

Redes de comunicación

Trabajo realizado por:

- **Alejandro Argüelles Rodríguez**
- **Brian Balayo Atanes**
- **José Luis Ares Sainz**

ASIGNATURA: TIC

PROFESOR: Ángel Acción Lamas

**ESTUDIOS DE BACHILLERATO
IES.EDUARDO BLANCO AMOR
A CORUÑA- 2016**

ÍNDICE

Las redes de comunicación

Fundamentos de las redes

Proceso de comunicación.

Redes de ordenadores.

Origen de las redes y modelos de referencia

Modelos de referencia OSI.

Capa física (Nivel 1).

Capa Enlace de Datos (Nivel 2).

Capa de Red (Nivel 3).

Capa de Transporte (Nivel 4).

Capa de Sesión (Nivel 5).

Capa de Presentacion (Nivel 6).

Capa de Aplicación (Nivel 7).

Familia de protocolos de Internet: TCP/IP

Protocolo IP

Direcciones IP.

Direcciones IPv4.

Direcciones IPv6.

IP estática

IP dinámica

Direcciones públicas

Direcciones privadas

Subredes.

Puertas de enlace o Gateway.

USROBOTICS. Recuperado de <http://support.usr.com/support/9113/9113-es-ug/install.html>

DNS.

Dirección MAC.

Tipos de redes

Según su área de cobertura.

Según su tipología.

Bus

Anillo

Estrella

Árbol

Híbrida

Según su nivel de acceso o privacidad

Red pública

Red privada

VPN

Según su relación funcional

Cliente-servidor

Redes entre iguales P2P.

Según su tecnología física de conexión.

Redes cableadas o guiadas.

Fast Ethernet o 100BASE-T.

Gigabit Ethernet o 1000BASE-T.

10 Gigabit Ethernet.

Redes inalámbricas o no guiadas.

Wi-Fi (Wireless Fidelity).

Bluetooth.

Infrarrojo.

La red Internet

Orígenes de Internet.

Servicios de Internet

La web.

La evolución de la web

Web 1.0 o web estática.

Web 2.0 o web social

Web 3.0 o web semántica

Tecnologías de acceso a internet

Acceso cableado.

Acceso inalámbrico.

Acceso móvil.

Línea telefónica.

RTC (Red de Telefonía Conmutada).

RDSI (Red Digital de Servicios Integrados)

ADSL (Línea de Abonado Digital Asimétrica)

Cable o HFC

Fibra óptica hasta el hogar

Internet por satélite

WIMAX y LMDS

Red eléctrica.

Conexión por telefonía móvil.

Primera generación, 1G

Segunda generación, 2G

Tercera generación, 3G

Cuarta generación, 4G

Seguridad en la red

Legislación en la red

LOPD

LPI

LSSI-CE

LAECSP

Ley de firma electrónica

Adopción de medidas de seguridad

Protección

Antivirus

Cortafuegos

Recuperación

Copias de seguridad

Información en la nube

SAN

Conexiones seguras y cifradas.

DNIe

Certificados digitales.

HTTPS.

Certificado electrónico.

Configuración segura del navegador.

Navegación privada.

Filtro contra la suplantación de identidad, Phishing.

Confidencialidad.

Autenticación.

Integridad.

Disponibilidad.

Amenazas a la seguridad.

Causas humanas.

Causas lógicas.

Causas físicas.

Las redes de comunicación

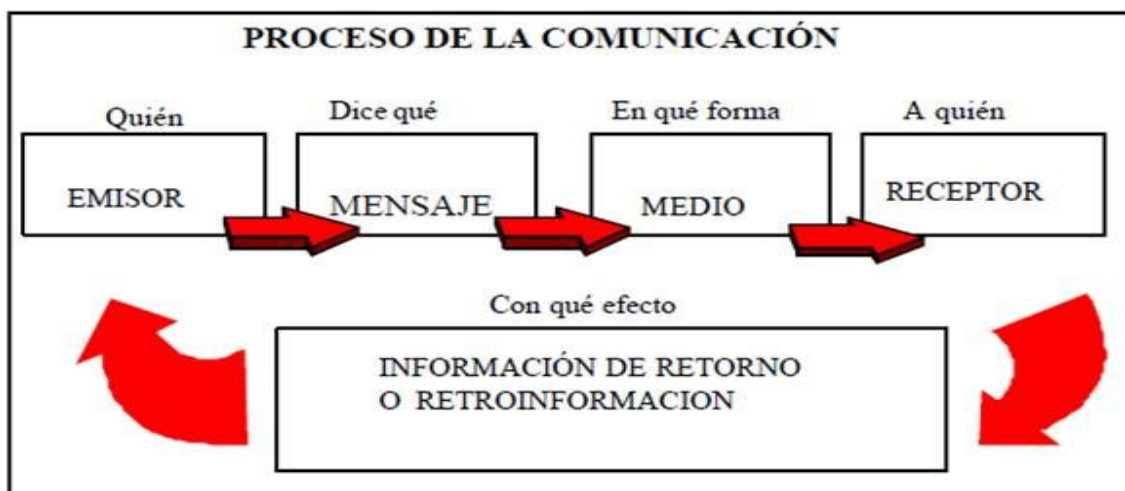
Una red de comunicación es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían impulsos electromagnéticos con el fin de compartir datos, recursos y ofrecer servicios.

Fundamentos de las redes

Actualmente las redes de comunicación facilitan los procesos de transiciones y colaborativos, por eso es fundamental conocer las tecnologías que nos permiten llevar a cabo estos procesos de forma rápida. Así mismo en pleno siglo XXI se puede decir que vivimos en un mundo globalizado en la que la transmisión de datos es instantánea lo que facilita y agiliza investigaciones científicas, propagación de información... Todo esto se debe al desarrollo tecnológico que se ha llevado a cabo durante los últimos años; Internet como la gran herramienta, nuevas redes de ordenadores presentes en todos los rincones de nuestra sociedad, etc.

Proceso de comunicación.

Desde el principio de nuestros tiempos el hombre ha desarrollado el proceso de comunicación como algo esencial, hasta el punto de que hoy en día podamos comunicarnos entre nosotros separados por grandes distancias. En todo proceso de comunicación (tanto en persona como a través de dispositivos) se necesitan los siguientes elementos.



Díaz Cabanillas, Cintia Marilu. Monografías. Recuperado de <http://www.monografias.com/trabajos82/proceso-comunicacion-organizacional/proceso-comunicacion-organizacional2.shtml>

En una red los dispositivos funcionan como receptores y emisores a la vez, el canal (o medio) es el gracias a lo que circula la información transmitida (cables, fibra óptica, ondas, etc).

Para que emisor y receptor se entiendan se utiliza una serie de normas comunes, en las redes se suelen emplear los protocolos TCP/IP.

Redes de ordenadores.

Una red de ordenadores no es más que un conjunto de estos dispositivos que se comunican entre sí a través de una cantidad de elementos que conforman un sistema de transmisión con una serie de propósitos específicos. Estas redes se constituyen principalmente para llevar a cabo los siguientes objetivos

- Uso compartido de recursos: Este es el objetivo principal pues las redes nos permiten acceder a archivos que no se encuentran en nuestros dispositivos, controlar de forma remota dispositivos a distancia (impresoras, otros ordenadores mediante softwares)
- Comunicaciones entre los equipos que integran la red: Hoy en día existen programas que nos permiten llevar a cabo intercambio de mensajes por vía escrita u oral ([Skype](#), [Team Speak](#)., [WhatsApp](#), etc)
- Simplificación en la gestión de los sistemas de trabajo: Las redes de ordenadores nos permiten mayor agilidad en la búsqueda de información fiable así como también las aumentan las posibilidades de trabajo,
- Aumentar la capacidades de procesamiento: Esto es un concepto claro de globalización pues se nos permite trabajar a nivel mundial en un mismo proyecto, esto agiliza enormemente el trabajo pues se produce una colaboración a gran escala.



