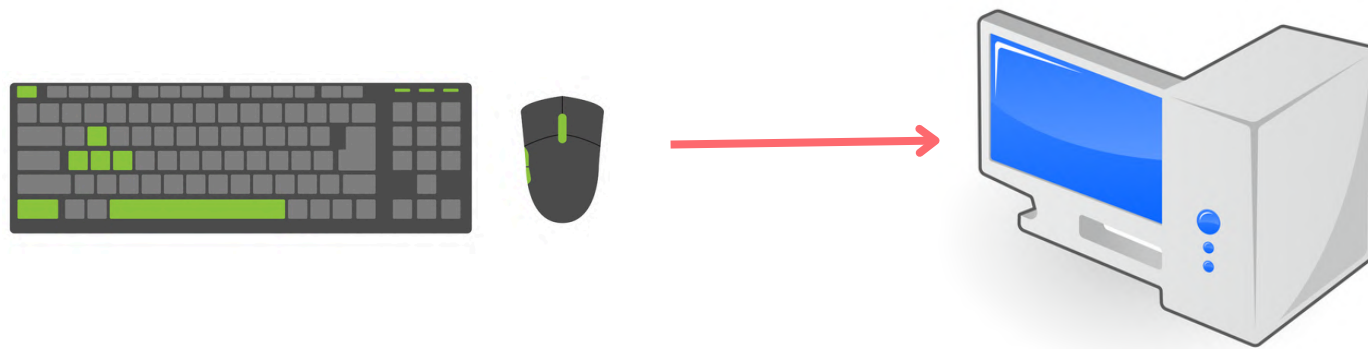
# DIRECCIÓN DE LOS DATOS |

Atendiendo al método de transmisión de los datos dentro de la red podemos distinguir entre:

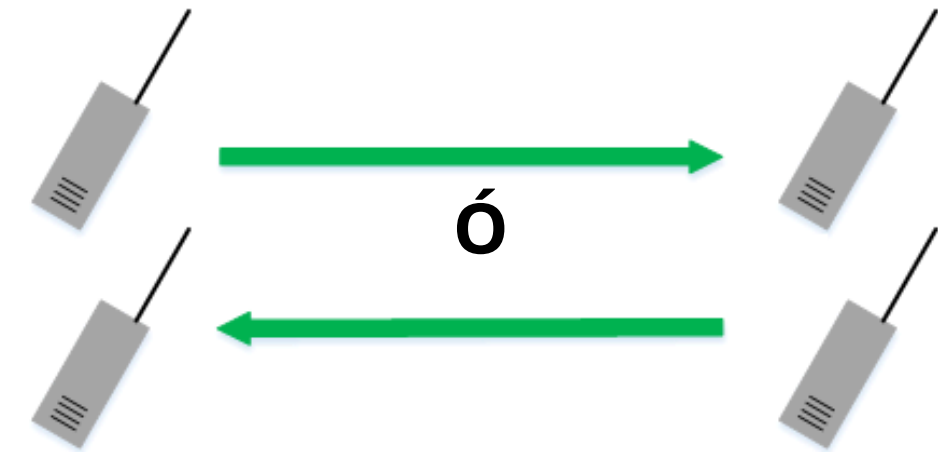
- **Símplex o unidireccional:** Los datos van en una sola dirección.
- **Half-duplex o semidúplex:** los datos pueden ir en ambas direcciones, pero no de forma simultánea.
- **Full-duplex o dúplex:** los datos pueden ir en las dos direcciones de forma simultánea



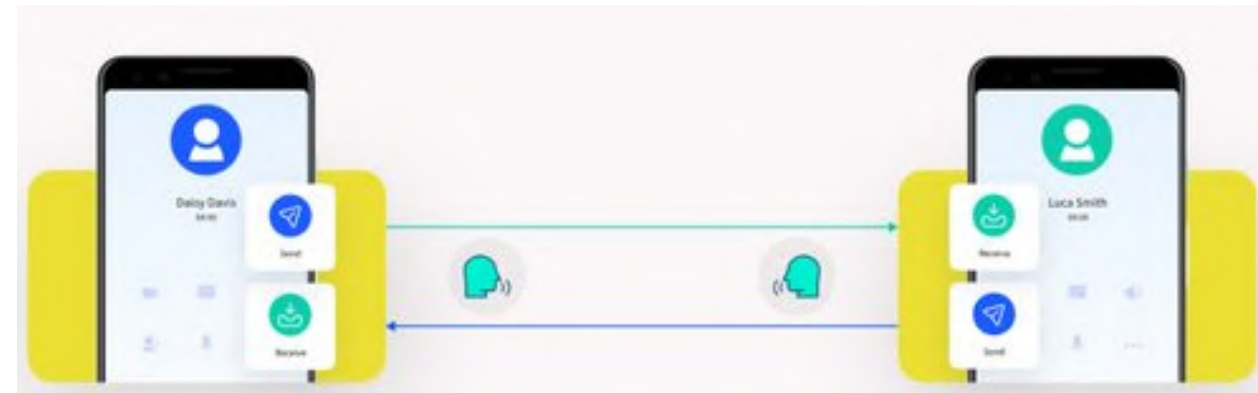
# DIRECCIÓN DE LOS DATOS II



**SIMPLEX**



**HALF-DUPLEX**



**FULL-DUPLEX**



# DESTINATARIOS

- **Unidifusión o unicast:** Los datos van de un usuario a otro. Ejemplo: Email
- **Multidifusión o multicast:** Los datos van de un usuario a varios. Ejemplo: Video streaming.
- **Difusión o broadcast:** Los datos van de un usuario a todos. Ejemplo: Address Resolution Protocol (ARP), el mensaje se emite a toda la red para identificar la dirección MAC relacionada con la dirección IP.





