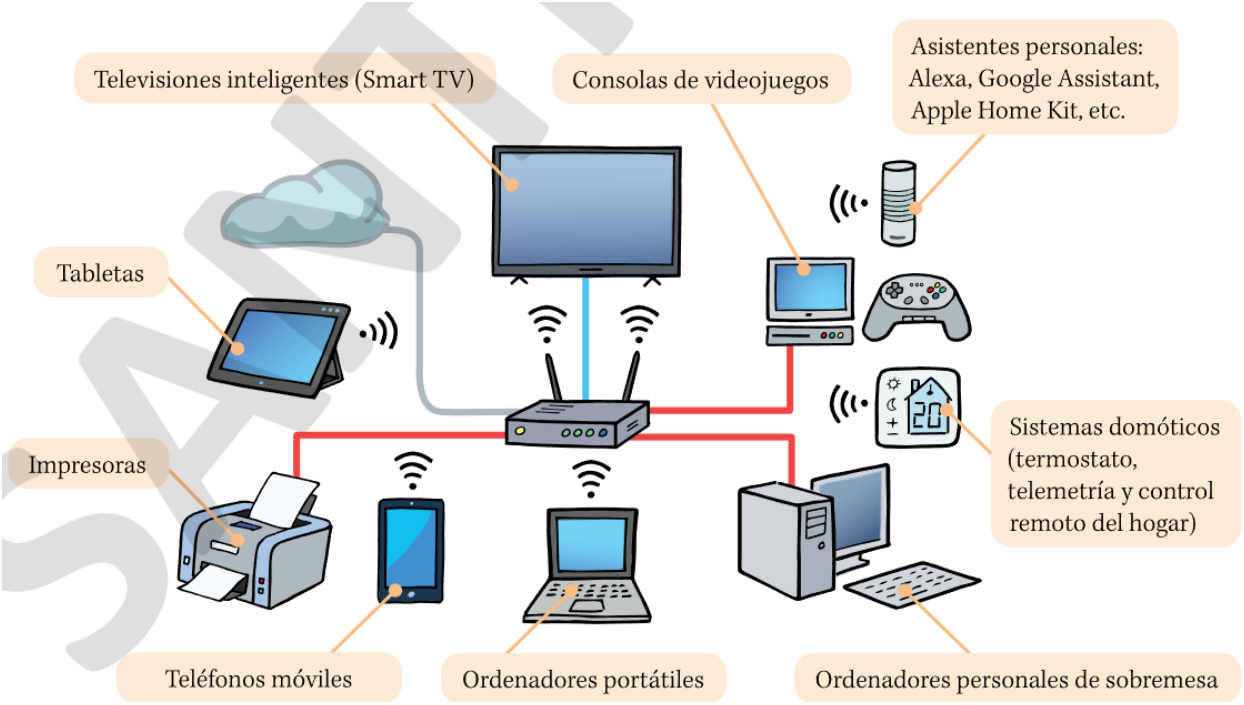
# UD 05: REDES E INTERNET

## 1.- REDES INFORMÁTICAS

Una **red informática** es un conjunto de ordenadores y otros dispositivos (impresoras, teléfonos móviles, Smart TV, asistentes personales, sistemas domóticos, wearables, etc.) conectados entre sí mediante cables o medios inalámbricos, con el objetivo de compartir datos y recursos.




### 1.1.- TIPOS DE REDES

Según la **cantidad de equipos conectados y la distancia** que hay entre ellos, las redes se dividen en:

- ***PAN (Personal Area Network):*** red de área personal, está formada por pequeña cantidad de equipos situados a corta distancia (máximo de 10 metros). Si la conexión es inalámbrica se denominan WPAN.

- ***LAN (Local Area Network):*** red de área local, conecta ordenadores en un área reducida, normalmente una casa u oficina. Su extensión está limitada físicamente a un edificio o a un entorno de hasta 200 metros. Cuando la conexión es inalámbrica se denominan WLAN.

- ***MAN/WMAN (Metropolitan Area Network):*** red de área metropolitana, conectan redes situadas en una ciudad, área industrial o varios edificios. Un ejemplo de ellas pueden ser las redes wifi gratuitas de las ciudades. Cuando la conexión es inalámbrica se denominan WMAN.

- ***WAN/WWAN (Wide Area Network):*** red de área amplia, conecta equipos en un entorno muy amplio como ciudades, países o continentes. Cuando la conexión es inalámbrica se denominan WWAN.

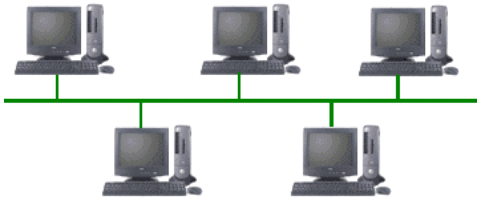
Según el **medio físico** utilizado pueden ser:

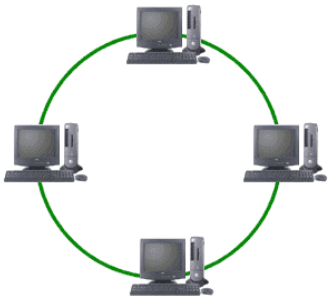
- ***Alámbricas***: utilizan cable para transmitir los datos.
- ***Inalámbricas:*** utilizan ondas electromagnéticas para transmitir los datos.
- ***Mixtas:*** utilizan cable y ondas electromagnéticas para transmitir los datos.