Origen de las redes y modelos de referencia

Las redes de comunicación nacen en los orígenes de la humanidad en el momento en el que el primer ser humano se comunica con otro, las redes sociales han ido evolucionando a lo largo del tiempo desde el inicio cuando las redes se limitaban a pequeñas tribus hasta la actualidad donde estamos en un mundo globalizado donde una persona es capaz de comunicarse con otra aunque estén a miles de kilómetros una de otra. También han cambiado los mecanismos que usamos para comunicarnos, desde las señales de humo, las cartas, el teléfono móvil hasta la actualidad donde la reina de las redes de comunicación es Internet.

Modelos de referencia OSI.

A finales del siglo XX con la aparición de nuevas redes de comunicación muchas empresas empezaron a tener problemas para transmitir la información ya que aparecieron redes con distintas especificaciones que tenían problemas para intercambiar datos.

Para solucionar este problema, la [ISO](#) investigó distintos modelos de conexión con el fin de encontrar un conjunto de normas que se pudiera aplicar a todas las redes, en base a esta investigación la ISO creó un modelo de red que permite a los fabricantes crear redes que sean compatibles entre sí.

Las diferentes capas de este modelo son:

- ***Capa física (Nivel 1).***

Esta capa hace referencia a las transformaciones que se le hacen a una secuencia de bits para transmitirlos de un lugar a otro.

Además, esta capa proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar conexiones físicas tales como cables etc...

- ***Capa Enlace de Datos (Nivel 2).***

Es la capa que se encarga de realizar una transmisión de información fiable. Utiliza los servicios de la capa física y recibe peticiones de la capa de red. Su objetivo es que la información fluya libre de errores entre dos dispositivos que están conectados entre sí, para ello monta bloques de información, los dota de una dirección MAC y se encarga de que un ordenador más potente no sobrepase a uno más lento.

- ***Capa de Red (Nivel 3).***

Esta capa proporciona conectividad entre dos sistemas que pueden estar situados en redes alejadas una de otra. La función de esta capa es hacer que los datos lleguen desde su origen a su destino. Esta capa utiliza las funciones de la capa de enlace y a su vez le proporciona servicios a la capa de transporte.

- ***Capa de Transporte (Nivel 4).***

Su función es proporcionar un transporte de datos confiable y económico del dispositivo de origen al dispositivo destino.

- ***Capa de Sesión (Nivel 5).***

Proporciona los mecanismos para controlar el diálogo entre las aplicaciones de los sistemas finales. Algunos de los servicios que puede proporcionar esta capa son :

- Control de diálogo: Puede ser del tipo full-duplex (Pueden transmitir los dos sistemas a la vez) o semi-duplex (solo puede transmitir uno de los dos a la vez, por lo que se van alternando)
- Agrupamiento : El flujo de datos se puede marcar para definir un grupo de datos.
- Recuperación : Puede establecer un procedimiento de puntos de comprobación por lo que en caso de ocurrir un error entre alguno de estos puntos la entidad de sesión puede transmitir la información desde el último punto de comprobación.

- ***Capa de Presentación (Nivel 6).***

Esta capa se encarga de la representación de datos de manera que aunque dos equipos puedan tener diferentes sistemas de representación internos la capa de presentación se encarga de que sean reconocibles para los dos equipos. Además, esta capa también nos permite el cifrado de datos y la compresión de datos.

- ***Capa de Aplicación (Nivel 7).***

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos

Familia de protocolos de Internet: TCP/IP

La familia de protocolos de Internet es un conjunto de protocolos en los que se basa Internet y que permite la transmisión de datos entre dos dispositivos. Los dos protocolos más importantes que componen esta familia son el protocolo TCP (Protocolo de Control de Transmisión) y el protocolo IP (Protocolo de Internet) ya que son lo más utilizados y los primeros que se definieron, pero hay muchos más tales como el HTTP (HyperText Transfer Protocol) que es el que utilizamos para buscar páginas web o el ARP (Address Resolution Protocol) que utilizamos para resolver direcciones.

El TCP/IP sirve para enlazar dispositivos que utilizan sistemas operativos distintos ya sea sobre redes de área local (LAN) o de área extensa (WAN). El modelo OSI se creó como una aproximación teórica al modelo TCP/IP que es el que realmente se usa, ambos modelos utilizan los mismos principios pero en el OSI es más fácil de entender, la diferencia principal entre estos modelos es que en el modelo TCP/IP las capas de aplicación, presentación y sesión del modelo OSI se agrupan en una sola en el modelo TCP/IP que sería la capa de aplicación.