# MEDIO FÍSICO

Atendiendo al medio físico por el que viajan los datos dentro de la red.

- **Cableadas.** Utilizan como medio físico o de transmisión **medios guiados** o cables.
- **Inalámbricas.** Utilizan como medio de transmisión **medios no guiados** como radio-frecuencias, infrarrojos o microondas.
- **Híbridas.** (Se emplean las dos anteriores en la misma red)



# RELACIÓN DE LOS EQUIPOS

Dependiendo de la función que realizan los nodos, la clasificación es como sigue:

- **Entre iguales o peer to peer (p2p).** Todos los nodos son iguales entre sí, no hay ninguno haciendo la función de servidor.
- **Cliente-servidor.** Uno o varios nodos hacen la función de servidores y sirven peticiones a los demás equipos o nodos que hacen las veces de cliente y lanzan peticiones al servidor o a los servidores.



# DIMENSIÓN Y ALCANCE I

Teniendo en cuenta el tamaño y alcance de la red, podemos diferenciar:

- **PAN (Personal Area Network)**. Red de muy corto alcance, puede decirse que es el ámbito de una persona.
- **LAN (Local Area Network)**. Tiene un alcance mayor que la anterior, pero sigue siendo para pequeñas áreas, como una sede de una oficina, una empresa o un centro educativo.

Dentro de este tipo también se puede englobar las siguientes:

- **HAN (Home Area Network)**: Podemos hablar de PAN o LAN de tamaño reducido.
- **VLAN (Virtual Local Area Network)**: Segmenta una LAN en varias LAN, mejorando la seguridad y el tráfico.





# DIMENSIÓN Y ALCANCE II

- **MAN (Metropolitan Area Network)**. Su tamaño es mayor que el de una LAN, pudiendo abarcar una o varias ciudades cercanas.
- **WAN (Wide Area Network)**. Son las redes de mayor alcance. A través de ella, los equipos se pueden conectar en diferentes ciudades, países o continentes. Pueden conectar equipos, redes LAN o MAN.



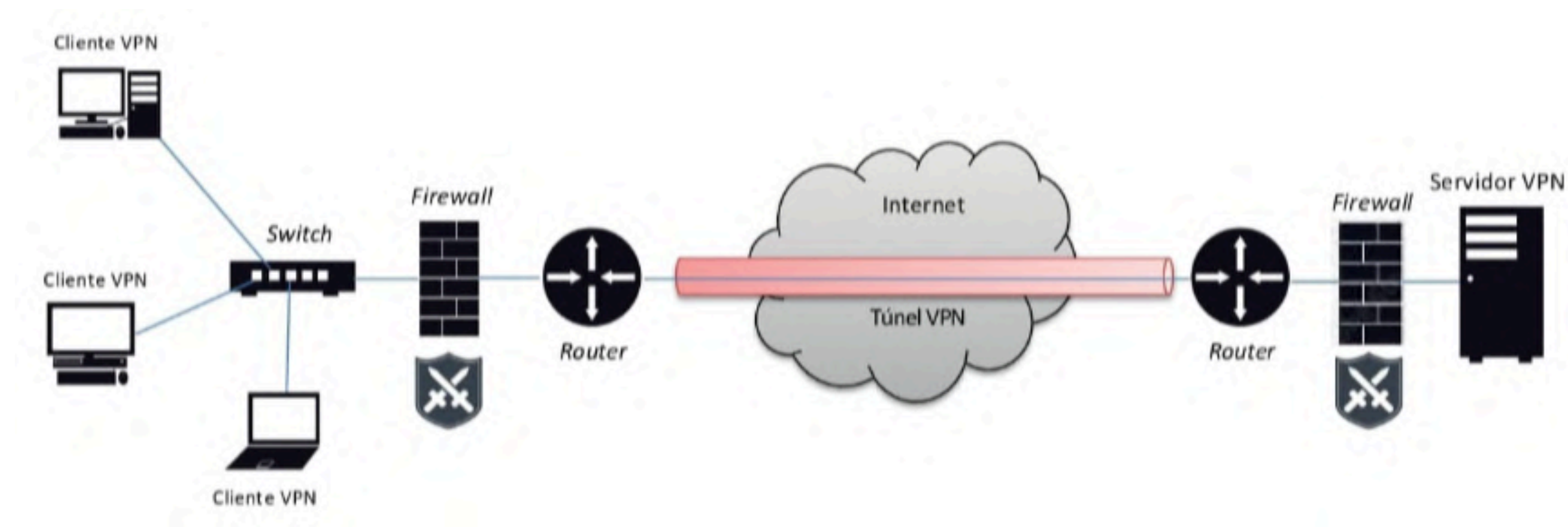
# PRIVACIDAD O PROPIETARIO I

Atendiendo al propietario y quién tiene acceso a la red, podemos distinguir:

- **Pública:** Es una red que ofrece acceso público para los usuarios. Un ejemplo de este tipo de red es internet.
- **Privada:** Solo tienen acceso sus propietarios y los usuarios a los que se les permita acceder. Si la red utiliza parte de red pública y parte de red privada se denomina **híbrida**.
- **Red privada virtual o VPN (Virtual Private Network):** Crea una red virtual entre dos o varios equipos a través de internet, de manera que cada equipo ve a los demás como si estuviesen en una red de área local. Para ello, se crea lo que se denomina un túnel VPN.