### 1.2.- TOPOLOGÍA DE REDES

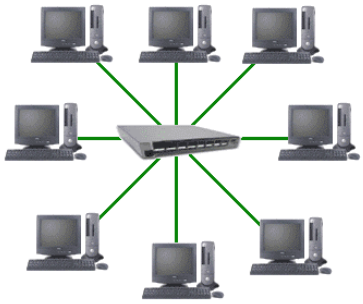
Se denomina **topología de una red** a la forma o distribución de los diferentes equipos que forman una red. Las principales son:

- ***Bus:*** consta de un único cable por el cual fluyen los datos, al que se conecta cada ordenador. Es fácil de instalar, mantener y añadir nuevos ordenadores además de que, si uno de estos se cae, la red sigue intacta, pero si el cable se rompe, la red deja de funcionar.





- ***Anillo:*** un equipo se conecta a otro y este al siguiente y así sucesivamente. Es fácil de detectar cuándo un equipo cae, pero si uno de estos falla, toda la red se paraliza.



- ***Estrella:*** todos los equipos están conectados a un único punto denominado nodo, que actúa de concentrador. Alguna de sus ventajas es que es fácil de detectar cuando hay averías, y si se desconecta uno de los ordenadores no se inutiliza la red.

- ***Árbol:*** es denominada así por su apariencia. En ella, un servidor o proveedor se conecta a un router central. En este, a su vez, se conectan otros switch, que se conectan a las estaciones de trabajo.

## 1.3.- DISPOSITIVOS DE RED

Una red consta de diferentes elementos que canalizan la información entre los distintos puntos (nodos) de la misma, los básicos son los siguientes elementos:

- ***Router:*** es un dispositivo destinado a **interconectar diferentes redes entre sí,** por ejemplo, una LAN con una WAN y también es el que nos permite **conectar nuestra red a Internet.** Es capaz de **guiar el tráfico de datos por el camino más adecuado**, conectar redes, gestionar direcciones IP y conectar los dispositivos a internet.

Switch

- **Conmutador o SWITCH**: este dispositivo recibe datos a través de un puerto de entrada y la transmite **solo a los puertos de salida a los que va dirigida.**

- **Concentrador o HUB**: este otro dispositivo recibe datos a través de un puerto de entrada y los **transmite a todos** los puertos de salida.


HUB


- ***Punto de acceso:*** es un dispositivo que se va a conectar al router mediante cable para poder ofrecer conexión en otro lugar. Lo que hace el punto de acceso es servir como si fuera una extensión del propio router y de esta forma va a permitir que la conexión llegue a otra zona sin que haya pérdida.

- ***Repetidor:*** un repetidor o amplificador a diferencia de un punto de acceso, va a recibir la señal del router de forma inalámbrica y, posteriormente, enviarla a otros equipos. Ahí hay pérdida de señal, evidentemente.

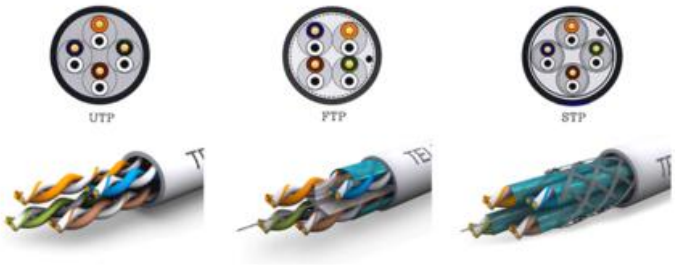

- ***Adaptador de red:*** es un componente interno de un ordenador u otro dispositivo que permite conectar nuestro equipo a la red. Hoy en día, la mayoría vienen integrados en la placa base del dispositivo. En caso contrario, se pueden instalar o bien en ranuras de expansión de nuestro equipo o bien en un puerto USB. Hay dos tipos: **Ethernet** (conexión por cable) e **inalámbricas** (conexión sin cables).


## 1.4.- MEDIOS DE CONEXIÓN

### *1.4.1.- Transmisión alámbrica*

La información se tramite por medio de cables, existen tres tipos básicos:

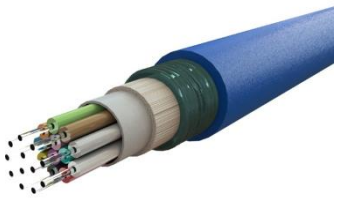
- ***Par trenzado:*** está formado por cuatro pares de hilos de cobre, que pueden estar sin apantallar (UTP) o apantallados para evitar interferencias (FTP/STP). Hay de varias categorías (que van de la 1 la 8) y a mayor categoría, mayor velocidad de transmisión de datos. Se conectan mediante un conector RJ45 similar a la clavija telefónica, pero de mayor tamaño.