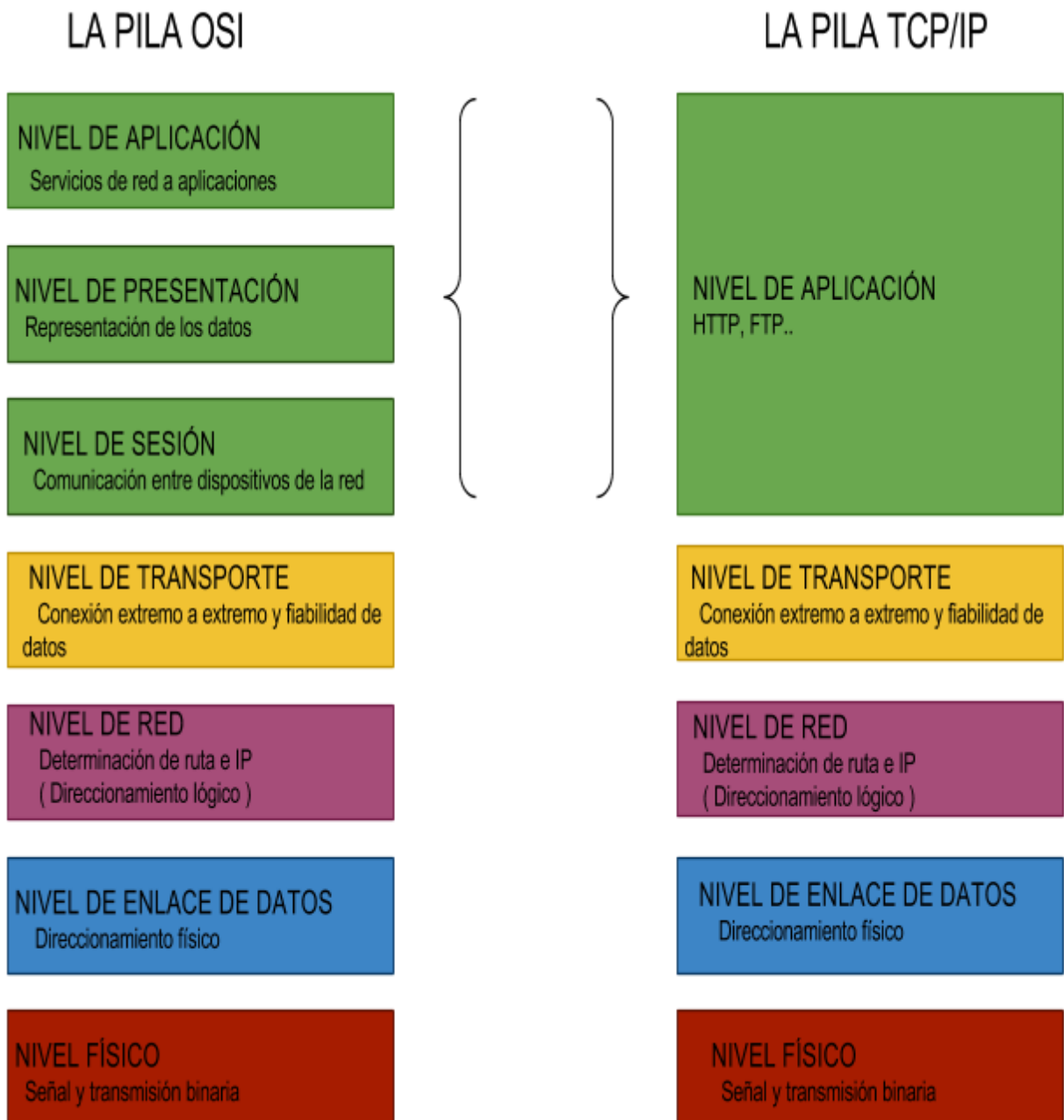


Imagen realizada por José Luis Ares Sainz.

Protocolo IP

Internet Protocol es un protocolo de comunicación de datos digitales clasificado fundamentalmente en la capa de red según el modelo internacional OSI que se ha convertido en el estándar más utilizado en redes.

Direcciones IP.

Una dirección IP es un número que identifica a un elemento de comunicación en red de un dispositivo que utilice un protocolo IP, Que corresponde al nivel de red del modelo IP. Hay diferentes direcciones de IP.

Direcciones IPv4.

Las direcciones IPv4 se expresan por un número binario de 32 bits, se pueden expresar como números de notación decimal: Se dividen los 32 bits de la dirección en 4 octetos.

Direcciones IPv6.

Tiene la misma función que los anteriores , pero se diferencia en que esta está compuesta por 128 bits y se expresa en una notación hexadecimal de 32 dígitos.

IP estática

Es una dirección IP asignada por el usuario de forma manual, o por el servidor de la red con base en la dirección MAC del cliente

IP dinámica

Es una dirección asignada mediante un servidor DHCP (Dynamic Host Configuration Protocol) al usuario.

Direcciones públicas

Las direcciones públicas son direcciones que se asignan a todos los dispositivos que conectan a Internet o a cualquier otra red pública.

Direcciones privadas

Las IP privadas son las que se asignan dentro de una red local.

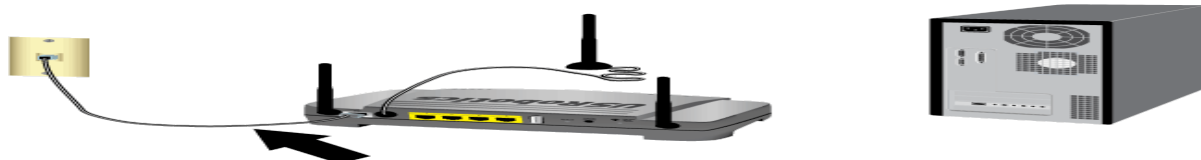
Podríamos comparar las direcciones públicas y privadas con una empresa donde tengan un número de teléfono para las comunicaciones exteriores a la empresa (IP pública) y otro para las comunicaciones dentro de la propia empresa (IP privada).

Subredes.

Las subredes son un método para maximizar el espacio de direcciones IPv4 de 32 bits y reducir el tamaño de las tablas de enrutamiento, esto permite tener más redes.

Puertas de enlace o Gateway.

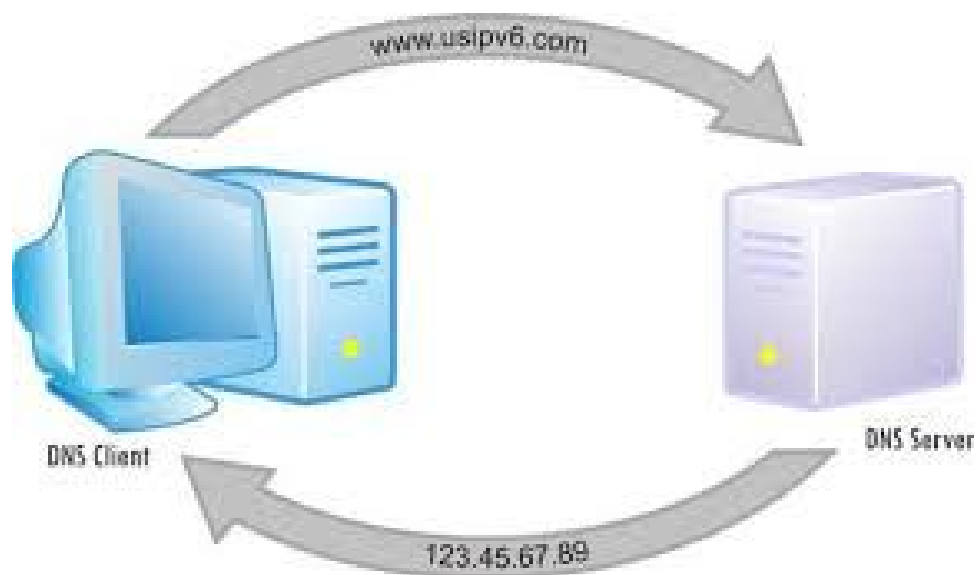
Un Gateway (puerta de enlace) es un dispositivo, por lo general un ordenador, cuya función es interconectar redes con arquitecturas y protocolos diferentes. Por lo tanto su propósito se basa en traducir la información utilizada en una red al protocolo utilizado en la red destino. A nivel doméstico la Puerta de enlace más conocida es el router, ya que este enlaza sistemas de protocolos diferentes a Internet.



USROBOTICS. Recuperado de <http://support.usr.com/support/9113/9113-es-ug/install.html>

DNS.