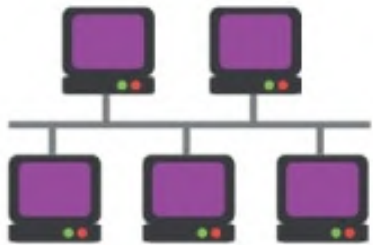



# PRIVACIDAD O PROPIETARIO II



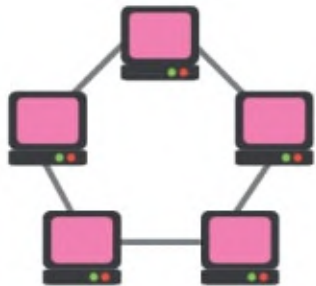
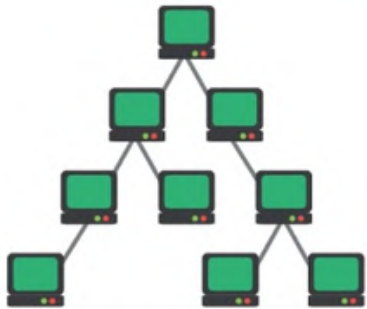

# TOPOLOGÍA I

La topología de una red es el modo en el que se conectan los diferentes nodos o equipos dentro de la misma. Existen diferentes tipos de redes atendiendo a su topología:

	<b>Bus</b>	Todos los hosts están conectados al mismo medio o bus. El problema que tiene es que si falla el bus falla la red entera y los nodos se quedan aislados entre sí.
	<b>Estrella</b>	Conecta los hosts a un dispositivo central. Es muy común por su facilidad de montaje y es fácilmente escalable. Salvo que falle el nodo central, si algún nodo falla la red sigue funcionando sin problemas.

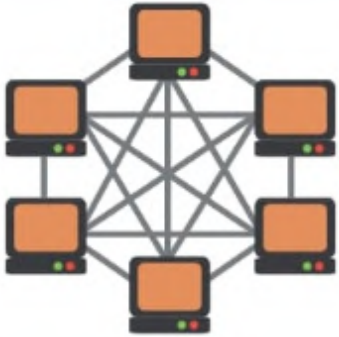



# TOPOLOGÍA II

	<b>Anillo</b>	Un nodo o host se conecta a los dos nodos más cercanos formando un anillo. Al fallar un nodo la red puede seguir funcionando.
	<b>Árbol</b>	Cada nodo está conectado a otros nodos de la red. Los mensajes pueden ir por varias rutas y aunque falle un nodo es posible encontrar otra ruta alternativa.
	<b>Malla</b>	Cada nodo está conectado a otros nodos de la red. Los mensajes pueden ir por varias rutas y aunque falle un nodo es posible encontrar otra ruta alternativa.



# TOPOLOGÍA III

	<b>Totalmente conectada</b>	Se llama también profunda o neuronal o totalmente conexa. Es difícil de implementar, es difícilmente escalable y es costosa. Al ser un sistema totalmente conectado, la red puede funcionar sin problemas aunque falle un nodo
	<b>Línea</b>	Parecida a la topología en bus, pero en este caso los nodos están conectados unos a otros. Si falla cualquier nodo, los demás pueden quedar aislados entre sí, al igual que la topología en bus.
	<b>Mixta</b>	Una red mixta está formada por varias redes de diferentes tipos.