- **Cable coaxial:** similar al de la antena de TV, contiene un **conductor de cobre en su interior,** envuelto por una capa aislante que lo separa de un apantallado metálico con forma de rejilla, que garantiza la resistencia a las interferencias eléctricas.

Coaxial

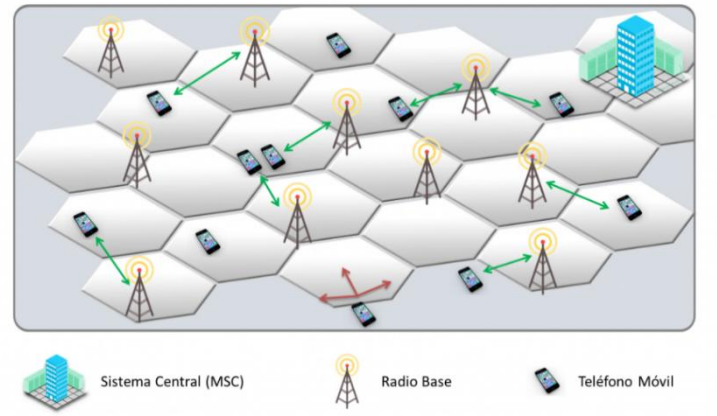


- **Fibra óptica**: está formado por **filamentos de vidrio transparentes** rodeados de varias capas de material protector. Es ideal para entornos donde hay gran cantidad de interferencias eléctricas, **transmite la señal en forma de pulsos de luz** en vez de señales eléctricas y es el que permite mayores velocidades de trasmisión.

### 1.4.2.- ***Transmisión inalámbrica***

La información se tramite por medio de ondas electromagnéticas sin necesidad de cables. Existen diferentes tecnologías, pero las más comunes son:

- ***Red de telefonía móvil (celular):*** los dispositivos móviles se conectan mediante ondas de radio con los **nodos base** (equipos electrónicos con antenas emisoras y receptoras de las señales de radio), que se distribuyen a lo largo de una determinada superficie en cuadrículas llamadas **celdas o células**, consiguiendo así, una **red de conexión** (zonas con cobertura). Actualmente se está **desplegando la red 5G** que permite ahorrar batería, conectar más dispositivos y mejorar las velocidades de conexión




- ***Wi-Fi:*** se basa en la transmisión y recepción de ondas de radio de corto alcance (100 m) en las frecuencias de 2,4 GHz o 5 GHz. Hay diferentes **estándares wifi** (conjunto de normas y protocolos de conexión) siendo la diferencia principal entre ellos la velocidad y la frecuencia de transmisión.

**ESTÁNDARES WIFI**
**IEEE 802.11**


- ***Bluetooth:*** es probablemente la tecnología inalámbrica más presente hoy en día en nuestras vidas, un estándar que **posibilita la transmisión de voz y datos** entre diferentes dispositivos (móviles, tabletas, portátiles...). Su uso más común es el de enlazar dispositivos para la función de audio. Su **rango efectivo de unos 10 metros**.



- ***Infrarrojo (IrDA):*** hoy en día sigue siendo el método de transmisión estándar implementado en los **mandos a distancia**. Debido a que las señales infrarrojas **no**

**atraviesan paredes,** su alcance dentro de la misma habitación no es superior a 15 metros. Los sensores de movimiento para seguridad del hogar funcionan también con señal infrarroja y tienen una sensibilidad de entre 1 y 5 metros.

- ***NFC***: (Near Field Communication) es una tecnología popularizada gracias a los sistemas de **pago mediante móvil.** Su punto fuerte está en la velocidad de comunicación, que es casi instantánea sin necesidad de emparejamiento previo. Como contrapartida, el alcance de la tecnología NFC es muy reducido, pues se mueve como máximo en un **rango de los 10 cm.**


### 1.5.- PROTOCOLOS DE COMUNICACIÓN

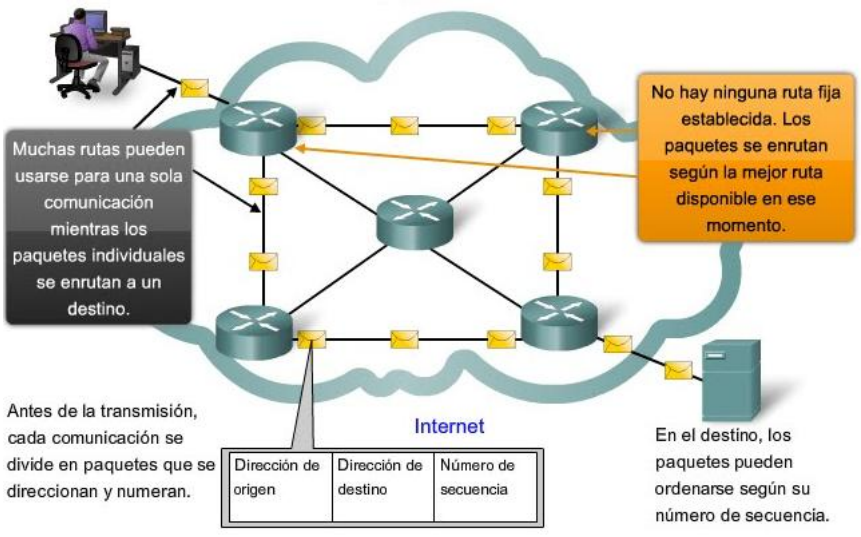
**Son las reglas y especificaciones técnicas que siguen los dispositivos conectados**. Si cada uno de ellos "hablase" de manera distinta, la comunicación se haría imposible. En las redes, la función de traducción la realizan tanto las tarjetas de red como los routers.