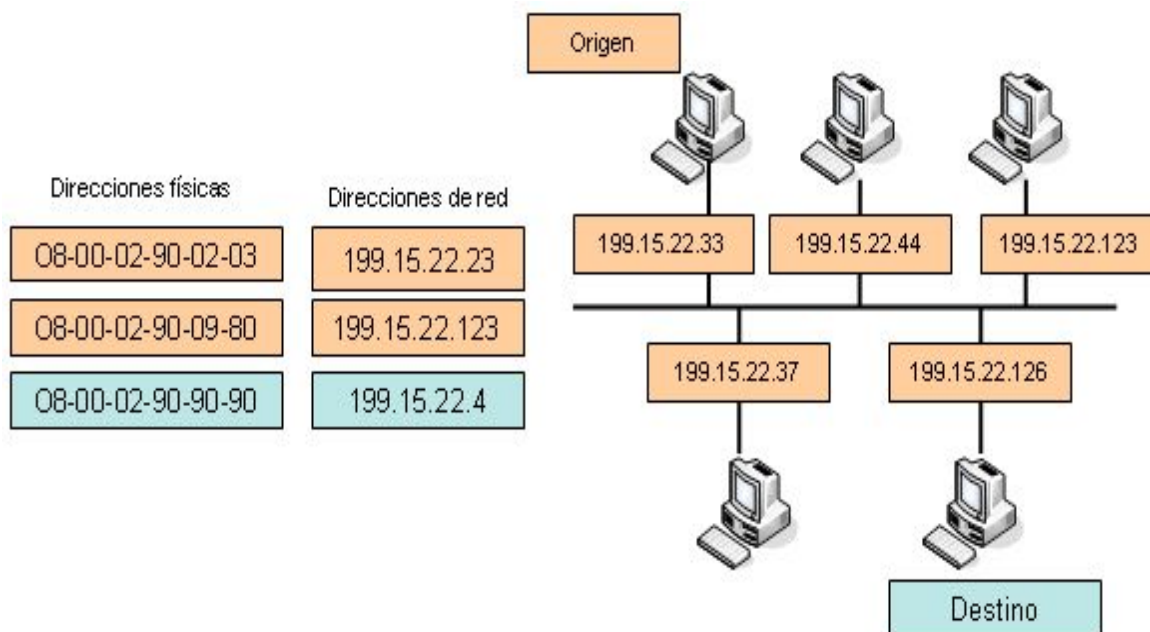
Cuando del Sistema de Nombres de Dominio (DNS, Domain Name Server) nos referimos a la asignación de un nombre a una dirección IP, de tal forma que se simplifica el modo de acceder a un servidor y también que lo recordemos más fácilmente. Un ejemplo claro de esto sería el siguiente, en el caso de querer entrar a google y no existiese un dominio asignado a este (<https://www.google.es/>) tendríamos que entrar a este escribiendo su dirección IP (un serie de números que en este caso corresponden a 64.233.187.99).



geekland. Recuperado de <http://geekland.eu/elegir-el-mejor-servidor-dns/>

Dirección MAC.

La dirección MAC es una dirección física (también llamada dirección hardware) porque identifica físicamente un elemento del hardware (móviles, ordenadores). Se trata de un identificador único de 6 bytes que asignan los fabricantes a las tarjetas y dispositivos de red. Los primeros 6 dígitos hacen referencia al OUI (Identificador Único de Organización, por lo que son iguales para todos los productos de un mismo fabricante. Ejemplo de dirección MAC 2C:3F:32:AC:5F:B2.



Tipos de redes

Las redes se pueden clasificar atendiendo a diversos criterios, tales como su área de cobertura, topología, tecnología, funcionalidad, etc.

Según su área de cobertura.

La más extensa se utiliza la WAN y es una red de ordenadores que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

Para áreas metropolitanas la MAN es una red de alta velocidad que da cobertura en un área geográfica extensa, proporcionando capacidad de integración de múltiples servicios mediante la transmisión de datos, voz, vídeos.

Red de área local se llama LAN es una red de ordenadores que abarca un área reducida, una casa, un edificio.

Red de área personal la PAN es una red de ordenadores para la comunicación entre distintos dispositivos cercanos al punto de acceso sería lo que nosotros llamamos WIFI.

Según su tipología.

- ***Bus***

Aquella topología que se caracteriza por tener el mismo canal de comunicación, al cual se conectan diferentes dispositivos. De esta forma los dispositivos comparten el mismo canal para comunicarse entre sí.

- ***Anillo***

En esta tipología cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un transmisor y un receptor que hacen la acción de traductor, pasando la señal a la siguiente estación.

- ***Estrella***

Es una red de computadoras que están conectadas directamente a un punto central y todas las comunicaciones se hacen a través de ese punto.

- ***Árbol***

Se llama así porque tiene forma de árbol, no tiene un nodo central pero tiene un nodo de enlace troncal, normalmente ocupado por un hub o switch.

- ***Híbrida***

Es la más frecuente, se deriva de la unión de varias topologías, por ejemplo: bus-estrella.

Según su nivel de acceso o privacidad

El ser una red pública o privada no se refiere a quien es propietario de la red, sino a la disponibilidad de los servicios que ofrece la red.

- Red pública

Estas redes brindan servicios de telecomunicaciones a cualquiera que pague una cuota ya sea una persona, empresa, universidad etc... Con el término público se refiere a que la disponibilidad del servicio ofrecido es para todos en general.

- Red privada

Este tipo de redes son administradas por una organización en particular. Los usuarios suelen ser personal de esa organización aunque el propietario puede darle acceso a cualquier otro que no pertenezca a la organización.

- VPN

Una conexión VPN permite crear una red local si la necesidad de que los usuarios estén conectados entre sí físicamente sino a través de Internet. Normalmente al conectarte a Internet tu dispositivo se pone en contacto con el proveedor de Internet que conecta los servicios web para que tu puedas acceder al contenido que quieras ver, esto con una conexión VPN cambia, todo empieza igual, el dispositivo se pone en contacto con el proveedor, pero desde ahí va directo al servidor VPN desde donde se dirige a su destino, la red está cifrada por lo que tu proveedor de Internet no puede saber a qué estás accediendo.

Un ejemplo práctico de uso de esta red sería el trabajador de una empresa para trabajar desde casa.

Según su relación funcional

- *Cliente-servidor*

Muchas de las aplicaciones que utilizamos se desenvuelve en un entorno cliente-servidor esto es que los equipos que forman parte de una red se conectan a un servidor que es un equipo muy potente con gran capacidad de entrada/salida que le proporciona servicios que a su vez proporcionan datos como la hora, archivos etc...

Los servicios los utilizan programas cliente que se ejecutan en los distintos equipos, la función de estos programas es procesar los datos recibidos del servidor.

Algunas de sus ventajas son:

- Recursos centralizados: Se pueden administrar los recursos desde un solo punto que es común a todos los usuarios.
- Red escalable: Se pueden agregar o eliminar usuarios del servidor sin que afecte a su funcionamiento.

Algunas de sus desventajas son:

- Coste elevado
- Un eslabón débil: Toda la red está construida en torno al servidor por lo que si deja de funcionar el servidor la red queda inutilizada.

Según su tecnología física de conexión.

Según su tecnología física de conexión podemos diferenciar entre redes cableadas (también llamadas redes guiadas) y redes inalámbricas (también llamadas redes no guiadas) cuya principal diferencia se encuentra en la disposición física de los equipos y la tecnología que utilizan para la conexión.

Redes cableadas o guiadas.

Este tipo de redes suponen una gran ventaja a la hora de subir a la red cantidades de datos a velocidades altas. La conexión entre los ordenadores y los dispositivos de red (routers, switches, etc) se realiza mediante cables, cuando conectamos un ordenador y un periférico (como una impresora) también estamos empleando una red cableada. La red alámbrica más extendida para la conexión a la red es el Ethernet, este cable utiliza una topología en forma de estrella y diferencia entre varios tipos de redes, según su velocidad.

- *Fast Ethernet o 100BASE-T.*

Su tasa de transferencia de datos es de 100 Mbps.

- *Gigabit Ethernet o 1000BASE-T.*

Su tasa de transferencia es de 1Gbps (lo que corresponde a 1000 Mbps)

- *10 Gigabit Ethernet.*

Se utiliza para redes troncales en aplicaciones que necesitan tasas de transferencia de datos muy altas, hasta 10 Gbps.

El cableado empleado en estas redes suele ser par trenzado (UTP, STP o FTP) y fibra óptica cuando se requiere de mayor velocidad.

Redes inalámbricas o no guiadas.

Se refiere a la [interconexión](#) entre distintos dispositivos capaces de transmitir información entre ellos sin el uso de un medio físico de transmisión de datos, en su lugar, la comunicación se realiza a través de ondas. Existen diversas tecnologías de de comunicación inalámbrica para este tipos de redes, aunque las más comunes son por ondas electromagnéticas, microondas terrestres, microondas por satélites e infrarrojos.