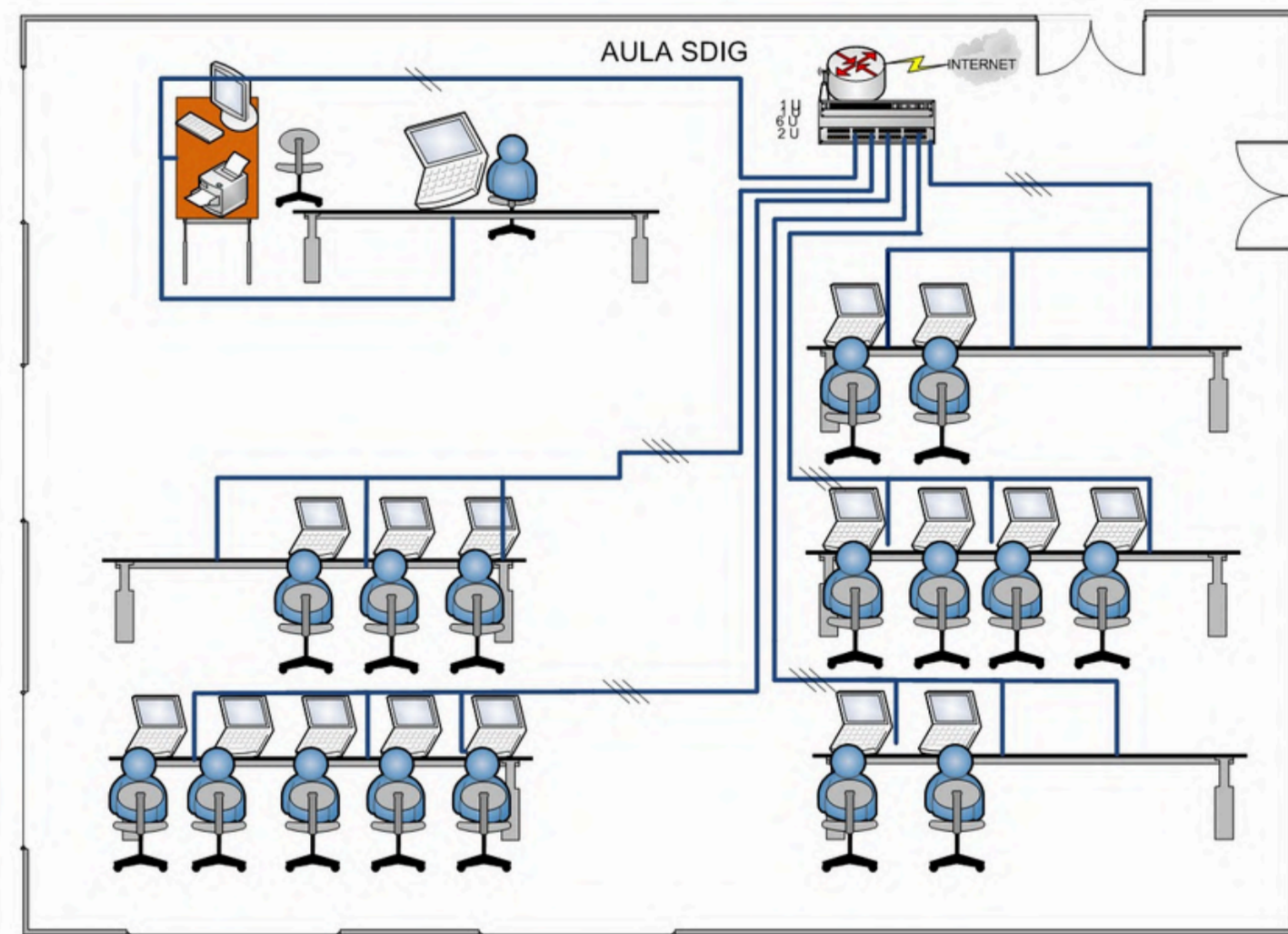
# MAPAS FÍSICOS Y LÓGICOS |

Cuando se quiere diseñar una red o ver y estudiar una ya creada para poder mejorarla o actualizarla, es necesario realizar un mapa físico y otro lógico de ella. Estos mapas pueden solucionar problemas de diseño o seguridad, además son útiles para documentar la red una vez creada y poder consultarlos para modificarla o buscar posibles errores.

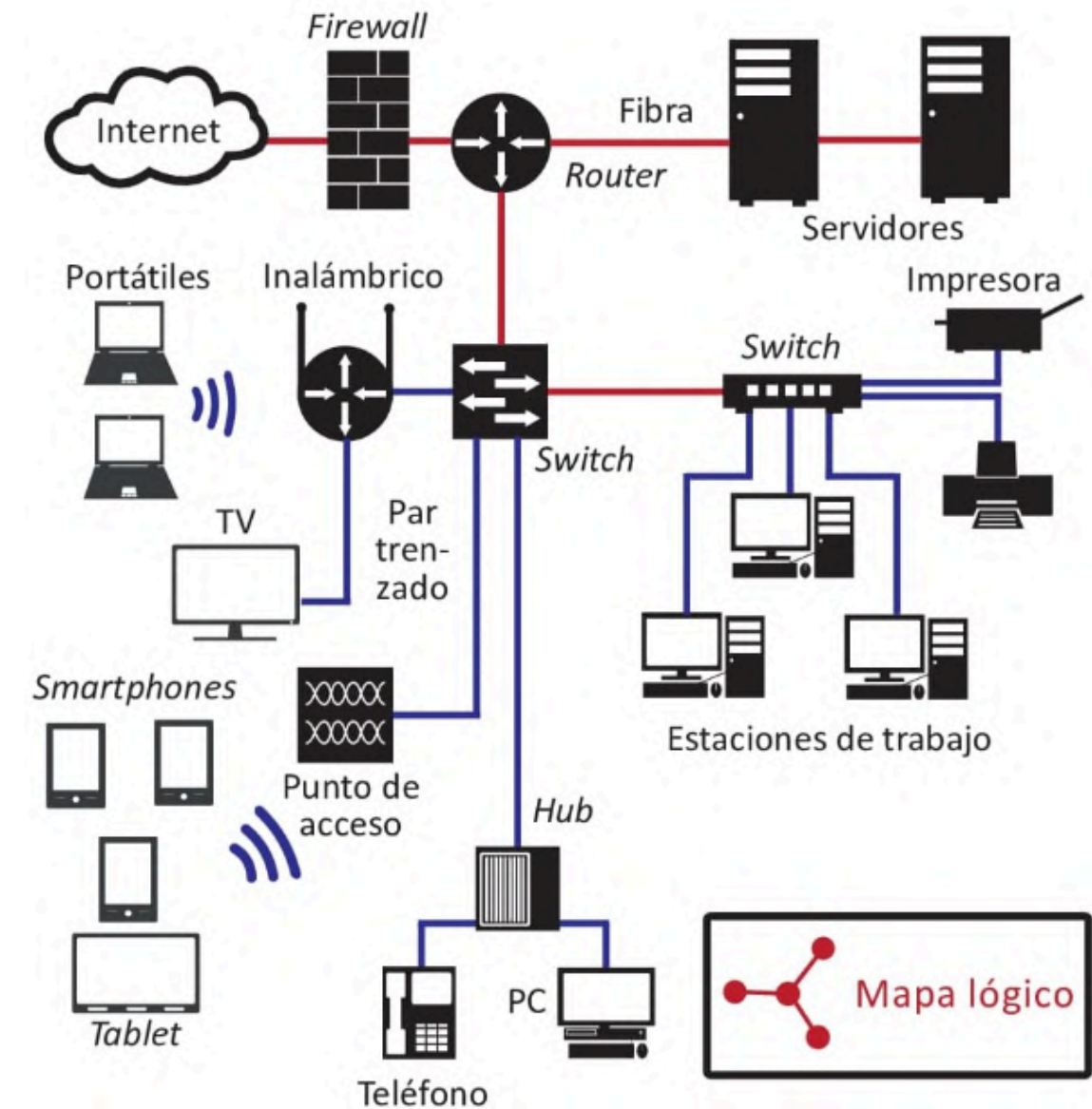
- **Mapa lógico:** es un gráfico esquemático que permite ver los elementos de una red, como sus hosts, los servidores, los dispositivos de conexión, los medios, las subredes dentro de la red, el tipo de direccionamiento, la dirección IP de los equipos que la tengan estática...
- **Mapa físico:** se puede representar la red dentro del espacio real donde se encuentra, como los edificios, las plantas donde se encuentra cada nodo, los metros entre ellos, etcétera