El protocolo más utilizado actualmente, tanto en redes locales como en Internet, es el **TCP/IP** y permite la comunicación entre los dispositivos conectados a una red independientemente del sistema operativo y del hardware que tengan.

Consta de dos protocolos:

- **TCP (*transmisión control protocol)*:** se encarga de dividir los datos a transmitir en pequeños paquetes, y a cada uno de esos paquetes se le numera y se le añade una información de control, la cual sirve para reconstruir el mensaje completo en el dispositivo de destino.

- **IP *(internet protocol):*** dirige los paquetes creados por el TCP a través de las redes necesarias e identifica los equipos de destino de dichos paquetes. Para ello emplea las llamadas direcciones IP, que identifican de manera única a todos los dispositivos conectados a una red.



- ***Dirección IP:*** cada equipo que pertenece a una red dispone un identificador único para poder saber a quién va dirigida la información en las transmisiones y quiénes son los remitentes. Este identificador se denominan **dirección IP** (Ejemplo 192.168.1.27)**.**

  Esta dirección la podemos elegir nosotros o bien, podemos configurar el router para que sea éste el que de manera automática asigne direcciones IP a todos los dispositivos que se le conecten (en este caso aparecerá en su configuración **servidor DHCP: habilitado**).

  La dirección IP puede ser pública o privada. La dirección IP pública es un número único que identifica nuestra red desde el exterior. La dirección IP privada es un número único que identifica a un dispositivo conectado en nuestra red interna, **(en nuestro caso, en el colegio utilizamos el formato llamado IPv4).**

- ***Máscara de subred:*** una red puede ser única o constar de otras subredes. La máscara de subred indica el número de ordenadores máximo que pueden estar conectados a una red o subred (existen 255 direcciones posibles en cada subred). Ejemplo 255.255.255.0

- ***Puerta de enlace predeterminada:*** es la IP del router, switch u otro elemento enrutador de la red, por lo tanto, la puerta de enlace tendrá una dirección IP única en toda la red o subred. Ejemplo: 192.168.1.1

- ***DNS:*** los servidores DNS son ordenadores en internet que convierten el texto que escribimos en la barra de direcciones en una IP y viceversa.

*Ejemplo: Supongamos que tenemos una red con una máscara 255.255.255.0, cuya dirección de router es 192.168.1.1 (puerta de enlace predeterminada). Podemos conectar a esa red teóricamente hasta 254 equipos. Como el router tiene la dirección IP 192.168.1.1, los ordenadores se podrán empezar a numerar desde el 192.168.1.2 y de ahí en adelante hasta el 192.168.1.255.*

El **comando ping (*Packet Internet Grouper*)**, se trata de una utilidad que comprueba el estado de la conexión con equipos remotos enviando paquetes de datos a una dirección de red concreta y solicitando confirmación de la recepción de manera automática. Es útil para diagnosticar errores en redes y se utiliza mediante una aplicación incluida en el sistema operativo llamada **Símbolo del sistema**.

## 2.- INTERNET

Internet es una **red mundial de redes de ordenadores (WAN),** que mediante el uso de diferentes **protocolos de comunicación y transferencia de información** permite a estos comunicarse y compartir información. No es una red "típica" de ordenadores, sino una red de redes, donde cada una de ellas es independiente y autónoma.

### 2.1.- HISTORIA DE INTERNET

Vamos a repasar una serie de hechos puntuales que han marcado la aparición y el desarrollo de Internet:

- **1969:** se realiza la **primera conexión** entre dos ordenadores remotos.
- **1971:** se envía el primer **correo electrónico**.
- **1983:** se desarrolla el **protocolo TCP/IP.**
- **1986:** aparece por primera vez el concepto **Internet** y se crea el primer **buscador**.
- **1989**: se crea el leguaje **HTML** y nace el sistema World Wide Web (**www**)
- **1993:** se desarrolla el **primer navegador gráfico** de Internet.
- **1998:** nace **Google**
- **2003:** surgen las **primeras redes sociales** modernas
- **2004:** se desarrolla el concepto de **Web 2.0** y nace **Facebook**
- **2005: nace YouTube y se lanza Twitter**
- **2007: se lanza el primer iPhone**
- **2010: se lanza Instagram**
- **2015: Internet alcanza más de 3.000 millones de usuarios**
- **2016: ….**

### 2.2.- COMUNICACIÓN POR INTERNET

Para poder comunicarnos por Internet, se utilizan programas que se denominan **navegadores**. Los **navegadores** son **aplicaciones que nos permiten visualizar las páginas web** mediante la **dirección URL.** Estas, están formadas por el nombre del **protocolo de transmisión**, seguidos del **nombre del dominio** donde se aloja el recurso que buscamos.