En redes locales y redes PAN, algunas de las tecnologías de conexión son:

- *Wi-Fi (Wireless Fidelity).*

En español significa literalmente fidelidad sin cables. También se les denomina WLAN ("Wireless Local Area Network") o redes de área local inalámbricas. Se trata de una tecnología de transmisión inalámbrica por medio de ondas electromagnéticas con muy buena calidad de emisión para distancias cortas (hasta teóricamente 100 m).

- *Bluetooth.*

Es un protocolo estándar de comunicación entre dispositivos para la transmisión de voz y datos sin cable, mediante una radiofrecuencia segura en la banda de 2.4 GHz. Permite establecer conexiones de corto alcance (Altavoces, impresoras, teclados, etc) y sus principales objetivos son los siguientes:

- Facilitar las comunicaciones entre equipos móviles.
- Eliminar los cables y conectores entre estos.
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales.

- *Infrarrojo.*

La luz infrarroja no es perceptible por el ojo humano, para su uso en redes los dispositivos deben incidir directamente uno sobre la superficie del otro con la ya mencionada luz para que se produzca el cambio de información. Por esta razón no se utiliza a gran escala, sus principales usos son; mandos a distancia, dispositivos móviles y en algunos periféricos. Uno de sus usos más empleados es el [IrDA](#).

La red Internet

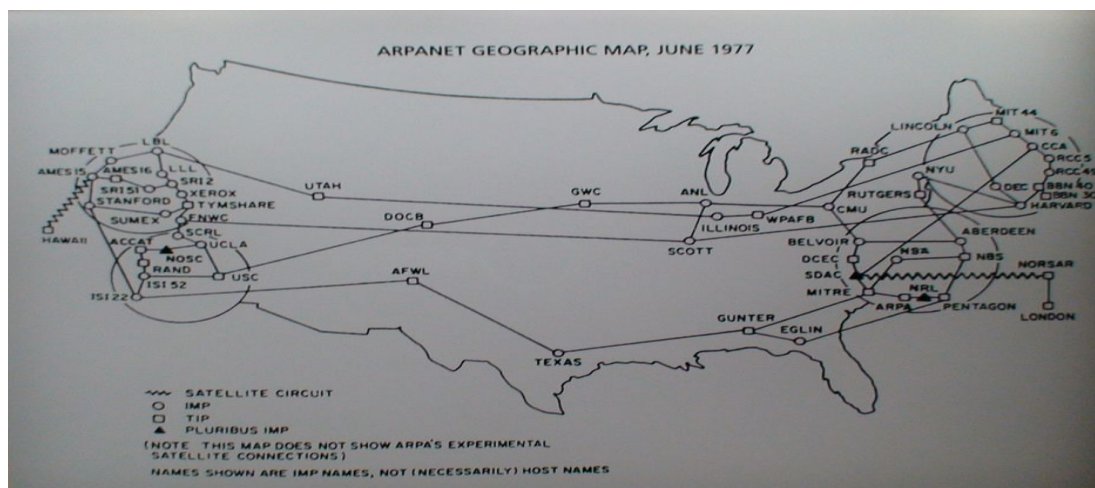
Orígenes de Internet.

Los orígenes de Internet se remontan a más de veinticinco años atrás, como un proyecto de investigación en redes de conmutación de paquetes, dentro de un ámbito militar. A finales de los años sesenta (1969), en plena guerra fría, el Departamento de Defensa Americano (DoD) llegó a la conclusión de que su sistema de comunicaciones era demasiado vulnerable. Estaba basado en la comunicación telefónica , y por tanto, con el consiguiente riesgo de quedar aislado parte del país en caso de un ataque militar sobre esas arterias de comunicación.

Como alternativa, el citado Departamento de Defensa, a través de su Agencia de Proyectos de Investigación Avanzados (Advanced Research Projects Agency, ARPA) decidió estimular las redes de ordenadores mediante becas y ayudas a departamentos de informática de numerosas universidades y algunas empresas privadas. Esta investigación condujo a una red experimental de cuatro nodos, que arrancó en Diciembre de 1969, se denominó ARPAnet. La idea central de esta red era conseguir que la información llegara a su destino aunque parte de la red estuviera destruida. Lo consiguieron enviando los datos en paquetes que viajaban a través de estos nodos, cuando un nodo caía los paquetes buscaban otra vía alternativa.

Los receptores de los paquetes estaban preparados para descifrar los archivos corruptos y detectar errores en la transmisión de datos.

Así nace ARPAnet, la red militar que es reconocida como la progenitora de lo que hoy se conoce como Internet.



Rory Finneren. Flickr. Recuperado de <https://www.flickr.com/photos/roryfinneren/2791016187>

En 1980 las empresas descubren la gran ventaja del uso de ordenadores conectados a la red por lo que comienza el auge de la comercialización de ordenadores y con esto el ascendente uso de Internet. Cabe destacar que en 1990 [Tim Berners-Lee](#) creó el sistema de links lo cual fue fundamental para el desarrollo de la web, el físico no patentó su invento pues no quería poner escollos a la evolución de Internet.

Servicios de Internet

Internet nos proporciona una gran cantidad de servicios, estos cada vez van mejorando para hacer que la navegación por esta red se más cómoda y accesible para todo el mundo.

Algunos de los recursos que nos proporciona Internet son:

- Correo electrónico: Fue una de las primeras aplicaciones que nos permitieron enviar mensajes a alguien a través de Internet. Sirve para enviar y recibir mensajes de cualquier persona que conozca tu dirección, además, puedes enviar o recibir documentos, imágenes vídeos etc...
- WWW (World Wide Web): Es el mecanismo que nos permite visualizar las páginas web en Internet.
- Banner cookies y enlaces: Son dispositivos que facilitan la navegación por Internet. Las cookies conducen a los usuarios hacia las páginas del comercio y permiten que el comerciante obtenga información del cliente.
- Buscadores: Mantienen la información organizada de manera que al introducir una palabra clave nos conduce a páginas web que contengan información sobre lo que estamos buscando.

La web.

Es un sistema de distribución de documentos conectados y que puede visitar cualquiera a través de Internet. Todos estos estos documentos son música, vídeos, imágenes, etc...

Algunos ejemplos de aplicaciones web son [Polarr](#) que sirve para modificar fotos, [Spotify](#) en la que puedes escuchar música gratis, [Netflix](#) que sirve para ver películas y series por internet pero es de pago.

La evolución de la web

A lo largo del tiempo las web han evolucionado hasta el punto de permitir a los desarrolladores la producción de experiencias web increíbles. Todo esto se debe en gran parte al esfuerzo de una comunidad abierta que favorece el desarrollo tecnológico ([HTML5](#), [CSS3](#) y [WebGL](#)).

- *Web 1.0 o web estática.*

Esta red nace en el siglo 20, es muy primitiva pues se trataba de una red unidireccional (el receptor era pasivo, un observador). En ella los contenidos no eran actualizados debido a la falta de tecnología de la época que dificultaba enormemente esta tarea que solo podía ser llevada a cabo por el “WebMaster”, por lo que estos se quedaban anticuados con mucha frecuencia. La web 1.0 tenía carácter divulgativo , en ella se colgaban documentos e información del tipo cultural.



hazhistoria. Recuperado de <http://www.hazhistoria.net/blog/historia-del-www-de-la-web-10-la-web-30>

- *Web 2.0 o web social*

Este término se acuñó en el 2003 y se refiere al fenómeno social producido gracias a la aparición de diversas aplicaciones en Internet tales como [Facebook](#), [YouTube](#) o [Wikipedia](#), estas herramientas tienen en común que su función es la de interactuar con el resto de usuarios o aportar contenido para que la navegación por Internet sea más completa.