# MAPAS FÍSICOS Y LÓGICOS II



Mapa Físico



Mapa lógico



## 3.4 Modelos de referencia



## 3.4 Modelos de referencia



# INTRODUCCIÓN

Para explicar la comunicación entre los equipos de una red, existen dos modelos de referencia fundamentales que descomponen la transmisión de datos en diferentes capas. Cada capa tiene funciones específicas y protocolos asociados, lo que facilita el diseño y la comprensión de las redes. Estos modelos son esenciales para asegurar la interoperabilidad y eficiencia en la comunicación entre dispositivos y tecnologías diversas.



# MODELO OSI |

El modelo OSI (**O**pen **S**ystems **I**nterconnection) es un modelo teórico de referencia utilizado para la interconexión de diferentes tipos de sistemas. Se usa para describir los componentes de la comunicación de datos, para poder establecer reglas y estándares acerca de las aplicaciones y la infraestructura de red. El modelo OSI contiene siete capas o niveles que se apilan (conceptualmente) de abajo a arriba. Cada nivel se comunica con los adyacentes añadiendo una serie de cabeceras o información a los paquetes que se trasladen verticalmente a través de los niveles.





# MODELO OSI

Capa o Nivel	Función
Aplicación	Permite a las aplicaciones acceder a las demás capas.
Presentación	Cifra y comprime los datos.
Sesión	Permite a los usuarios establecer más de una sesión.
Transporte	Se asegura y confirma que los datos han llegado a su destino.
Red	Encamina de la manera más adecuada (óptima) los datos por la red.
Enlace	Agrupar los datos y se encarga de que no haya errores en la transmisión.
Física	Se encarga de todo lo relativo a la parte física de la transmisión.





# MODELO TCP/IP

El modelo TCP/IP es una arquitectura de red formada por gran variedad de protocolos. Es la más usada, ya que es la base de la comunicación en Internet. Toma su nombre de los dos protocolos más importantes del modelo: TCP (**T**ransmission **C**ontrol **P**rotocol) e IP (**I**nternet **P**rotocol). Se podría decir que el modelo TCP/IP es en realidad una pila o conjunto de protocolos que cubren los distintos niveles del modelo OSI.

El modelo TCP/IP está compuesto por cuatro capas o niveles que realizan una función similar a las capas del modelo OSI. Cada capa realiza una función para preparar el envío y la recepción de los datos a través de una red.



# MODELO TCP/IP II

Capa o Nivel	Función
<b>Aplicación</b>	Se encarga de lo relacionado con los datos del usuario, del envío y recepción
<b>Transporte</b>	Se dividen los datos y se crean paquetes
<b>Internet</b>	Envía los paquetes por la red y establece la mejor ruta.
<b>Acceso a la red</b>	Se encarga de lo relacionado con el envío físico de los paquetes.



## MODELO TCP/IP III

El usuario envía los **datos** desde la capa de aplicación a la capa de transporte, donde se dividen en **segmentos** (TCP) o **datagramas** (UDP) y se les añade una cabecera; posteriormente se les añade otra cabecera IP para indicar dónde enviar esos **paquetes**, que finalmente viajan en **tramas** por el medio físico.

Capa TCP/IP	Direccionamiento	En la cabecera del mensaje se incluyen:	Ejemplo
Transporte	Puertos asociado a la aplicación de origen-destino	Puertos	HTTP: Puerto 80
Internet/Red	Direcciones lógicas de origen/destino (host de origen-host de destino final)	Direcciones IP	IP del PC de origen que solicita ver una web IP del servidor web que contiene la web.
Acceso a red/Subred	Direcciones físicas de origen/destino para cada salto del trayecto (de una tarjeta de red a la siguiente)	Direcciones MAC	Primer salto: MAC de la tarjeta de red del host de origen - MAC de la tarjeta de red del router de su red local



# MODELO TCP/IP - OSI

Mientras que el modelo OSI es más detallado e incorpora un mayor número de niveles o capas, lo que lo hace útil para comprender los principios de la comunicación en red, el modelo TCP/IP es más práctico y es utilizado en la implementación real de redes.

Los modelos también se diferencian en cómo viajan los datos a través de los niveles. En ambos modelos la información del usuario viaja desde la capa superior a la inferior en el envío de los datos, viajan por la red, y en el destino la información va desde la capa inferior a la superior.