No confundir un navegador (Chrome, Firefox, Safari, Edge, Opera, etc.), con un buscador (Google, Bing, DuckDuckGo, Yahoo, etc.). Los **buscadores** son programas que **localizan páginas web con la información que buscamos**.

Google

bing

DuckDuckGo

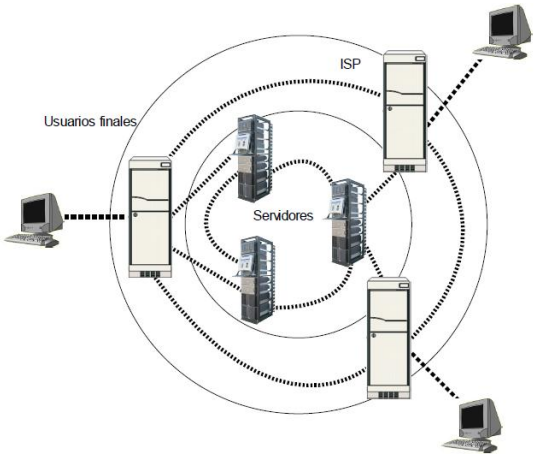
YAHOO!

Resumiendo, nosotros **usamos un navegador para poder acceder a Internet** (Chrome por ejemplo), y una vez que tenemos ese acceso, **buscamos la información que queremos usando un buscador** (Google por ejemplo), que localiza las páginas web que contiene la información que nos interesa y que abrimos y visualizamos usando el navegador.

### *2.2.1.- Funcionamiento de Internet*

La Web funciona siguiendo un modelo **cliente-servidor**. Existe un servidor, que es quien presta el servicio (contiene la información que se solicita), y un cliente, que es quien solicita la información y la recibe.

El **cliente** normalmente es un navegador y el **servidor** es un programa que está permanentemente escuchando las peticiones de los clientes. Si encuentra en su sistema de archivos el documento solicitado por el cliente, lo envía y cierra la conexión, si no, envía un mensaje de error típico, como “No es posible encontrar la página” o “Documento no encontrado”.




Localizados entre los servidores y los clientes están las **ISP** (Internet Service Provider), es decir las empresas que ofrecen el servicio de acceso a Internet mediante la conexión a sus equipos.

### *2.2.2.- Protocolo de comunicación*

Como hemos visto anteriormente, el **protocolo de comunicación** más utilizado tanto en redes locales como en Internet es el llamado **TCP/IP**. La **dirección IP** de un dispositivo es un identificador único para poder saber a quién va dirigida la información en las transmisiones y quiénes son los remitentes.

La información digital que se envía es "cortada" en paquetes de datos que llevan etiquetadas las **direcciones IP del dispositivo remitente y del destinatario** y como hemos visto anteriormente, el Router se encargan de dirigir esos paquetes de datos de manera correcta.

### *2.2.3.- Protocolo de transmisión*

Las direcciones URL normalmente comienzan por **http:// o https://.** Estas siglas definen el protocolo para la **transmisión de información de las páginas de web (el protocolo https** es un protocolo de comunicación cifrado de extremo a extremo y es seguro). Se basa en un mecanismo sencillo de solicitud y respuesta. El cliente, normalmente un navegador, envía una solicitud a un servidor y este le envía una respuesta.

### *2.2.4.- Los dominios de Internet*

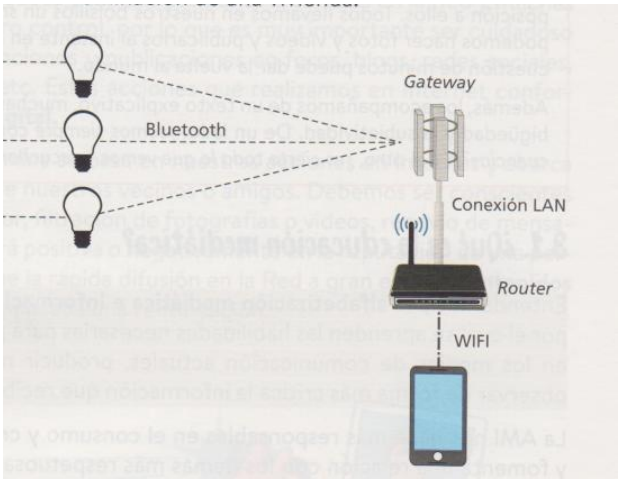
Acceder a los diferentes servicios de Internet mediante la dirección IP sería prácticamente imposible. Para traducir estas direcciones IP a texto aparece el concepto de dominio**. Un dominio es una cadena de texto que equivale a una dirección IP.** Los dominios están formados por dos partes, la primera llamada **dominio de segundo nivel** es el nombre del servicio (por ejemplo, google), la segunda llamada **dominio de primer nivel** es un código de dos o tres letras que indican el ámbito en el que se enmarca la información que contienen.