Web 2.0. Recuperado de https://es.wikipedia.org/wiki/Web_2.0

- *Web 3.0 o web semántica*

Es una expresión que se utiliza para describir la evolución del uso y la interacción de las personas en internet a través de diferentes maneras entre ellas la transformación de la red en una base de datos. Esta web apareció en 2006 por lo tanto no es muy antigua.



Emaze. Recuperado de <https://www.emaze.com/@AIZWLWWZ/la-evolucion-de-la-web>

Tecnologías de acceso a internet

Acceso cableado.

Son aquellas tecnologías que requieren de un cable para establecer la conexión, este cable irá hasta el terminal del usuario, por lo tanto la ubicación de este ha de ser relativamente fija. Este es el caso de la mayoría de servicios de banda ancha domésticos, estos accesos se suelen basar en las siguientes tecnologías.

- *xDSL*: Comúnmente conocida como [ADSL](#), provén de acceso a internet a través de la línea telefónica tradicional. Estas redes son muy comunes pero están siendo sustituidas progresivamente por la fibra óptica pues presenta mejores características para la transmisión de datos a alta velocidad y a largas distancias.
- *Cable o HFC*: Esta tecnología se basa en los cables coaxiales aunque en sus tramos troncales también presentan cables de fibra óptica, por esta se les denomina redes híbridas de fibra óptica y cable ([HFC](#))
- *Fibra óptica hasta el hogar*: Están sustituyendo a los accesos tradicionales basados en cable de cobre debido a su gran capacidad para transmitir datos, están basados exclusivamente en [fibra óptica](#) para ofrecer acceso a internet.

Acceso inalámbrico.

Son aquellas que no necesitan un cable para conectarse con el terminal del usuario, ya que la comunicación se establece a través de ondas electromagnéticas, estas permiten una mayor movilidad del usuario que no se debe encontrar en una posición fija aunque también presenta límites (el usuario no puede estar en una distancia superior al punto de alcance). La velocidad real de acceso a Internet dependerá de la velocidad que se tenga contratada con el proveedor de servicio de acceso a Internet y se debe tener en cuenta también que a mayor distancia esté el terminal del punto de acceso se perderá más agilidad en la conexión. Este tipo de accesos se basan principalmente en las siguientes tecnologías.

- *WiFi*: Es la conexión inalámbrica más popular en las redes domésticas sustituyendo la conexión por cable del terminal.
- *WiMAX*: El [WiMAX](#) al igual que el WiFi permite una conexión inalámbrica a través de ondas electromagnéticas, su rendimiento es similar pero se diferencia en la magnitud de transmisión de datos pues tiene un alcance teórico de hasta unos 50 kilómetros para dispositivos fijos y de 15 kilómetros para dispositivos móviles.
- *Satélites de telecomunicaciones*: Permiten una conexión inalámbrica y su principal característica es que esta es prácticamente universal pero su velocidad de conexión se ve limitada por varios [factores](#) (obstáculos, climatología...)

Acceso móvil.

Son aquellos accesos inalámbricos que permiten una movilidad prácticamente plena al usuario gracias a la disposición de una red de múltiples accesos, de tal forma que este obtiene una cobertura mucho más amplia que con un único punto de acceso a la red. Es el caso de los servicios de banda ancha a través del móvil. Se basa en las siguientes tecnologías principalmente.

- *UMTS (3G)*: El UMTS (Universal Mobile Telecommunications System o Sistema Universal de Telecomunicaciones Móviles) es una tecnología móvil de la llamada tercera generación (3G), sucesora de la tecnología GSM (Global System for Mobile) o 2G.
- *LTE (4G)*: El LTE (Long Term Evolution) supone el siguiente escalón tras la tecnología UMTS (3G), introduciendo importantes mejoras en cuanto a la gestión de las conexiones de datos y la eficiencia en la transmisión, lo que redundará en redes móviles con alta capacidad para la descarga de datos y con menores costes de operación y mantenimiento.

Línea telefónica.

Es también llamada Dial-Up, este es el método de acceso a Internet más antiguo y el que se utilizó cuando Internet estaba dando sus primeros pasos. Utiliza la red de telefonía para acceder a Internet.

- RTC (Red de Telefonía Conmutada).

La transmisión de datos no supera los 56 kbps lo que hace que la navegación sea lenta, esta transmisión se lleva a cabo a través de un [módem](#), en su estado más primitivo encontramos las siguientes ventajas y desventajas:

Ventajas.

Bajo coste: Es el método más barato de conexión a Internet

Seguridad: La rotación de rotación de las direcciones asignadas al usuario la convierten en el acceso más seguro.

Desventajas.

Baja velocidad: Como ya se comentó no supera los 56 kbps, lo que hace imposible las visiones de streamings que requieren de una buena conexión.

Internet o hablar por teléfono: Así es, cuando se usaba el Internet la línea telefónica se mantenía ocupada por lo que no se podían utilizar ambas cosas a la vez.

Pero la conexión RTC por línea telefónica evolucionó con el tiempo dando lugar a sistemas mucho más desarrollados:

- ***RDSI (Red Digital de Servicios Integrados)***

Esta conexión es la evolución de la RTC y supone un gran cambio, las conexiones se realizan de extremo (red) a extremo (impresoras, ordenadores...) y proporcionan servicios a los cuales lo usuarios acceden a través de una interfaz normalizada.

- Acceso Básico ([BRI](#)): Es un acceso simultáneo a 2 canales de 64 Kbps., denominados canales B, para voz o datos, posee un canal de 16 Kbps, o canal D el conjunto de los tres canales usados de manera conjunta proporciona 144 Kbps.
- Acceso Primario (PRI): Acceso simultáneo a 30 canales tipo B, de 64 Kbps. para voz y datos, posee un canal de 64 Kbps. o canal D, para la realización de la llamada y la señalización entre dispositivos de la red. En conjunto proporciona 1.984 Kbps.

Ventajas de los RDSI:

- Calidad de servicio: gran velocidad en los tiempos de establecimiento y liberación de las llamadas. Alta velocidad de transmisión y baja tasa de errores.
- Posibilidades de utilización: integración de voz, datos, texto e imagen, Terminales multiservicio, Integración de redes.
- Economía: transferencia de grandes volúmenes de información en menos tiempo. Solución única a las diversas necesidades de comunicación.

- ***ADSL (Línea de Abonado Digital Asimétrica)***

La transmisión de datos se realiza de forma analógica a través del cable de pares simétricos de cobre o lo que es lo mismo, el usuario se accede a la red utilizando la línea telefónica a través de la banda ancha.

En este tipo de conexiones un enrutador (es la traducción castellana de la palabra inglesa “[Router](#)”) se encarga de modular las señales con los datos en una banda de frecuencias superior a la empleada en las comunicaciones telefónicas, después, un filtro hace posible que las señales no sufran distorsiones.

De esta forma el ADSL trabaja con 3 canales de comunicación unidos en un mismo cable tales que un canal posibilita la transmisión de datos, un segundo se utiliza para la descarga de datos y un tercero facilita el desarrollo de las comunicaciones telefónicas convencionales.

Dado que los usuarios bajan más archivos de la red de lo que suben, el ADSL lleva a cabo un aprovechamiento de datos de tal forma que la velocidad de descarga de datos es superior a la de subida (es por eso que se considera asimétrica).

Cable o HFC

Cable: Este sistema nos permite estar conectado a la red permanentemente.

Sus ventajas son:

- El coste se reduce ya que se paga por mes y no por minuto.
- La velocidad es mayor que la de estar conectado mediante un módem.

HFC: Este sistema implementa a su vez la fibra óptica y el cable coaxial para crear una red de banda ancha, para ello, la empresa conecta al cliente mediante cable a un nodo zonal y posteriormente conecta los nodos zonales con fibra óptica. Con esta tecnología se aprovechan las ventajas de los dos sistemas y se minimizan las limitaciones de cada uno.

Fibra óptica hasta el hogar

La fibra óptica es un gran medio de transmisión gracias a sus buenas características de capacidad y baja atenuación. Hay dos tipos de redes de fibra óptica:

- Redes punto a punto: Cada usuarios está conectado mediante una fibra individual a la central.
- Redes punto-multipunto: Cuando varios usuarios comparten un mismo tramo de fibra desde su vivienda a la central.

Con este sistema se consiguen velocidades de descarga superiores a las de las redes convencionales.

Internet por satélite

Este sistema es parecido al que utilizan las televisiones digitales, pero en este caso el usuario además de recibir una señal tiene que poder emitir, para ello se necesita un módem, un decodificador y una parabólica. Sus principales ventajas son:

- Su amplia cobertura ya que llega a lugares donde el cable no llega, además supera en velocidad al ADSL convencional.
- Este tipo de servicios ya está muy extendido por lo que no será difícil encontrar un buen proveedor.

WIMAX y LMDS

Wimax es la tecnología destinada a ofrecernos conexiones a Internet más rápidas y con mejor cobertura que el actual wifi. Esta tecnología nos proporciona una cobertura de unos 70 Km y una velocidad de 124 Mbps. Hasta ahora las redes wifi más rápidas proporcionan unos 54 Mbps y una cobertura de 300 metros.

LMDS es una tecnología que gracias a su ancho de banda nos permite la conexión a Internet, esta tecnología utiliza una frecuencia de 28 GHz, estas frecuencias tan altas no son capaces de atravesar obstáculos por lo que desde la estación base hasta la antena del cliente no puede haber ningún obstáculo ya que si no, el cliente no tendría acceso a los servicios que solicita.

Red eléctrica.

Este sistema proporciona acceso a la red a través de la red eléctrica sin necesidad de realizar ninguna instalación, solo es necesario colocar un PLC, lo que nos abarata mucho la transmisión de internet (con una mayor calidad que la conexión Wi Fi) a comparación de una instalación por transmisión de Ethernet (que nos ofrece mayor calidad de conexión que víaa PLC)

PLC (Power Line Communications) es un concepto que engloba diferentes tecnologías que permiten enviar transmisiones de datos a través de líneas de electricidad. Con este nuevo concepto, podemos utilizar la instalación eléctrica de casa como infraestructura de telecomunicaciones. Hay que puntualizar que el rendimiento que ofrece el dispositivo depende de la calidad de la señal eléctrica que tengamos en casa; por tanto, este sistema se perfila mucho más fiable que el WiFi (especialmente en largas distancias).



Serglobin. Recuperado de <http://serglobin.es/blog/plc-internet-a-traves-de-la-red-electrica-de-casa/>

Conexión por telefonía móvil.

Es la comunicación inalámbrica a través de ondas electromagnéticas, como cliente de este tipo de redes se utiliza un dispositivo llamado teléfono móvil.

Primera generación, 1G

Es la generación de los móviles de los 80, es analógico y usa un sistema digital para conectar las radiobases al resto del sistema telefónico.

Segunda generación, 2G

Esta generación es de los 90, deriva de la necesidad de tener una mayor manejabilidad a la hora de tener que llamar, abarca varios protocolos de diferentes compañías.

Tercera generación, 3G

Se empezó a utilizar hace unos años esta generación ofreció conexión a internet, y permiten conexión a wifi y bluetooth.

Cuarta generación, 4G

Es la generación más actual, permite una mayor velocidad de conexión a internet, esta generación también se usa para tecnologías que en Japón han hecho que un vehículo alcanzase los 200km/h.

Seguridad en la red

Con la normalización y abaratamiento de conexiones de banda ancha Internet se ha convertido en una herramienta masificada, la gran mayoría de personas cuentan con uno o más dispositivos para acceder a la red.

Esto hace que entre tantas personas se produzcan daños inintencionados o incluso se creen grupos con el fin de llevar a cabo actos ilícitos. Por esto es necesario llevar a cabo medidas de protección para cada caso en concreto y así prevenir ataques de hackers que producen malwares, ejemplos de este tipo de infecciones de los equipos informáticos o agresiones al usuario son los siguientes; virus, [gusanos](#), ciberbullying, grooming, spam, software espía (que se hace con tus datos financieros), etc.



CyL Digital. Recuperado de <http://www.cyldigital.es/articulo/seguridad-en-la-red-definicion-y-conceptos-basicos>

Legislación en la red

- **LOPD**

Es la ley que regula la protección de datos personales ya que es un derecho fundamental para todas las personas el tener la potestad de decidir lo que hace con sus datos personales. esta ley consigue evitar que se llegue a disponer de información que pueda afectar a nuestra intimidad.

- **LPI**

La LPI (Ley de Propiedad Intelectual) es el conjunto de derechos que tienen los creadores de obras literarias, artística, científicas etc...

Los creadores de las obras tienen que conocer su derechos que son:

- Derechos morales: Son derechos que acompañan al autor durante toda su vida y que pasan a sus herederos al morir el autor. Destacan el derecho al reconocimiento del autor de la obra y el de respetar la integridad de la obra.
- Hay dos grupos de derechos patrimoniales:
 - Derechos de explotación de la obra: El autor recibe una remuneración por la creación de su obra.
 - Derechos compensatorios: Como el derecho por copia privada que permite a la persona que visualice la obra el hacer una copia de la obra original siempre y cuando sea para uso propio sin ánimo de lucro.

- **LSSI-CE**

La función de la LSSI-CE (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico) es dar más confianza a los usuarios de internet para que utilicen esta red como herramienta para las transacciones cotidianas, para ello recoge las obligaciones de los prestadores de servicios para garantizar la seguridad de los consumidores.



LSSI-CE. Recuperado de <http://www.legislacioninternet.com/lssi-ce/>

- **LAECSP**

La LAECSP (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos) es una ley que reconoce el derecho de los ciudadanos a comunicarse con las administraciones públicas y obliga a estas a dar la posibilidad de comunicarse con ellas.

- ***Ley de firma electrónica***

La firma electrónica es el equivalente electrónico a la firma manuscrita, en España se distinguen tres tipos de firmas:

- Firma electrónica: Conjunto de datos en forma electrónica que pueden ser utilizados como medio de identificación.
- Firma electrónica avanzada: Esta firma permite identificar al firmante y detectar cambios en los datos firmados, esta firma la crea el firmante mediante medios que él puede mantener bajo su propio control.
- Firma electrónica reconocida: Es como la anterior pero basada en un certificado reconocido y creada mediante un dispositivo seguro de creación de firma.
-

Adopción de medidas de seguridad

Protección

Antivirus

Un antivirus es una aplicación que se encarga de detectar los virus de nuestro ordenador o de eliminarlos, hoy en día es una aplicación casi imprescindible ya que estamos continuamente expuestos a que nos entre cualquier virus al entrar en páginas web o al descargar cualquier archivo. Cada poco tiempo aparecen nuevos virus por lo que es importante que nuestro antivirus esté siempre actualizado, los antivirus son muy importantes ya que además de protegernos contra los propios virus nos protege contra más tipos de ataques como pueden ser troyanos, spyware o adware.

Cortafuegos

En los inicios de Internet cuando la red todavía era un esbozo de lo que es actualmente ya había gente que se dió cuenta de que podía infiltrarse en los equipos ajenos a través de la conexión a Internet, para ello se empezaron a investigar métodos para evitar que accedan a tu ordenador sin tu autorización, esa es la función del cortafuegos, definir quien puede y quien no puede acceder a tu ordenador. Hay dos tipos de cortafuegos:

- Cortafuegos de hardware: Proporcionan una fuerte protección contra los ataques del exterior pero no es tan eficaz como un cortafuegos de software.
- Cortafuegos de software: Este cortafuegos protege a tu equipo de que intenten controlar o acceder a tu ordenador desde el exterior.
-

Recuperación

Copias de seguridad

Es una copia de unos datos originales para disponer de un medio para recuperarlos en caso de que perdamos el original.



Información en la nube

Otro método para recuperar la información es el almacenamiento en la nube, para ello, hay servicios online que nos permiten almacenar archivos en la nube de manera que en caso de que perdamos un archivo de nuestro ordenador podemos irnos a la aplicación que utilicemos y recuperar de ahí nuestra información.



Almacenamiento en la nube. Recuperado de

<http://comunidad.movistar.es/t5/Bienvenida-y-Noticias/Los-servicios-de-almacenamiento-en-la-nube-que-m%C3%A1s-espacio/td-p/189405>

1

SAN

Una red SAN (Red de Área de Almacenamiento) es una red dedicada al almacenamiento de información, la capacidad de estas redes es casi ilimitada ya que aumenta al añadir más conexiones de acceso.

Conexiones seguras y cifradas.

Hoy en día se ha vuelto muy práctico identificarse en la red para llevar a cabo múltiples procesos con mayor comodidad y rapidez que con los métodos tradicionales, es por eso que es muy importante tener métodos de identificación seguros tales como los DNIe y los certificados digitales, así como saber que estamos accediendo a páginas de confianza libres de malware gracias a los HTTPS, etc.

DNIe

Este es un documento que se puede utilizar tanto para la identificación virtual como la personal, sus siglas se corresponden a la nomenclatura de Documento Nacional de Identidad electrónico, es emitido por una autoridad oficial. Su principal característica es que posee un chip capaz de almacenar información de forma segura y de procesarla internamente.

Este [DNIe](#) fue suplantado sucesivamente al DNI tradicional pues agrega nuevas aplicaciones; realizar compras firmadas a través de Internet, hacer trámites Completos con las Administraciones Públicas (peticiones de becas...), realizar transacciones seguras con entidades bancarias.



DNIe. Recuperado de <http://www.dnieshop.com/es/content/7-sobre-el-dnie>

Certificados digitales.

El certificado digital es un documento que facilita cualquier tipo de trámite en la red así como compras online y que te ofrece la seguridad y privacidad de tus datos, este, garantiza la vinculación entre una persona o entidad con su llave pública. Contiene información del usuario y del propio documento; nombre, correo, empresa, número de serie único, periodo de validez, etc.

HTTPS.

Cuando en una página web utiliza el protocolo HTTPS significa que emplea un sistema en el que se produce la encriptación de la información transmitida dificultando así la interceptación de esta por terceros. Para saber si un portal utiliza dicho protocolo podremos ver en la barra de las URL que “http://” será sustituido por “https://” (siendo el primero un protocolo que envía información plana, es decir sin encriptar, anterior y menos avanzado que el segundo) y un candado que nos lo verificará. Si además de esto en la barra observamos un fondo de color verde querrá decir que la página utiliza [Certificados de Validación Extendida](#) (ofrecen mayor seguridad).



Certificado electrónico.

Un [Certificado Electrónico](#) es un documento expedido por una Autoridad de Certificación e identifica a una persona (física o jurídica) con un par de claves, este, tiene como misión validar y certificar que una firma electrónica se corresponde con una persona o entidad concreta.

Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, claves de firma...

La Autoridad de Certificación da fe de que la firma electrónica se corresponde con un usuario concreto. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación.

Configuración segura del navegador.

Dado que a la red accede todo tipo de personas es necesario una configuración de tu navegador adecuada con el fin de evitar cualquier tipo de incidencia. Cuando hablamos de configuración segura de nuestro navegador, nuestros objetivos son los siguientes:

- Que no nos rastreen, para esto tan solo ofrecemos a las páginas web los datos necesarios y esenciales.
- No acceder a páginas fake (páginas falsas) que tienen el fin de robarnos datos como contraseñas.
- Evitar todo riesgo de instalación de malware en nuestro terminal
- Evitar la contaminación de nuestras cuentas así como de nuestros sistemas con spam.
- Tras la desconexión, que no queden datos de nuestras cuentas de usuario o cualquier tipo de información personal.

Para eso podemos ajustar los siguientes parámetros en nuestros navegadores:

Navegación privada.

Este apartado de configuración es muy recomendado para que nadie que utilice un mismo terminal que tu tenga ningún tipo de información a cerca de ti. Cuando activamos esta opción lo hacemos con cinco objetivos esenciales (esta información está sacada de la [navegación segura de Google](#))

- Cookies, estas desaparecen al apagar el ordenador.
- Eliminación del caché web.
- Eliminación del historial.
- Supresión de datos para autocompletar cuestionarios.
- Eliminación de datos como contraseñas, listas de descargas...

Filtro contra la suplantación de identidad, Phishing.

Este filtro tiene la función de identificar la presencia de actividades sospechosas en una página, la cual está utilizando una identidad falsa con el fin de conocer datos personales y normalmente de alta privacidad del usuario. Cabe destacar que es muy sencillo hoy en día llevar a cabo este tipo de engaños, los hackers de no muy alto nivel pueden llevarlo a cabo con simples descargas de softwares presentes en la propia red. Aquí os dejo un [video](#) de [Chema Alonso](#) (una persona que se encarga de luchar por la seguridad en la red) en el Hormiguero el cual tiene multitud de vídeos y posts en los que nos muestra lo sencillo que puede llegar a ser hacer este tipo de cosas.

Confidencialidad.

Es la propiedad de prevenir la divulgación de la información a personas o sistemas no autorizados, más o menos la confidencialidad es el acceso a la información únicamente por las personas que tengan una autorización.

Autenticación.

Es la verificación de la identidad de una persona o usuario para acceder a determinados recursos o realizar unas tareas.

Integridad.

Es la capacidad de garantizar que los datos no han sido modificados desde su creación.

Disponibilidad.

Nos referimos a este término cuando hablamos del acceso de personas u organismos a los datos con los que se trabaja.

Amenazas a la seguridad.

Es el área de la informática que se enfoca en la protección de la infraestructura computacional y la información contenida o circulante.

Causas humanas.

Son todas las acciones en las que interviene el ser humano, que están penadas y violan la ley.

Causas lógicas.

Son las que ocurren por decisiones humanas que tiene poder e influencia sobre el sistema.

Causas físicas.

Son todos las de origen físico y técnico, sino también eventos indirectamente causados por la intervención humana.