# PROTOSCOLOS DEL MODELO TCP/IP

Se denomina pila de protocolos TCP/IP porque sobre los protocolos TCP e IP hay toda una serie de protocolos que completan la función de estos dos. Se utiliza el término pila porque los protocolos van asociados a una capa o nivel, es decir, como si estuviesen apilados unos sobre otros.

A continuación veremos los más utilizados en los diferentes niveles o capas del modelo.



# CAPA DE APLICACIÓN

Nombre	Función
<b>DNS</b>	Protocolo del sistema de nombres de dominio
<b>HTTP, HTTPS</b>	Protocolos web
<b>FTP, TFTP</b>	Protocolos de transferencia de ficheros.
<b>SMTP, POP, IMAP</b>	Protocolos de correo electrónico
<b>LDAP, LADPS</b>	Protocolos de los servicios de directorios.

Nombre	Función
<b>Telnet, SSH</b>	Acceso remoto y acceso remoto con seguridad.
<b>HTTP, HTTPS</b>	Protocolos web
<b>SMB/CIFS</b>	Protocolo para compartir archivos e imprimir.
<b>NFS</b>	Protocolo para acceder remotamente a archivos y directorios.
<b>SNMP</b>	Protocolo usado para la gestión de la red.





# CAPA DE TRANSPORTE

- **TCP** (**T**ransmisión **C**ontrol **P**rotocol): Se encarga de crear conexiones y garantiza la entrega de los datos.
- **UDP** (**U**ser **D**atagram **P**rotocol): Es un protocolo que no requiere conexión y envía la información a través de mensajes o datagramas.
- **SCTP** (**S**tream **C**ontrol **T**ransmission **P**rotocol): Reúne características de los dos anteriores. Está orientado a la conexión y la transferencia la realiza transmitiendo mensajes.
- **TLS** (**T**ransport **L**ayer **S**ecurity): Se utiliza para la transferencia de la información entre sitios web de forma segura y cifrada, para evitar que pueda ser interceptada o modificada. Es una subcapa que se encuentra entre los niveles de aplicación y transporte, ya que trabaja con muchos protocolos de la capa de aplicación añadiendo seguridad a los mismos. Su antecesor es **SSL** (**S**ecure **S**ocket **L**ayer).



# CAPA DE INTERNET

- **IPv6** y **IPv4** (Internet **P**rotocol) son los protocolos encargados de encaminar los datos a través de su dirección IP. No están orientados a la conexión y trabajan con datagramas.
- **IPSec** incorpora seguridad a los protocolos IP. Es un conjunto de protocolos que se encarga de asegurar el cifrado y la autenticidad de los paquetes.
- **ARP** (**A**ddress **R**esolution **P**rotocol) y **RARP** (Reverse ARP) se utilizan para conocer la dirección IP de un host a través de la MAC o al revés.
- **ICMP** (Internet **C**ontrol **M**essage **P**rotocol) se utiliza para enviar mensajes de control entre redes. Se utiliza para ver si hay conexión entre dos nodos y para comprobar la latencia.
- **IGMP** (Internet **G**roup **M**anagement **P**rotocol) se utiliza para gestionar la multidifusión en las redes.



# CAPA DE ACCESO A LA RED

- **Ethernet** es el protocolo para acceder al medio. Todos los nodos comparten el mismo canal, es de difusión y un mensaje puede llegar a todos los nodos.
- **Wifi** es un protocolo para acceder al medio en las redes inalámbricas.
- **PPP** (**P**oint to **P**oint **P**rotocol). **PPPoE** (PPP over Ethernet, PPP sobre Ethernet) y **PPPoA** (**PPP** over **A**TM) son protocolos para las conexiones punto a punto.



# NÚMERO DE PUERTO |

Cada protocolo suele trabajar en un número de puerto por defecto. Los puertos son un número entero que utiliza TCP/IP para identificar la aplicación a la que debe enviar y de la que debe recibir los paquetes y los datos que se envían por la red.

El puerto de origen se asigna de forma dinámica para que pueda haber más de una comunicación a la misma aplicación. El puerto de destino suele ser un puerto predeterminado, pero es configurable. Por ejemplo, se puede tener un servidor web escuchando los puertos 80 y 443, dependiendo del protocolo con el que se accedan.



# NÚMERO DE PUERTO II

En general, no puede haber dos aplicaciones escuchando un mismo puerto. Por ejemplo, para tener dos servidores web en funcionamiento, se puede hacer que cada uno escuche en un número de puerto diferente. Cuando se accede a ese servidor se indican la dirección IP (que identifica al equipo dentro de la red) y el número de puerto (que identifica a la aplicación dentro del servidor). El conjunto de dirección IP y número de puerto se denomina **socket**.

Los puertos se representan por un número entero de 16 bits, es decir, el rango de números de puertos es del 0 al  $2^{16}-1$  (65535) y dentro de ellos los primeros 1024, es decir, del 0 al 1023 se les conoce como puertos bien conocidos, que están reservados para aplicaciones y servicios más utilizados.



# NÚMERO DE PUERTO III

Otros puertos son los registrados por diferentes aplicaciones de usuarios (1024 a 49151) y los puertos efímeros o dinámicos o privados (49152 a 65535) que se generan en el equipo del cliente para una comunicación o servicio.