https://www.cruzroja.org

En este ejemplo, **https://** es el protocolo de transmisión empleado, **www.cruzroja** sería el dominio de segundo nivel y **.org** el dominio de primer nivel. Este último puede ser muy variado, los más comunes son .com (organización comercial), .edu (institución educativa), .org (organización sin ánimo de lucro) .es (España), etc…

## 2.3.- INTERNET DE LAS COSAS: IOT


Hoy en día una cantidad enorme de dispositivos están conectados a Internet y no sólo ordenadores o smartphones, sino también objetos tan diversos como relojes o pulseras inteligentes (**wearables**), sensores de presencia, termostatos de sistemas de calefacción o de aire acondicionado, bombillas, cámaras de




vídeovigilancia, automóviles, electrodomésticos, ropa, etc. Este concepto de objetos conectados se ha popularizado con el nombre de **Internet de las cosas** (Internet of things; IoT).

Normalmente, muchos de estos objetos suelen funcionar con baterías, por lo que para que su consumo eléctrico sea bajo, se conectan por Bluetooth (su consumo energético es mucho menor que Wifi) a un aparato llamado "Gateway" que hace de pasarela o intermediario, y es este el que se conecta mediante Wifi o LAN al router que es el que da el acceso a Internet.

## 3.- SEGURIDAD

Entendemos por **seguridad informática** al conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de **confidencialidad** (impide el acceso a datos a usuarios no autorizados)**, integridad** ((impide la modificación de los datos almacenado**s) y disponibilidad** (permitir al usuario autorizado acceder a los datos con facilidad).

En este apartado vamos revisar de manera breve una serie de consejos, herramientas y dispositivos que nos permitiran usar de manera segura nuestros equipos informaticos.

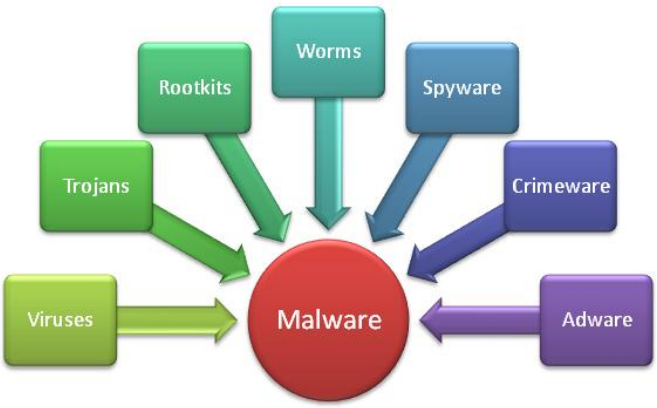
### 3.1.- SEGURIDAD DEL HARDWARE


Para mejorar la protección de nuestro equipo físicamente frente a averías o accidentes eléctricos, como por ejemplo sobrecargas o cortocircuitos, es conveniente seguir estos consejos:

- Usar regletas específicas para ordenador con protección frente a sobretensiones y que soporte la potencia máxima que va a necesitar el sistema.
- Usar enchufes que tengan toma de tierra y evitar sobrecargarlos con muchas conexiones.
- Apagar siempre el ordenador usando el botón de inicio/apagado, nunca desconectándolo directamente del enchufe.

## 3.2.- SEGURIDAD DE LOS DATOS

La conexión en red de un equipo ofrece muchas ventajas, pero también implica una serie de amenazas. Nuestro equipo puede verse atacado deliberadamente desde el exterior por diferentes tipos de **malware** (ramsonware, spyware, troyanos, adware, gusanos, bots, etc.) cuyo objetivo final suele ser o **modificar y dañar archivos del sistema** u **obtener información con algún fin, generalmente económico**.




### *3.2.1.- Medidas preventivas*

Algunas **medidas preventivas** que se deben tener en cuenta son: **no hacer clic en enlaces dudosos, no aceptar desconocidos en nuestros contactos, no usar siempre la misma contraseña y las contraseñas que se usen deberían cambiarse de manera periódica mezclando números, letras y caracteres especiales, no publicar datos personales de manera pública, no subir fotos comprometedoras y denunciar cuando veamos un posible delito.**

### *3.2.2.- Seguridad pasiva*

Su fin es **minimizar los efectos causados** por un ataque de malware. Las principales medidas de seguridad pasiva se resumen en **hacer copia de seguridad** de nuestros datos y disco de sistema de manera periódica y en el uso de **puntos de restauración** que crea el propio sistema operativo, para restaurar el sistema a un estado anterior al ataque.

### *3.2.3.- Seguridad activa*

Su fin es **proteger y evitar** posibles ataques de malware. Las principales medidas de seguridad activa son uso de **cortafuegos** (permite o prohíbe la comunicación con la red), **antivirus** (detecta software peligroso y lo elimina**), antispam** (filtro que detecta correo basura) y **antiespías** (detecta y elimina programas de recopilación de información).

## 3.3.- SEGURIDAD DE LAS REDES

La seguridad de las redes, ya sean inalámbricas o cableadas, para evitar que intrusos puedan acceder a nuestra conexión es de vital importancia. No solo podría afectar a la velocidad de Internet, sino que también peligraría el buen funcionamiento de los dispositivos conectados y lo que es más importante, todo el contenido personal que tenemos almacenado en ellos. A continuación, se describen una serie de recomendaciones y acciones a llevar a cabo para mejorar la seguridad de nuestras conexiones:

### *3.3.1.- Proteger el acceso al router*

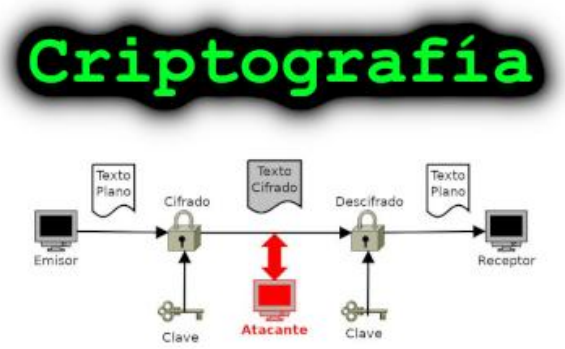
Cuando adquirimos **un router nuevo,** normalmente viene configurado con contraseñas de acceso predeterminadas que los hackers conocen si saben el fabricante. Por lo tanto, **cambiar la contraseña predeterminada de acceso al router** contribuye a proteger nuestra red doméstica. También es importante **cambiar la contraseña de acceso a la red Wi-Fi** que viene por defecto.

### *3.3.2.- Modificar el nombre de la red wifi o (SSID)*

Es muy recomendable **cambiar el nombre de nuestra red Wi-Fi** que emite el **router nuevo por defecto** para que no incluya ningún tipo de información que pudiera ser de utilidad para un potencial atacante (proveedor de servicios contratado, modelo de router, etc.).

### *3.3.3.- Usar criptografía*

La criptografía se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para cifrar la información y así protegerla y dotar de seguridad a las comunicaciones y a las entidades que se comunican. Ejemplos de métodos criptográficos son: la firma digital, mensajes de correo encriptados, protocolos seguros como TLS, HTTPS, WPA2, etc.




### *3.3.4.- Desactivar la función WPS*

Muchos routers modernos traen la función WPS incorporada. Se trata de un mecanismo que facilita la conexión de dispositivos con nuestro router a través de un código PIN de 8 dígitos. El dispositivo que se quiere conectar a la wifi debe transmitir el código numérico al router y éste a cambio le enviará los datos para acceder a la red. Tener activada esta opción implica una vulnerabilidad que podría ser utilizada por un atacante para acceder a nuestra red Wi-Fi, ya que el tiempo que se necesita para averiguar un PIN de 8 dígitos es mucho menor que el que necesitaría para averiguar una contraseña WPA3.

### *3.3.5.- Activar el cifrado Wi-Fi (WEP, WPA, WPA2 y WPA3)*

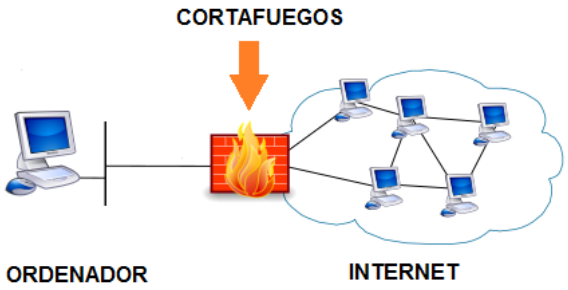
Son sistemas de cifrado para proteger el acceso a las redes inalámbricas. El primero en crearse fue WEP, es sencillo de romper y apenas se usa. El segundo WPA, fue creado para corregir las deficiencias del sistema previo, aunque hoy en día también es vulnerable. Posteriormente WPA2 fue creado para corregir las deficiencias WPA, utiliza algoritmos de cifrado que dan mayor seguridad a la red. Actualmente los routers más modernos incorporan WPA3 que es el sistema de cifrado más seguro.