# HTTP Y HTTPS I

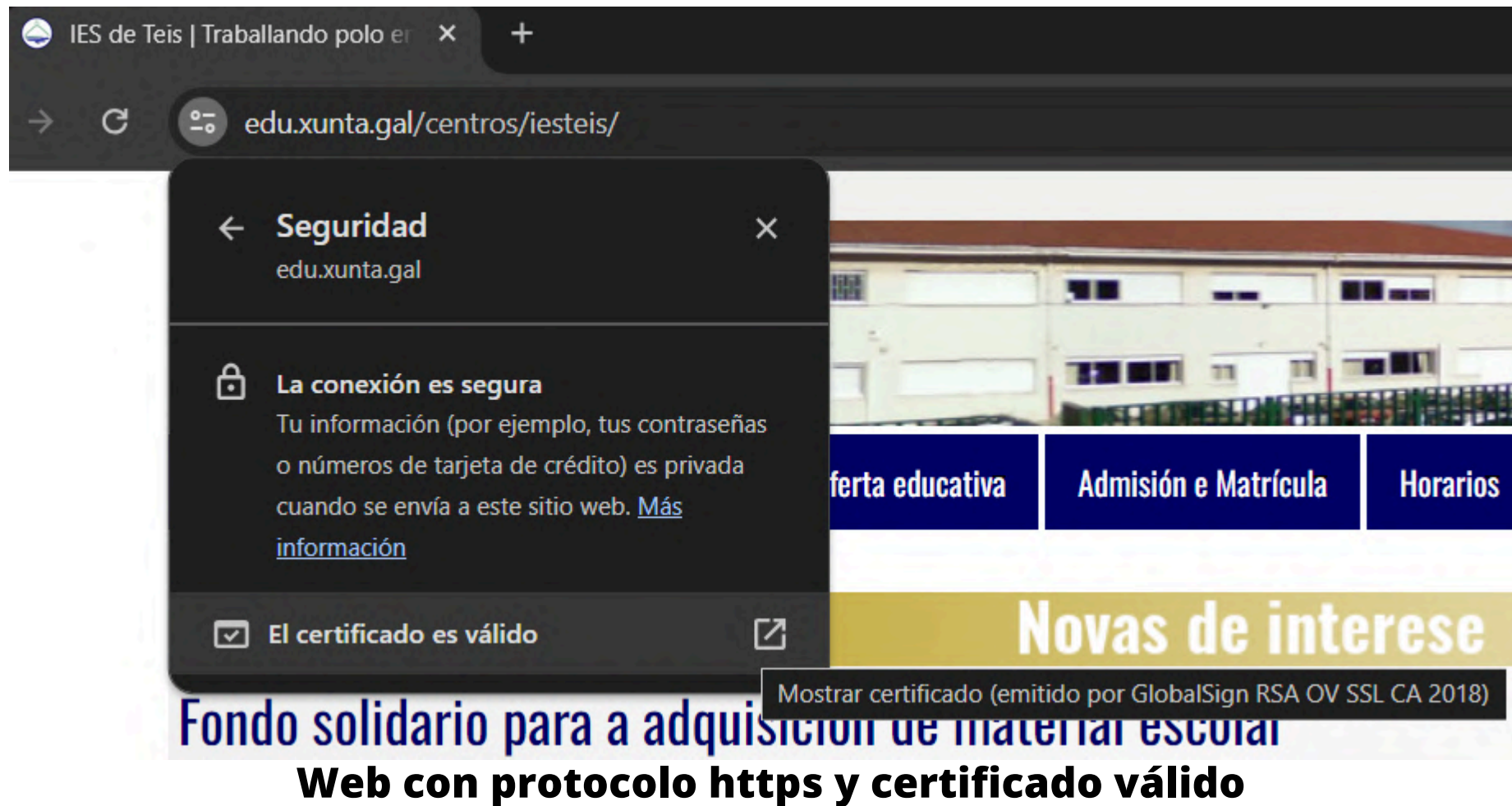
**HTTP** (**H**ypertext **T**ransfer **P**rotocol) y **HTTPS**(HTTP sobre SSL/TLS) permiten la transferencia de información desde un servidor con archivos de tipo HTML. El cliente usa un navegador web para ver la información. HTTP utiliza por defecto el puerto 80, mientras que HTTPS utiliza el 443.

**HTTPS** (**H**ypertext **T**ransfer **P**rotocol **S**ecure, protocolo seguro de transferencia de hipertexto) es la versión segura de HTTP. Utiliza un certificado SSL, la transferencia es cifrada a tra-vés de la red y solamente el navegador y el servidor web pueden descifrarla. El certificado debe estar instalado en el servidor.



## 3.4 Modelos de referencia

# HTTP Y HTTPS II



El protocolo se basa en ofrecer protección en el envío de la información a través de inter-net, basada en una confianza proporcionada por una autoridad certificadora. El estándar actual es HTTP/2, que funciona con TCP, pero se está desarrollando un estándar HTTP/3 que trabaja con UDP para hacerlo más rápido.



# TRANSFERENCIA DE FICHEROS I

- El protocolo **FTP** (**F**ile **T**ransfer **P**rotocol) se utiliza para transferir archivos entre equipos. En la capa de transporte utiliza el protocolo TCP. Utiliza por defecto el puerto 21.
- **TFTP** (**T**rivial **F**TP) es un protocolo FTP que funciona bajo el protocolo UDP, con lo cual es simple, rápido, pero tiene algunas restricciones y es menos seguro, no asegura la descarga o subida libre de errores y se suele utilizar en archivos pequeños y cuando no se requiera mucha seguridad. Por defecto utiliza el puerto 69.



# TRANSFERENCIA DE FICHEROS II

FTP es un protocolo rápido para utilizarlo en descargas de archivos, pero si se quiere seguridad habrá que utilizar una versión segura del mismo, como:

- **FTPS** (**S**ecure **F**ile **T**ransfer **P**rotocol) es el protocolo FTP sobre SSL.
- **SFTP** (**S**ecure **F**ile **T**ransfer **P**rotocol). Este protocolo es FTP sobre SSH. Es diferente al anterior ya que se basa en el protocolo SSH y realiza una conexión segura donde hay que autenticarse y se cifra la información a transferir. Utiliza el método de clave pública y privada o cifrado asimétrico: la clave pública es la encargada de cifrar la información y la clave privada se encarga de descifrar esa información. En FTP también se pueden utilizar nombres de usuario y contraseñas, pero en este protocolo estos datos están cifrados. Utiliza por defecto el puerto 22.



# CONEXIÓN REMOTA

El equipo debe tener un servidor y el equipo desde el que se acceda deberá tener un cliente de estos protocolos o utilizar un programa como Putty. Al conectar de forma remota al equipo servidor se puede realizar cualquier operación como si se estuviera trabajando en el mismo equipo. Protocolos:

- **Telnet** es un protocolo no seguro que escucha por defecto el puerto 23. **En desuso.**
- **SSH** (**S**ecure **S**hell) es un protocolo seguro, que ha venido a sustituir al anterior. Trabaja por defecto en el puerto 22. Se utiliza para acceder a equipos de forma remota mediante un intérprete de órdenes o comandos. Además del acceso remoto tiene otras funciones, como la de transferir ficheros de forma segura utilizando el protocolo SFTP, o crear un canal seguro para intercambiar información entre equipos. SSH genera una clave pública y otra privada. La clave pública se envía al destino y allí se asocia a la cuenta de origen.



# PROTOSCOLOS DE ESCRITORIO REMOTO

Estos protocolos permiten al igual que los anteriores conectarse mediante acceso remoto a un equipo remoto, pero usando el entorno gráfico. Accedemos al escritorio del otro equipo.

- **VNC (Virtual Network Computing)**. Protocolo de escritorio remoto de software libre. Se puede utilizar con diversas aplicaciones en sistemas operativos Linux, Windows y macOS. Utiliza por defecto el puerto 5900.
- **RDP (Remote Desktop Protocol)**. Protocolo desarrollado por Microsoft. Utiliza por defecto el puerto 3389. Se puede utilizar en Linux con XRDP, que es una implementación de software libre de este protocolo





# PROTOSCOLOS DE CORREO ELECTRÓNICO

Los protocolos de correo electrónico se utilizan para establecer una comunicación entre dos nodos de manera que se pueda transferir un mensaje de correo electrónico de uno a otro. El envío de estos correos se hace a través de un servidor de correo electrónico. Existen varios protocolos que se diferencian en la forma de establecer la conexión y la forma de trabajar con los correos.

- **SMTP y SMTP seguro (SMTP sobre TLS/SSL)** se utilizan para enviar correos electrónicos desde una aplicación cliente de correo. Utiliza por defecto el puerto 464 (o 25), y el 587 en su forma segura.
- **POP3 y POP3 seguro (POP3 sobre TLS/SSL)** se utilizan para recibir correos electrónicos desde una aplicación cliente de correo. Utiliza por defecto el puerto 110, y el 995 en su forma segura.
- **IMAP e IMAP seguro (IMAP sobre TLS/SSL)** se utilizan en lugar de POP3 para no descargar los correos desde el servidor en el equipo propio, sino trabajando con ellos en el servidor. Utiliza por defecto el puerto 143, y el 993 en su forma segura



# PROTOCOLO PARA COMPARTIR RECURSOS

**SMB**(**S**erver **M**essage **B**lock) es un protocolo para ofrecer acceso a recursos dentro de una red, como archivos, directorios o impresoras. Utiliza por defecto el puerto 445. Inicialmente era **SMB/CIFS** en la versión 1.0 del protocolo, que fue mejorando en las versiones siguientes, como SMB 2.0. SMB 3.1.1 implica también tener una conexión segura. Linux puede implementar este protocolo a través de Samba.



# PROTOSCOLOS PARA COPIAS REMOTAS

Existen varios protocolos que permiten realizar copias remotas de un equipo a otro.

- **RCP** (**R**emote **C**opy) se utiliza en los sistemas Linux. No es seguro, por lo que se recomienda alguno de los siguientes.
- **SCP** (**S**ecure **C**opy **P**rotocol) es la versión segura del protocolo anterior; utiliza RCP sobre SSH.
- **RSYNC** (**R**emote **S**ynchronization) permite copiar y sincronizar carpetas remotas.



# PROTOSCOLOS DE DIRECTORIO ACTIVO

Se utilizan para iniciar sesión en los ordenadores a través de la red. Sirven para controlar quién se puede conectar y quién tiene acceso a determinados recursos. El protocolo de servicio de directorio activo y su variante con seguridad son **LDAP** (**L**ightweight **D**irectory **A**ccess **P**rotocol) y **LDAPS**. En Windows este protocolo lo usa Active Directory y en Linux se instala a través de OpenLDAP. Utiliza los puertos predeterminados 389 y 636 para la versión segura.



Realizar **tarea 2** del aula virtual