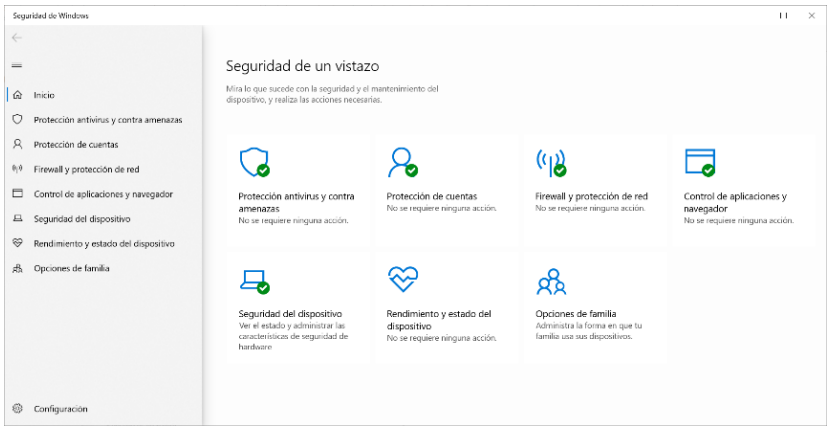
### *3.3.6.- Usar filtrado MAC*

Una dirección MAC es el identificador único asignado por el fabricante a una pieza de hardware, es algo equivalente al DNI de cada dispositivo. El filtrado MAC consiste en dar instrucciones al router para que permita conectarse a los dispositivos cuya MAC aparezca en un listado. Cualquier otro terminal cuyo identificador de red no se encuentre en esta lista no podrá acceder.

### *3.3.7.- Usar cortafuegos (Firewall)*

Es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar y descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware, software o una combinación de ambos.




➢ ***Usar antivirus:*** como ya vimos en la UD 1, Windows 10 proporciona una **protección antivirus** bastante efectiva mediante el Centro de Seguridad que ayuda activamente a proteger tu dispositivo mediante la detección de malware (software malintencionado), virus y otras amenazas de seguridad.

## 3.4.- SEGURIDAD EN INTERNET

### *3.4.1.- Usar contraseñas seguras*

Una contraseña segura contiene al menos 12 caracteres y suele ser una combinación aleatoria de números, símbolos y letras mayúsculas y minúsculas. Además, es recomendable cambiar la contraseña de manera periódica, por ejemplo, cada seis meses, no usarla para diferentes servicios y evitar que esté relacionada con fechas o nombres que puedan ser asociados contigo.

### 3.4.2.- Usar encriptación de archivos

La información que viaje por Internet pasa por un número indeterminado de servidores en los que puede haber algún programa espía con el fin de hacer uso de dicha información. Para evitar ese peligro, cuando la información enviada es sensible o importante, debe de ser ocultada o encriptada.

Para encriptar información y protegerla, se utilizan algoritmos criptográficos basados en una clave secreta. Estos algoritmos toman un texto y mediante una clave de cifrado, lo modifican dejándolo incomprensible. Este texto cifrado solo puede ser descifrado por el receptor si tiene la clave de descifrado.

### 3.4.3.- Usar la identidad digital

Uno de los problemas de la navegación por Internet es poderse identificar y poder ser identificado de manera inequívoca y segura, con el fin de evitar accesos no permitidos y dejar acceder tan solo al servicio si el usuario identificado de manera correcta. Para poder asegurar que somos quienes decimos ser, existen varios tipos diferentes de sistemas, los principales son los siguientes:

#### 3.4.3.1.- Firma electrónica

Es un equivalente digital de la firma manuscrita. Mediante ella podemos dar por válido un documento electrónico, su falsificación es prácticamente imposible y sólo puede ser usada por mayores de edad.

#### 3.4.3.2.- Certificado digital


Este certificado nos identifica de manera segura e inequívoca tanto ante organismos públicos y ante empresas o para firmar documentos electrónicamente. Para obtenerlo debemos ser mayores de edad (o menores emancipados) y hay que solicitarlo a entidades certificadoras como la **Fábrica Nacional de Moneda y Timbre (FNMT)**. Con él, podemos realizar gestiones de manera telemática en la administración pública o acceder de manera segura a cuentas bancarias u otros servicios privados. Se trata de una serie de archivos electrónicos que hay que solicitar presencialmente con el DNI (y renovar cada 4 años) y que son enviados por correo electrónico a la persona solicitante, la cual deberá instalarlos en los dispositivos electrónicos en los que quiera utilizarlos.

### *3.4.3.3.- DNI electrónico*


El DNI electrónico conocido también como **DNIe**, incorpora un microchip que contiene un certificado digital protegido por contraseña, que nos identifica inequívocamente y que puede ser usado por mayores de edad o menores emancipados para conectarse con la Administración o empresas privadas de forma digital o firmar documentos electrónicamente.

Desde 2015 se expide el nuevo DNIe, denominado **DNI 3.0** que cuenta con un microchip con interfaz dual que permite la conexión mediante hardware (lector de tarjetas), pero también de forma inalámbrica a través de la tecnología NFC. Además, este nuevo DNI 3.0 incorpora también información referente al carnet de conducir y a la tarjeta sanitaria.

### *3.4.3.4.- El sistema Cl@ve*

Este sistema está pensado específicamente para realizar trámites electrónicos con la administración pública. Funcina mediante un sistema de usuario y contraseña con autentificación a través de mensajes SMS en el móvil y su uso es más sencillo que el certificado digital. Entre otras cosas, sirve para presentar la declaración de la renta, consultar información clínica, descargar la vida laboral, acceder al carnet de conducir digital o firmar documentos electrónicamente.

cl@ve
IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES