# REDES

# INALÁMBRICAS

Diego Castro Freire

Yannick Juncal García

Rubén Lado Martínez

Tecnologías de la Información y de la Comunicación I

Instituto de Educación Secundaria Eduardo Blanco Amor

Culleredo, 2016

ÍNDICE

- Según su área de cobertura
    - Red de área extensa, WAN
    - Red de área metropolitana, MAN
    - Red de área local, LAN
    - Red de área personal, PAN
- Según su tipología
    - Bus
    - Anillo
    - Estrella
    - Árbol
    - Híbrida
- Según su nivel de acceso o privacidad
    - Red pública
    - Red privada
    - VPN (red privada virtual)
- Según su relación funcional
    - Cliente-Servidor
    - Redes entre iguales, P2P
- Según su tecnología física de conexión
    - Redes cableadas
        - Fast Ethernet
        - Gigabit Ethernet
        - 10 Gigabit Ethernet
    - Redes inalámbricas

- Wi-Fi
- Bluetooth
- Infrarrojos

**La red Internet**

- Orígenes de internet
- Servicios de internet
- La web
- 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
- RDSI
- ADSL

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**

- Confidencialidad
- Autentificación
- Autorización
- Integridad
- Disponibilidad

Amenazas a la seguridad

- Causas humanas
- Causas lógicas
- Causas físicas

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
- Bloqueador de elementos emergentes
- Java/JavaScript
- Filtrado Active X
- Configuración de las cookies

**·ORIGEN:**

Es en 1880 cuando se inventa el primer aparato de comunicación sin cables, el fotófono, teniendo como padre al británico Alexander Graham Bell, quien acompañado por Charles Sumner Tainter lo patentaría.

Este novedoso invento para la época, que permitía la transmisión de sonido mediante una emisión de luz, no tendría demasiado éxito, ya que, por aquel entonces aún no se distribuía la electricidad y tan solo había transcurrido un año desde la invención de las primeras bombillas.

Ocho años más tarde el físico alemán Rudolf Hertz realizó la primera transmisión sin cables con ondas electromagnéticas con un oscilador que usó como emisor y un resonador que usó como receptor. Seis tardarían desde entonces las ondas de radio en convertirse en un medio de comunicación. Sería más tarde, en 1899, cuando Guillermo Marconi consiguió establecer comunicación inalámbrica a través del canal de la Mancha, entre Dover y Wilmereux. En 1907, los primeros mensajes completos ya "cruzaban el charco" de un lado a otro del Atlántico. Conocemos en la actualidad las numerosas barbaries y las terribles consecuencias del gran conflicto bélico del siglo XX, la Segunda Guerra Mundial, pero por el contrario, en este campo produjo importantes avances.

Primera red local inalámbrica

No fue hasta 1971 cuando un grupo de investigadores de la Universidad de Hawaii, crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por

radio, a la que dieron el nombre de “Aloha”. Ésta es la primera red de área local inalámbrica (WLAN), formada por siete computadoras, situadas en distintas islas, que se podían comunicar con un ordenador central, al que pedían que realizara cálculos. Uno de los primeros problemas que tuvieron fue el control de acceso al medio (MAC), es decir, el protocolo a seguir para evitar que las distintas estaciones solapen sus mensajes entre sí. En un principio se solucionó haciendo que la estación central emitiera una señal intermitente en una frecuencia distinta a la del resto de computadoras mientras estuviera libre, de tal forma que cuando una de las otras estaciones se disponía a transmitir, antes “escuchaba” y se cercioraba de que la central estaba emitiendo dicha señal para entonces enviar su mensaje, esto se conoce como CSMA (Carrier Sense Multiple Access).

Un año después Aloha se conectó mediante ARPANET (red de computadoras creada por el Departamento de Defensa de los EEUU que se utilizaba como medio de comunicación entre los diferentes organismos del país) al continente americano.

**Funcionamiento**

Se utilizan ondas electromagnéticas para transportar información de un punto a otro, para este objetivo se hace uso de ondas portadoras. Ondas de una frecuencia muy superior a la de la onda moduladora (señal que contiene la información a transmitir). La onda moduladora se acopla con la portadora, hecho llamado modulación, surgiendo una señal de radio que ocupa más de una frecuencia (un ancho de banda) debido a que la frecuencia de la primera se acopla a la de la segunda. Gracias a esto, pueden existir varias portadoras simultáneamente en el mismo espacio sin interferirse, siempre que se transmitan en diferentes frecuencias. Otra ventaja de la modulación mediante ondas portadoras es la mayor facilidad en la transmisión

de la información. Resulta más barato transmitir una señal de frecuencia alta (como es la modulada) y el alcance es mayor. El receptor se sintoniza para seleccionar una frecuencia de radio y rechazar las demás, tras esto demodulará la señal para obtener los datos originales, es decir, la onda moduladora. El dispositivo electrónico encargado de esta tarea se llama módem debido a que MOdula y DEModula.

https://es.scribd.com/doc/28065286/Origenes-de-Las-Redes-Alambricas-e-Inalambricas

**-FUNDAMENTOS DE LAS REDES:**

**-Procesos de comunicación:**

El proceso de comunicación ha cambiado mucho hasta la actualidad. Hoy los canales se han multiplicado haciendo más compleja cualquier estrategia de comunicación. Internet ha generado una mayor accesibilidad, bidireccionalidad y abundancia en el flujo de la información, modificando las dinámicas de la comunicación, cuya gestión, en la sociedad digital, debe plantearse de forma integral.

La comunicación por medio de una red se lleva a cabo en dos diferentes categorías la **capa física** y la **capa lógica .**

La capa física incluye todos los elementos de los que hace uso un equipo para comunicarse con otros equipos dentro de la red, como, por ejemplo, las tarjetas de red, los cables… La comunicación a través de la **capa lógica** se rige por normas muy rudimentarias, con las cuales se formarán los diferentes protocolos, normas más complejas que dan lugar a resultados de alto nivel.

http://www.tecnohotelnews.com/2012/05/el-proceso-de-comunicacion-en-el-mundo-digital/

**-Redes de ordenadores:**

Una red de computadoras es un conjunto de equipos conectados por medio de cables o señales, ondas o cualquier otro método de transporte de datos. Las redes de ordenadores nacen como evolución de los sistemas de transmisión y acceso a la información y permiten el acceso a información remota, entretenimiento interactivo y comunicación entre personas. Un ejemplo que cumple esta función es internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos. A cada una de las computadoras que están conectadas a la red la denominaremos nodo. Además, también encontramos la estación de trabajo (cualquier terminal) y el bus (cable o canal de trasmisión que une los distintos componentes de la red)

Como en todo proceso de comunicación, se requiere un emisor, un mensaje, un canal y un receptor. La comunicación por medio de una red se lleva a cabo en la capa física y la capa lógica, como ya vimos.

Para poder formar una red se requieren elementos: Hardware, software y protocolos, siendo el fin de una red interconectar los componentes hardware a los equipos que ponen los servicios red.

## ORIGEN Y MODELOS DE REFERENCIA

**-MODELO OSI**

La mayoría de los conjuntos protocolos de red se estructuran en capas. La Organización Nacional para la Estandarización (ISO) (organización que representa a 130 países) diseñó el modelo de referencia de Interconexión de Sistemas Abiertos (un sistema abierto es un sistema que puede conectarse con algún medio y no es exclusivo de alguna tecnología) en el año 1980, sistema que utiliza capas estructuradas.

- ➔ Origen: A principios de 1980 se produjo un crecimiento de la cantidad y el tamaño de las redes. Las diferentes empresas comenzaron a sufrir así diversos problemas a causa de esta expansión. Las diferentes redes contaban con distintos especificadores e implementadores ,lo cual dificultó mucho el intercambio de información. Muchas empresas desarrollaron tecnologías de forma propietaria, lo que hacía que su implementación a otros equipos estuviese sujeta al copyright., y que limitó aún más la comunicación entre redes. Para enfrentar el problema de incompatibilidad de redes, la ISO investigó modelos de conexión con el fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. Con base en esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes.

- ➔ Capas: existen siete en el modelo OSI.

    **1. Aplicación:** Provee servicios generales relacionados con aplicaciones (transferencia de archivos)

    **2. Presentación:** Formato de datos (ej. ASCII)

    **3. Sesión**: Coordina la interacción en la sesión de los usuarios

    **4. Transporte**: Provee una trasmisión de datos fiables punto a punto.

**5. Red:** Administra las direcciones de datos y la transferencia entre redes

**6. Vínculo de datos:** Administra la transferencia de datos en el medio de red.

**7. Física:** Define las características del hardware de red.

**·PROTOCOLO IP:**

**-DIRECCIONES IP**

Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, *smartphone*) que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del modelo TCP/IP. La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red.

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

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

***DIRECCIONES IPv4**

Las direcciones IPv4 se expresan por un número binario de 32 bits permitiendo un espacio de direcciones de hasta 4.294.967.296 ($2^{32}$) direcciones posibles. Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el intervalo de 0 a 255 [el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255].

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

Un ejemplo de representación de dirección es: IPv4: 10.128.1.253

En las primeras etapas del desarrollo del Protocolo de Internet, los administradores de Internet interpretaban las direcciones IP en dos partes, los primeros 8 bits para designar la dirección de red y el resto para individualizar la computadora dentro de la red. Este método pronto probó ser inadecuado, cuando se comenzaron a agregar nuevas redes a las ya asignadas. En 1981 el direccionamiento internet fue revisado y se introdujo la arquitectura de clases. (classful network architecture). En esta arquitectura hay tres clases de direcciones IP que una

organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

- En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los *hosts (*computadoras conectadas a una red, que proveen y utilizan servicios de ella), de modo que la cantidad máxima de *hosts* es $2^{24}$ - 2, es decir, 16 777 214 *hosts*.

- En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los *hosts*, de modo que la cantidad máxima de *hosts* por cada red es $2^{16}$ - 2, o 65 534 *hosts*.

- En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los *hosts*, de modo que la cantidad máxima de hosts por cada red es $2^{8}$ - 2, o 254 *hosts*.

El diseño de redes de clases (*classful*) sirvió durante la expansión de internet, sin embargo este diseño no era escalable y frente a una gran expansión de las redes en la década de los noventa, el sistema de espacio de direcciones de clases fue reemplazado por una arquitectura de redes sin clases Classless Inter-Domain Routing (CIDR)[4] en el año 1993. CIDR está basada en redes de longitud de máscara de subred variable (variable-length subnet masking VLSM) que permite asignar redes de longitud de prefijo arbitrario. Permitiendo una distribución de direcciones más fina y granulada, calculando las direcciones necesarias y "desperdiciando" las mínimas posibles.

***DIRECCIÓN IPv6:**

La dirección IPv6 es una etiqueta numérica usada para identificar una interfaz de red (elemento de comunicación/conexión) de un ordenador o nodo de red participando en una red IPv6.

Las direcciones IP se usan para identificar de manera única una interfaz de red de un host, localizarlo en la red y de ese modo encaminar paquetes IP entre hosts. Con este objetivo, las direcciones IP aparecen en campos de la cabecera IP indicando el origen y destino del paquete.

IPv6 es el sucesor del primer protocolo de direccionamiento de Internet, Internet Protocol versión 4 (IPv4). A diferencia de IPv4, que utiliza una dirección IP de 32 bits, las direcciones IPv6 tienen un tamaño de 128 bits. Por lo tanto, IPv6 tiene un espacio de direcciones mucho más amplio que IPv4.

Las direcciones IPv6 se clasifican según las políticas de direccionamiento y encaminamiento más comunes en redes: direcciones unicast, anycast y multicas.

- Una dirección unicast identifica un único interface de red. El protocolo de Internet entrega los paquetes enviados a una dirección unicast al interface específico.
- Una dirección anycast es asignada a un grupo de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección anycast se entrega únicamente a uno de los miembros, típicamente el host *con menos coste*, según la definición de métrica del protocolo de encaminamiento. Las direcciones anycast no se identifican fácilmente pues tienen el mismo formato que las unicast, diferenciándose únicamente por estar presente en varios puntos de la red. Casi cualquier dirección unicast puede utilizarse como dirección anycast.

- Una dirección multicast también es usada por múltiples interfaces, que consiguen la dirección multicast participando en el protocolo de multidifusión (multicast) entre los routers de red. Un paquete enviado a una dirección multicast es entregado a todos los interfaces que se hayan unido al grupo multicast correspondiente.

IPv6 no implementa direcciones broadcast. El mismo efecto puede lograrse enviando un paquete al grupo de multicast de enlace-local todos los nodos *(all-nodes)* ff02::1. Sin embargo, no se recomienda el uso del grupo *all-nodes*, y la mayoría de protocolos IPv6 usan un grupo multicast de enlace-local exclusivo en lugar de molestar a todos los interfaces de la red.

***IP ESTÁTICA O FIJA:**

Cuando nos conectamos a Internet, nuestro proveedor de acceso a Internet (ISP) nos asigna una dirección IP. Este nos puede asignar siempre la misma dirección IP (**IP fija**) o darnos una diferente (**IP dinámica**) cada vez que nos conectamos. Una **dirección IP fija** es una dirección IP asignada por el usuario de manera manual (en algunos casos el ISP o servidor de la red no lo permite), o por el servidor de la red (ISP en el caso de internet, *router* o *switch* en caso de LAN) con base en la Dirección MAC del cliente. Muchas personas confunden IP fija con IP pública e IP dinámica con IP privada.

Una IP puede ser privada ya sea dinámica o fija como puede ser IP pública dinámica o fija.

Una IP pública se utiliza generalmente para montar servidores en internet y necesariamente se desea que la IP no cambie. Por eso la IP pública se la configura, habitualmente, de manera fija y no dinámica.

En el caso de la IP privada es, generalmente, dinámica y está asignada por un servidor DHCP, pero en algunos casos se configura IP privada fija para poder controlar el acceso a internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos. Si esta cambiara (si se asignase de manera fuera dinámica) sería más complicado controlar estos privilegios (pero no imposible).

Las aplicaciones que precisan el uso de una IP fija son:

• Servidor de correo propio.

• Servidor para alojar una web o Intranet.

• Servidor FTP para ficheros.

• Aplicaciones online.

• Conexiones seguras en una Red Privada Virtual.

• Pasarelas de pago.

• Servicios interactivos: videoconferencia.

• Servicios de vigilancia: telealarma o televigilancia.

***IP DINÁMICA:**

Una **dirección IP dinámica** es una IP asignada mediante un servidor DHCP (**Dynamic Host Configuration Protocol**) al usuario. La IP que se obtiene tiene una duración máxima determinada. El servidor DHCP provee parámetros de configuración específicos para cada cliente que desee participar en la red IP. Entre estos parámetros se encuentra la dirección IP del cliente.

Las IP dinámicas son las que actualmente ofrecen la mayoría de operadores. El servidor del servicio DHCP puede ser configurado para que renueve las direcciones asignadas cada tiempo determinado. Estas direcciones tienen una serie de desventajas y desventajas a la hora de usarlas, aquí os mostramos algunos de ellos:

**Ventajas:**

- Reduce los costos de operación a los proveedores de servicios de Internet (ISP).
- Reduce la cantidad de IP asignadas (de forma fija) inactivas.
- El usuario puede reiniciar el *modem o router* para que le sea asignada otra IP y así evitar las restricciones que muchas webs ponen a sus servicios gratuitos de descarga o visionado multimedia en línea.

**Desventajas**

- Obliga a depender de servicios que redirigen un *host* a una IP.

**Asignación de direcciones IP**

Dependiendo de la implementación concreta, el servidor DHCP tiene tres métodos para asignar las direcciones IP:

- **manualmente**, cuando el servidor tiene a su disposición una tabla que empareja direcciones MAC con direcciones IP, creada manualmente por el administrador de la red. Solo clientes con una dirección MAC válida recibirán una dirección IP del servidor.
- **automáticamente**, donde el servidor DHCP asigna por un tiempo preestablecido ya por el administrador una dirección IP libre, tomada de un intervalo prefijado también por el administrador, a cualquier cliente que solicite una.

- **dinámicamente**, el único método que permite la reutilización de direcciones IP. El administrador de la red asigna un intervalo de direcciones IP para el DHCP y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie. El proceso es transparente para el usuario y tiene un periodo de validez limitado.

***IP PÚBLICA:**

Una dirección IP pública se denomina de tal modo cuando es visible en todo Internet. Cuando accedemos a Internet desde nuestro ordenador obtenemos una dirección IP pública suministrada por nuestro proveedor de conexión a Internet, esa dirección IP es nuestra dirección IP de salida a Internet en ese momento, por lo que una IP pública es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet. Algunos ejemplos son: los servidores que alojan sitios web como Google, los router o modems que dan a acceso a Internet, otros elementos de hardware que forman parte de su infraestructura, etc.

Las IP públicas son siempre únicas. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí. Por ejemplo, tu router con un servidor web. O dos servidores web entre sí.

***IP PRIVADA:**

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los *hosts*

que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los *hosts* que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas se clasifican en A, B y C según su número de bits:

- La clase A tiene 8 bits red, 24 bits hosts
- La clase B tiene 16 bits red, 16 bits hosts, y se usa en universidades y grandes compañías.
- La clase C tiene 24 bits red, 8 bits hosts, y se usa en compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los *hosts* de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

**-SUBREDES:**

Una subred es un rango de direcciones lógicas. Cuando una red de computadoras se vuelve muy grande, conviene dividirla en subredes, por los siguientes motivos:

- Reducir el tamaño de los dominios de broadcast.
- Hacer la red más manejable, administrativamente. Entre otros, se puede controlar el tráfico entre diferentes subredes mediante ACLs.

Existen diversas técnicas para conectar diferentes subredes entre sí. Se pueden conectar:

- a nivel físico (capa 1 OSI) mediante repetidores o concentradores (*hubs*),
- a nivel de enlace (capa 2 OSI) mediante puentes o conmutadores (*switches*),
- a nivel de red (capa 3 OSI) mediante *routers*,
- a nivel de transporte (capa 4 OSI),
- aplicación (capa 7 OSI) mediante pasarelas.

También se pueden emplear técnicas de encapsulación (*tunneling*).

En el caso más simple, se puede dividir una red en subredes de tamaño fijo (todas las subredes tienen el mismo tamaño). Sin embargo, por la escasez de direcciones IP, hoy en día frecuentemente se usan subredes de tamaño variable.

Los *routers* constituyen los límites entre las subredes. La comunicación desde y hasta otras subredes es hecha mediante un puerto específico de un *router* específico, por lo menos momentáneamente.

Una subred típica es una red física hecha con un *router*, por ejemplo: una Red Ethernet o una "red de área local virtual" (*Virtual Local Area Network*, **VLAN**). Sin embargo, las subredes

permiten a la red ser dividida lógicamente a pesar del diseño físico de la misma, por cuanto es posible dividir una red física en varias subredes configurando diferentes computadores *host* que utilicen diferentes *routers*. La dirección de todos los nodos en una subred comienzan con la misma secuencia binaria, que es su ID de red e ID de subred. En IPv4, las subredes deben ser identificadas por la base de la dirección y una máscara de subred.

Las subredes simplifican el enrutamiento, ya que cada subred típicamente es representada como una fila en las tablas de ruteo en cada *router* conectado. Las subredes fueron utilizadas antes de la introducción de las direcciones IPv4, para permitir a una red grande tener un número importante de redes más pequeñas dentro, controladas por varios *routers*. Las subredes permiten el enrutamiento entre dominios sin clases (CIDR). Para que las computadoras puedan comunicarse con una red, es necesario contar con números IP propios, pero si tenemos dos o más redes, es fácil dividir una dirección IP entre todos los *hosts* de la red. De esta forma se pueden partir redes grandes en redes más pequeñas.

**-PUERTA DE ENLACE (o Gateway):**

La **pasarela** (en inglés ***gateway*** ) o **puerta de enlace** es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.

Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

La pasarela es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local (*Local Area Network*, LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red

(*Network Address Translation*, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada "enmascaramiento de IP" (*IP Masquerading*), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

**-DNS:**

El sistema de nombres de dominio (DNS, por sus siglas en inglés, *Domain Name System*) es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombre de dominio asignado a cada uno de los participantes. Su función más importante es "traducir" nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

El servidor DNS utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio Google es 216.58.210.163, la mayoría de la gente llega a este equipo especificando www.google.es y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable.[2] La dirección numérica podría

cambiar por muchas razones, sin que tenga que cambiar el nombre tan solo la IP del sitio web.

Estos son los tipos de servidores de acuerdo a su función:

- **Primarios o maestros:** guardan los datos de un espacio de nombres en sus ficheros.
- **Secundarios o esclavos:** obtienen los datos de los servidores primarios a través de una transferencia de zona.
- **Locales o caché:** funcionan con el mismo software, pero no contienen la base de datos para la resolución de nombres. Cuando se les realiza una consulta, estos a su vez consultan a los servidores DNS correspondientes, almacenando la respuesta en su base de datos para agilizar la repetición de estas peticiones en el futuro continuo o libre.

**-DIRECCIÓN MAC:**

En las redes de computadoras, la dirección MAC (siglas en inglés de *Media Access Control*) es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Está determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits) utilizando el *organizationally unique identifier*. La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE (MAC-48, EUI-48, y EUI-64), las cuales han sido diseñadas para ser identificadores

globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet, usándose esta sólo a niveles internos de la red. Sin embargo, es posible añadir un control de hardware en un conmutador o un punto de acceso inalámbrico, para permitir sólo a unas MAC concretas el acceso a la red. En este caso, deberá saberse la MAC de los dispositivos para añadirlos a la lista. Dicho medio de seguridad se puede considerar un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

La dirección MAC es utilizada en varias tecnologías entre las que se incluyen:

- Ethernet
- 802.3 CSMA/CD
- 802.5 o redes en anillo a 4 Mbps o 16 Mbps
- 802.11 redes inalámbricas (Wi-Fi).
- Asynchronous Transfer Mode

MAC opera en la capa 2 del modelo OSI, encargada de hacer fluir la información libre de errores entre dos máquinas conectadas directamente. Para ello se generan tramas, pequeños bloques de información que contienen en su cabecera las direcciones MAC correspondiente al emisor y receptor de la información.

**·TIPOS:**

**-Según su área de cobertura:**

**-WAN: Red de Área Amplia (Wide Area Network)**

Son redes que se extienden sobre un área geográfica extensa (permite la interconexión entre continentes y países). Contiene una colección de máquinas dedicadas a ejecutar programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro. Estas LAN de host acceden a la subred de la WAN por un router.

Estas redes están formadas por líneas de comunicación (mueven los bits de una máquina a otra), elementos de con (routers).

Una WAN contiene numerosos cables conectados a un par de conmutadores.

**-MAN: Red de Área Metropolitana (Metropolitan Area Network)**

Una red MAN es aquella que, a través de una conexión de alta velocidad, ofrece cobertura en una zona geográfica extensa (como una ciudad o un municipio).

Con una red MAN es posible compartir todo tipo de datos y supone un avance a partir de la red LAN.

Una red de área metropolitana puede ser pública o privada. Un ejemplo de MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores público. Por su parte, un ejemplo de MAN pública sería la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de internet a ella.

**-LAN:**

Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión (por ejemplo la red del instituto). La utilizamos para conectar computadoras privadas con el objetivo de compartir recursos o intercambiar información.

**-PAN: Wireless Personal Area Network:**

En este tipo de **red de cobertura personal**, existen tecnologías basadas en **HomeRF** (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); **Bluetooth**; **ZigBee** ( utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); **RFID** (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio y Piconet.

El alcance típico de este tipo de redes es de unos cuantos metros, alrededor de los 10 metros máximo. La finalidad de estas redes es comunicar cualquier dispositivo personal (ordenador, terminal móvil, PDA, etc.) con sus periféricos, así como permitir una comunicación directa a corta distancia entre estos dispositivos.

-La tecnología **HomeRF**, basada en el protocolo de acceso compartido, Shared Wireless Access Protocol (SWAP), encamina sus pasos hacia la conectividad sin cables dentro del hogar. Los principales valedores de estos sistemas se agrupan en torno al consorcio que lleva

su mismo nombre, HomeRF, teniendo a Proxim, una filial de Intel, como el miembro que más empeño está poniendo en la implantación de dicho estándar.

el HomeRF Working Group (HRFWG) es un grupo de compañías encargadas de proporcionar y establecer un cierto orden en el océano tecnológico, obligando a que los productos fabricados por las empresas integrantes de este grupo tengan una plena interoperabilidad *(habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada*). En sí, la especificación SWAP define una nueva y común interfaz inalámbrica que está diseñada para poder soportar tanto el tráfico de voz como los servicios de datos en redes LAN dentro de los entornos domésticos e interoperar con las redes públicas de telefonía e Internet. Esta nueva normativa ha sido definida para asegurar la interoperatividad de una numerosa cantidad de productos con capacidades de comunicación sin hilos que se desarrollan para ordenadores para el mercado doméstico. Esta especificación permitirá que los ordenadores, periféricos, teléfonos y electrodomésticos puedan comunicarse con otros dispositivos de similar naturaleza sin la obligada presencia de los molestos cables de interconexión.

**-Bluetooth** es una especificación industrial para Redes Inalámbricas de Área Personal (WPAN) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2.4 GHz. Los principales objetivos que se pretenden conseguir con esta norma son: facilitar las comunicaciones entre equipos móviles, eliminar los cables y conectores entre éstos y ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre equipos personales. Los dispositivos que con mayor frecuencia utilizan esta tecnología pertenecen a sectores de

las telecomunicaciones y la informática personal, como PDA, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras o cámaras digitales.
Para conectar dos aparatos con esta tecnología, hay que proceder al "emparejamiento". Ambos aparatos van a reconocerse en respuesta a una llamada de uno hacia el otro y en respuesta a un envío de un código común.
Se pueden dar dos casos posibles: el código es enviado por ambos aparatos o el código es enviado por uno de ellos, especialmente cuando el segundo no tiene teclado.
Luego de que el primer contacto se efectúe, los códigos son memorizados y la conexión se hace automáticamente

**-ZigBee** es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radiodifusión digital de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal area network, WPAN).
Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías. En principio, el ámbito donde se prevé que esta tecnología cobre más fuerza es en domótica, como puede verse en los documentos de la ZigBee Alliance, en las referencias bibliográficas que se dan más abajo en el documento «ZigBee y Domótica». La razón de ello son diversas características que lo diferencian de otras tecnologías, como su bajo consumo, su topología de red en malla o su fácil integración (se pueden fabricar nodos con muy poca electrónica).

**-RFID** (siglas de Radio Frequency IDentification, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID.

El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID (automatic identification, o identificación automática).

Las etiquetas RFID (RFID Tag, en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor. En la actualidad, la tecnología más extendida para la identificación de objetos es la de los códigos de barras. Sin embargo, éstos presentan algunas desventajas, como la escasa cantidad de datos que pueden almacenar y la imposibilidad de ser reprogramados. La idea mejorada constituyó el origen de la tecnología RFID; consistía en usar chips de silicio que pudieran transferir los datos que almacenaban al lector sin contacto físico, de forma equivalente a los lectores de infrarrojos utilizados para leer los códigos de barras

**-**Una **Piconet** es una red formada por dispositivos móviles utilizando tecnología Bluetooth. Es una derivación de WPAN. Formada por dos a siete dispositivos, la Piconet sigue una estructura de maestro - esclavo, donde el maestro es el que proporciona la conexión mediante

un request que envía el esclavo, el maestro al establecer la conexión, define en que frecuencia va a trabajar. Tiene un alcance máximo de 10 metros y puede aumentar juntando varias piconets formando una Scatternet, donde un nodo esclavo hace a su vez el rol de un maestro proporcionado conexión a demás esclavos.

**-Según su tipología:**

**-Bus:**

En la topología de bus todos los nodos (computadoras) están conectados a un circuito común (bus).

La información que se envía de una computadora a otra viaja directamente o indirectamente, si existe un controlador que enruta los datos al destino correcto. La información viaja por el cable en ambos sentidos a una velocidad aproximada de 10/100 Mbps y tiene en sus dos extremos una resistencia (terminador). Se pueden conectar una gran cantidad de computadores al bus, si un computador falla, la comunicación se mantiene, no sucede lo mismo si el bus es el que falla. El tipo de cableado que se usa puede ser coaxial, par trenzado o fibra óptica.

**-Anillo:**

En la topología de anillo los nodos computadoras (nodos) están conectadas a la siguiente, formando un anillo. Cada computadora tiene una dirección única.

Cuando un mensaje es enviado, este viaja a través del lazo de computadora en computadora. Cada una de ellas examina la dirección de destino. Si el mensaje no está direccionado a ella, reenvía el mensaje a la próxima computadora, y así hasta que el mensaje encuentre la computadora destino. Si se daña el cable, la comunicación no es posible**.**

**-Estrella:**

Una red en estrella es una red de computadoras donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto (conmutador, repetidor o concentrador). Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central "activo" que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo para redes locales (LAN). La mayoría de las redes de área local que tienen un conmutador (*switch*) o un concentrador (*hub*) siguen esta topología. El punto o nodo central en estas sería el *switch* o el *hub*, por el que pasan todos los paquetes de usuarios.

Es la topología utilizada por la plataforma de Google.

**-Árbol:**

La red en árbol es una topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. Es una variación de

la red en bus, el fallo de un nodo no implica una interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones.

La topología en árbol puede verse como una combinación de varias topologías en estrella. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en esta topología las ramificaciones se extienden a partir de un punto raíz (estrella), a tantas ramificaciones como sean posibles, según las características del árbol.

Los problemas asociados a las topologías anteriores radican en que los datos son recibidos por todas las estaciones sin importar para quién vayan dirigidos. Es entonces necesario dotar a la red de un mecanismo que permita identificar al destinatario de los mensajes, para que estos puedan recogerlos a su arribo. Además, debido a la presencia de un medio de transmisión compartido entre muchas estaciones, pueden producirse interferencia entre las señales cuando dos o más estaciones transmiten al mismo tiempo.

**-Híbrida:**

En la topología híbrida o topología mixta las redes pueden utilizar diversas topologías para conectarse.

La topología mixta es una de las más frecuentes y se deriva de la unión de varios tipos de topologías de red, de aquí el nombre de “híbridas” o “mixtas”.

Ejemplos de topologías mixtas: en árbol, estrella-estrella, bus-estrella, etc.

Su implementación se debe a la complejidad de la solución de red, o bien al aumento en el número de dispositivos, lo que hace necesario establecer una topología de este tipo. Las topologías mixtas tienen un costo muy elevado debido a su administración y mantenimiento, ya que cuentan con segmentos de diferentes tipos, lo que obliga a invertir en equipo adicional para lograr la conectividad deseada.

**-Según su nivel de acceso o seguridad:**

**-Red pública:**

Las redes públicas proporcionan servicios de telecomunicaciones a cualquier usuario que pague una cuota. El usuario o suscriptor puede ser un individuo, una empresa, una organización, una universidad, un país, etcétera.

El término público se refiere a la disponibilidad del servicio para todos en general, no se refiere a la privacidad de la información. Cabe mencionar que los PST se rigen por regulaciones que varían de país a país para proteger la privacidad de los datos de los usuarios.

Ejemplos de compañías operadoras que ofrecen su red pública de telecomunicaciones son: telefonía fija, telefonía celular, televisión por cable, televisión por satélite, radio por satélite, etcétera.

Ejemplos de redes públicas, de acceso abierto que no cobran cuota alguna al usuario, son las radiodifusoras de radio AM y FM, así como las televisoras en UHF y VHF. Este tipo de

empresas también tienen una concesión del Estado para operar y difundir señales, y se mantienen por el cobro de tiempo a sus anunciantes.

**-Red privada:**

Una red privada es administrada y operada por una organización en particular. Generalmente, los usuarios son empleados o miembros de esa organización, aunque, el propietario de la red podrá dar acceso a otro tipo de usuarios que no pertenecen a la institución pero que tienen ciertos privilegios. Una universidad, por ejemplo, puede constituir una red privada, sus usuarios son estudiantes, maestros, investigadores, administrativos, etc. Personas ajenas a estas organizaciones no tendrán acceso a los servicios. Una red privada también podrá ser usuaria de los servicios de una red pública, pero seguirá siendo una red restringida a usuarios autorizados.

Una red privada pura es aquella que no utiliza los servicios de terceros para interconectarse, sino sus propios medios. En cuestiones de seguridad, podría decirse que una red privada es más segura debido a que la información no está tan expuesta más que en sus propias premisas, pero cuando esta red privada hace uso de una red pública para algunos servicios, la seguridad está comprometida. Muchas veces se hace uso de esquemas de encriptación para hacer que los datos se transporten de una manera segura. Un ejemplo de esto, son las redes

privadas virtuales VPN (Virtual Private Network), las cuales usan redes redes públicas bajo ciertos mecanismos de seguridad para el manejo de su información.

Una red pública (PST) puede suministrar a una compañía servicios para establecer una red privada que interconecte mediante enlaces a una o más entidades o sucursales de esa misma empresa; en otras palabras, los PST están autorizados para brindar a sus usuarios opciones servicios de telecomunicaciones para establecer redes privadas.

No hay que confundir las redes privadas y públicas respecto a las direcciones de Internet IP (Internet Protocol), las cuales explicaremos más adelante. Una red privada puede tener en sus nodos direcciones IP públicas o privadas. El concepto de red pública o privada se refiere a quienes (usuarios) tienen acceso a sus servicios en particular.

**-VPN (red privada virtual):**

Una red privada virtual (RPV), en inglés: *Virtual Private Network* (VPN), es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública, que permite que la computadora envíe y reciba datos como si se tratase de una red privada con toda su fun

Un ejemplo es la posibilidad de conectar diferentes sucursales de una empresa a través de internet.

La conexión VPN a través de Internet es técnicamente una unión *wide area network* (WAN) entre los sitios pero *al usuario le parece* como si fuera un enlace privado— de allí la designación "virtual private network".

**-SEGÚN SU RELACIÓN FUNCIONAL**

**-Relación cliente servidor:**: La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que la información se reparte entre los proveedores de servicios, llamados servidores y los demandantes, llamados clientes. Un cliente realiza peticiones a otro programa, el servidor, quien le da respuesta. En esta relación, el servidor no se ejecuta necesariamente sobre una sola máquina ni es necesariamente un solo programa.

**-Relación P2P:**

Una red p2p (peer to peer o redes entre pares o iguales) es una red que conecta un gran número de ordenadores (nodos) para compartir cualquier cosa que este en formato digital (videos, música etc.)

La conexión entre nodos se realiza de forma aleatoria y basándose en el ancho de banda. Los nodos de las redes P2P realizan la función de cliente2 y servidor3 al mismo tiempo con respecto al resto de nodos de la red.

**-SEGÚN SU TECNOLOGÍA FÍSICA DE CONSTRUCCIÓN:**

**- Redes cableadas:**

Definimos estas cómo las redes que conectan dos o más ordenadores mediante un cable.

- **Fast Ethernet:**

Denominamos Fast Ethernet o Ethernet de alta velocidad a una serie de estándares de IEEE de redes Ethernet de 100 Mbps (megabits por segundo). El nombre Ethernet procede del concepto físico de *ether*. Se le agregó el prefijo *fast* para diferenciarla de la versión original Ethernet de 10 Mbps.

Las redes tradicionales operaban entre 4 y 16 Mbps. Más del 40 % de todos los ordenadores están conectados a Ethernet. Tradicionalmente Ethernet trabajaba a 10 Mbps.

Fast Ethernet no es hoy en día versión más rápida de Ethernet, siendo actualmente Gigabit Ethernet y 10 Gigabit Ethernet (las dos siguientes) las más veloces.

- **Gigabit Ethernet:**

Gigabit Ethernet (GigaE), es una ampliación del estándar Ethernet, que consigue una capacidad de transmisión de 1 gigabit por segundo, correspondientes a unos 1000 megabits por segundo de rendimiento contra unos 100 de Fast Ethernet.

- **10 Gigabit Ethernet:**

10-gigabit Ethernet (XGbE o 10GbE) es el más reciente es el estándar Ethernet más rápido y reciente(2002). IEEE 802.3 se define una versión de Ethernet con una velocidad nominal de 10 Gbit/s, diez veces más rápido que gigabit Ethernet.

El estándar 10 Gigabit Ethernet contiene siete tipos de medios para LAN, MAN y WAN.

**-Redes inalámbricas:**

## LA RED INTERNET

### - Orígenes de internet

Los orígenes de internet se remontan hasta la década de los 60, dento de ARPA (hoy DARPA, siglas que en inglés significan Defense Advanced Research Projects Agency), creada como respuesta a la necesidad de la incansable de buscar mejores maneras de usar los computadores. Pero su verdadero orígen sería con ARPANet (Advanced Research Projects Agency Network) en castellano, red para los proyectos de investigación avanzada de Estados Unidos, quien creó la red individual de comunicaciones de alta velocidad, a la cual se fueron integrando paulatinamente otras instituciones gubernamentales y redes académicas en la década de los 70.

En julio de 1961, Leonard Kleinrock publicó desde el MIT (Massachusetts Institute of Technology) el primer documento sobre la teoría de conmutación de paquetes. Este convencería a Lawrence Robertsde la factibilidad teórica de las comunicaciones vía paquetes en lugar de circuitos, lo cual resultó ser un gran avance en el camino hacia el trabajo informático en red.

Tras este “gran avance” vendría otro aún más mayor, en 1965, cuando Roberts conectó una computadora TX2 (en Massachusetts) con un Q-32 (en California) con una línea telefónica conmutada de baja velocidad, creando así la primera y mayor red de computadoras construida hasta entonces.

- **1969**

  Nace la primera red interconectada, cuando se crea el primer enlace entre las universidades de UCLA y Stanford por medio de la línea telefónica conmutada, a pesar del mito de que ARPANET, la primera red, se construyó simplemente para

sobrevivir a ataques nucleares sigue siendo muy popular, este no fue el único motivo, si bien es cierto que ARPANET fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables.

- **1972**

  Se realiza la Primera demostración pública de ARPANET, que funcionaba de forma distribuida sobre la red telefónica conmutada. Este éxito sirvió para que, la DARPA (Defense Advanced Research Projects Agency) iniciara un programa de investigación sobre posibles técnicas para interconectar redes de distintas clases. Fin para el que se desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas.

- **1983**

  ARPANET cambia el protocolo NCP por TCP/IP. Ese mismo año, se creó el IAB (Internet service provider) con el fin de estandarizar el protocolo TCP/IP y de proporcionar recursos de investigación a Internet.

- **1986**

  La NSF (National Science Foundation) comenzó el desarrollo de NSFNET (National Science Foundation's N**et**work) que se convertiría en la principal *Red en árbol* de Internet. Paralelamente, otras redes troncales en Europa, tanto públicas como comerciales, junto con las americanas formaban el esqueleto básico ("backbone") de Internet.

- **1989**

  Con la integración de los protocolos OSI (Open System Interconnection) en la arquitectura de Internet, se inició la interconexión de redes de estructuras dispares, además de facilitar el uso de distintos protocolos de comunicaciones.

  El CERN (Conseil Européen pour la Recherche Nucléaire) de Ginebra, creó el lenguaje HTML (HyperText Markup Language), basado en el SGML (Standard Generalized Markup Language).

- **1990**

  El mismo equipo (CERN) construyó el primer cliente Web, llamado WorldWideWeb (WWW), y el primer servidor web.

  En los inicios de los 90, con la introducción de nuevas facilidades de interconexión y herramientas gráficas simples para el uso de la red, se inició el auge de Internet. Auge que trajo consigo un nuevo perfil de usuarios, mayoritariamente personas comunes, que ninguna relación guardaban con los sectores académicos, científicos y/o gubernamentales.

  Lo que conllevó a cuestionar la subvención del gobierno estadounidense para el sostenimiento y la administración de la red, así como la prohibición del uso comercial del Internet. Los hechos se sucedieron rápidamente y para 1993 ya se había levantado la prohibición al uso comercial del Internet y alcanzado la transición hacia un modelo de administración no gubernamental que permitiese, la integración de redes de acceso privado. A finales de abril de 1993 la Web entró al dominio público, ya que el CERN entregó las tecnologías de forma gratuita para que cualquiera pudiera utilizaras.

- **2006**

  En este año, Internet alcanzó los mil cien millones (1.100.000.000) de usuarios y la previsión es que en diez años, la cantidad de navegantes de la Red aumente a dos mil millones (2.000.000.000).

**- Servicios de Internet**

- **La World Wide Web (WWW)**

  Servicio mediante el que accedemos a la información organizada en bloque, también llamadas páginas Web.

  Las características de la www son:

  - Información muy abundante sobre cualquier temática.
  - Las páginas web son archivos que pueden incorporar elementos multimedia: imágenes estáticas, animaciones, sonidos o vídeos.
  - Navegar por ellas es muy fácil, simplemente empleando un ratón, basta con hacer clic sobre elementos que aparecen resaltados en la pantalla (hipertextos o hiperenlaces).
  - Permiten el acceso a archivos situados en equipos remotos.

- **El correo electrónico**

  Servicio mediante el que podemos enviar y recibir mensajes escritos entre usuarios de una red informática.

  Es uno de los servicios más antiguos y extendidos de Internet. Se pueden añadir, también, archivos de todo tipo a los mensajes: documentos escritos con un procesador de textos, imágenes, etc.

La gran mayoría de los usuarios de Internet emplean este servicio que permite la comunicación con otras personas que habitan en regiones diferentes del planeta con un coste reducido.

- **El servicio de conversación en línea**

  Servicio mediante el que podemos comunicarnos al instante con otro usuario.

  Si en el correo electrónico no hacía falta que los dos interlocutores estuviesen conectados al mismo tiempo para recibir los mensajes, en el servicio de conversación en línea, si es necesario. Sin embargo, existen en Internet muchos otros servicios que sí permiten la comunicación simultánea, véanse los ejemplos de Skype, Facebook, Twitter y un largo etcétera.

- **El control remoto de equipos**

  Este servicio permite controlar un ordenador desde un lugar distante, sin sentarnos necesariamente delante del mismo.

  Facilita, este servicio, por ejemplo, el acceso al ordenador de un empleado desde la sede de la empresa en otra ciudad.

- **La videoconferencia**

  Servicio que permite la comunicación entres dos usuarios de la red de forma visual y sonora simultánea, servicio muy usado, por ejemplo, para las familias que viven en distintos países o continentes, además de ser usado con fines laborales, como las videoconferencias que cada vez son más habituales.

- **La transferencia de archivos**

  Servicio por excelencia de internet y uno de los más antiguos, utilizado desde el momento de su creación hasta la actualidad, desde la creación de Drive, un servicio

de Google, la transferencia de archivos a aumentado su calidad e hizo su accesibilidad más práctica.

En algunos casos, los archivos almacenados se protegen con una contraseña, de manera que sólo los usuarios autorizados pueden manipularlos.

- **La web**

La World Wide Web (WWW) o red informática mundial es un sistema de distribución de documentos de hipertexto o hipermedios interconectados y accesibles vía Internet. Podemos visualizar con un navegador web, sitios web compuestos de páginas web que pueden contener textos, imágenes, vídeos u otros contenidos multimedia.

La Web se desarrolló entre los años 1989 y 1990 por el inglés Tim Berners-Lee y el belga Robert Cailliau mientras trabajaban en el CERN (Consejo Europeo para la Investigación Nuclear) en Ginebra, Suiza, y hecho público en 1992. Tim Berners-Lee, científico de la computación y en ese momento empleado del CERN, escribió una propuesta destinada a un sistema de comunicación de la CERN, con lo que se convertiría en la World Wide Web, dándose cuenta más tarde de que el concepto podría aplicarse en todo el mundo. Berners-Lee y Robert Cailliau propusieron utilizar el hipertexto "para vincular y acceder a información de diversos tipos como una red de nodos en los que el usuario puede navegar a voluntad", y Berners-Lee terminó el primer sitio web.

- **Evolución de la web**

- **Web 1.0 o web estática**

Web 1.0 es en general un término usado para describir la Web antes del impacto de la «fiebre punto com» en 2001, que es considerado el momento en que el internet dio un giro.

El concepto Web 1.0 surgió simultáneamente al de Web 2.0, y se usa en relación con el segundo para la comparación de ambos.

Algunas características de la Web 1.0:

- Páginas estáticas.
- El uso de framesets.
- Extensiones propias del HTML como <blink> y <marquee>, etiquetas introducidas durante la guerra de navegadores web.
- Libros de visitas en línea.
- Botones GIF, casi siempre con una resolución de 88x31 píxeles, para promocionar navegadores web u otros productos.
- Formularios HTML enviados vía correo electrónico. Un usuario llenaba un formulario y después de hacer clic se enviaba a través de un cliente de correo electrónico, con el inconveniente de que en el código se podía observar los detalles del envío del correo electrónico.
- No se podían añadir comentarios.
- Todas sus páginas se creaban de forma fija y muy pocas veces se actualizaban.
- No se trata de una nueva versión, sino de una nueva forma de ver las cosas.

- **Web 2.0 o web social**

La Web 2.0 o Web Social comprende aquellos sitios web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web.

Permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual.

Algunas características de la Web 2.0:

- El auge de los blogs.
- El auge de las redes sociales.
- Las webs creadas por los usuarios, usando plataformas de auto-edición.
- El contenido agregado por los usuarios como valor clave de la Web.
- El etiquetado colectivo.
- La importancia del *long tail*.
- El beta perpetuo: la Web 2.0 se inventa permanentemente.
- Aplicaciones web dinámicas.
- La World Wide Web como plataforma.
- Crear entornos lúdicos multimedia y reproducirlos en grupos.
- Crear un sistema de puntuación de actividades y logros de objetivos.
- Crear un sistema que estimule la adquisición de conocimientos.
- Crear sistemas colaborativos para alcanzar logros comunes y que sean puntuados.
- Crear sistemas de refuerzo positivos entre los componentes del grupo cuando uno de ellos alcanza un logro.

**Web 3.0 o web semántica**

Web 3.0 es una expresión que se utiliza para describir la evolución del uso y la interacción de las personas en internet a través de diferentes formas cómo la transformación de la red en una base de datos, un movimiento social con la finalidad de crear contenidos accesibles por múltiples aplicaciones *non-browser* (sin navegador), el empuje de las tecnologías de inteligencia artificial, la web semántica, la Web Geoespacial o la Web 3D.

Algunas características de la Web 3.0:

- Bases de datos.
- Inteligencia artificial.
- Web semántica y SOA.
- Evolución al 3D.

**-TECNOLOGÍAS DE ACCESO A INTERNET**

**-Acceso cableado:**

Son aquellos accesos que requieren una conexión por medio de un cable hasta el terminal del usuario, por lo que el usuario se ubica en una posición fija. Este es el caso de servicios de banda ancha domésticos.Estos accesos se basan en las tecnologías xDSL, HFC o la fibra óptica del hogar, entre otras.

**-Acceso inalámbrico.**

Son aquellos que no requieren una conexión por cable hasta el terminal del usuario, dado que la comunicación se produce de forma inalámbrica, pero que requieren que el usuario esté a una distancia del punto de acceso no superior al alcance del mismo.

Este tipo de accesos normalmente suplen o complementan a los accesos cableados, sustituyendo el último tramo de cable que conecta el terminal de usuario a la red, por un enlace inalámbrico, como sucede en las redes Wi-Fi domésticas. Estos accesos, aunque dan cierta movilidad al usuario, ésta no es total, ya que está limitada a una zona concreta que depende de la cobertura del punto inalámbrico de acceso. Entre las tecnologías de este tipo se encuentran la tecnología WI-FI, la WiMAX y la vía satélite.

**-Acceso móvil:**

El acceso móvil a internet se basa en el conjunto de contenidos, servicios y aplicaciones específicamente diseñados para usuarios móviles, independientemente de la plataforma móvil. Las primeras conexiones se efectuaban mediante una llamada telefónica a un número del operador, a través del cual se trasmitían los datos. Posteriormente, nació el GPRS (o 2G), que permitió acceder a Internet a través del protocolo TCP/IP. La velocidad del GPRS es de 54 kbit/s en condiciones óptimas. Otras tecnologías más recientes permiten el acceso a Internet con banda ancha, como son EDGE, EV-DO, HSPA y 4G.

**-Línea telefónica:**

- **RTC:** Es la red de telecomunicaciones que básicamente sirve de soporte para la transferencia de audio entre terminales situados en ubicaciones fijas. La RTC utiliza la conmutación de circuitos entre las dos ubicaciones. En cada extremo el usuario coloca su teléfono al punto de terminación de red. En ese punto se inicia la red de acceso que lo conecta con una central telefónica. El transporte de información entre centrales se realiza mediante redes de transporte.

- **RDSI:** Red que procede por evolución de la Red Digital Integrada (RDI). La Línea RDSI es la mejor solución para combinar flexiblemente diferentes tipos de comunicaciones (voz, datos, Internet, fax, videoconferencia) a través de una única línea. Un Acceso Básico RDSI se compone de 2 canales de comunicación de alta velocidad
- **ADSL:** ADSL es una clase de tecnología que permite la conexión a Internet mediante el uso de la línea telefónica tradicional. Así, el usuario se conecta a la red utilizando su línea telefónica, pero con banda ancha.

**-Cable o HFC:** En el mundo de la tecnología este tipo de red en telecomunicaciones está incorporada dos tipos de cableado que son la fibra óptica y coaxial, formándose una red poderosa de banda ancha, en la cual pude tener una capacidad del ancho de banda de 1 gigaherts, esto ayuda a las compañías grandes operadoras de cables a cubrir grandes distancias de cierta región geográfica ya que puede transportar sus datos por fibra óptica y luego la pasan a cableado coaxial, les permite al cliente tener una experiencia memorable no solo de cable sino también de Internet y voz **.** Su función comienza en el nodo Híbrido que transforma las señales análogas a digitales y viceversa. Sus frecuencias de radio son trasmitidas desde la línea coaxial que transforma en datos que son enviados por la línea de fibra óptica, de ahí son trasmitidos por un cable CMTS y son convertidos en una señal análoga hasta la línea de cobre compartido.

- **Fibra óptica hasta el hogar**

La tecnología de telecomunicaciones FTTH (*Fiber To The Home*), también conocida como fibra hasta la casa o fibra hasta el hogar, se basa en la utilización de cables de fibra óptica y sistemas de distribución ópticos adaptados a esta tecnología para la distribución de servicios avanzados, como la telefonía, el Internet de banda ancha y la televisión, a los hogares y negocios de los abonados.

La implantación de esta tecnología es cada mayor, especialmente en países como España, Estados Unidos, Colombia, Uruguay, Japón y países de Europa, donde muchos operadores reducen la promoción de servicios ADSL en beneficio de la fibra óptica con el objetivo de proponer servicios muy atractivos de banda ancha para el usuario (música, vídeos, fotos, etc.)

- **Internet por satélite**

Internet por satélite es el producto idóneo para todas aquellos que tienen una necesidad de acceso a Internet en una zona en la que no hay cableado ni de Fibra óptica ni ADSL, y por lo cual no tienen posibilidad de tener una conexión de acceso a Internet de Banda Ancha en dicha ubicación.

Con Internet por satélite los usuarios tienen plena garantía de que tendrán conectividad a Internet donde quiera que esté su lugar de conexión, ya que, es el único producto de acceso a Internet con una cobertura del 100%.

Para poder utilizar este producto, se instala una antena parabólica junto con un modem que permiten alcanzar unas velocidades de navegación de banda ancha de muy buena calidad.

- **WIMAX y LMDS**

WiMAX trabaja en la banda de 2 a 11 GHz. Una de las consecuencias principales es que WiMAX puede trabajar tanto sin visibilidad directa, como con visibilidad directa. Otra diferencia fundamental es la capacidad de WiMAX de adaptarse a las condiciones variables del medio, mediante mecanismos de control de potencia emitida, modulación adaptativa y selección automática de frecuencia que permiten una combinación de abasto y de velocidad de transmisión de datos superior.

LMDS (Local Multipont Delivery Service) es una tecnología inalámbrica de acceso a la banda ancha. Trabaja en la banda de 25 GHz y superiores, según las regulaciones locales aplicables. Las radiocomunicaciones en la banda de 25 GHz necesitan visibilidad directa entre antenas. El abasto del servicio LMDS, viene limitado por las características del medio y las exigencias de disponibilidad contratadas, entre otros factores técnicos. Se puede hablar de distancias máximas entre 2,5 Km. y 14 Km, aunque las utilizaciones típicas de LMDS acostumbran a cubrir distancias de entre 3 y 5 Km., con un grado de disponibilidad muy alto.

- **Red eléctrica**

- **Conexión por telefonía móvil**

    - **Primera generación, 1G**

1G (o 1-G) es la abreviación para la telefonía móvil de la primera generación. Estos teléfonos utilizan tecnología digital y fueron lanzados en los años 80. La mayor diferencia entre el 1G y el 2G es que el 1G es analógico y el 2G es digital; aunque los dos sistemas usan sistemas digitales para conectar las Radiobases al resto del sistema telefónico, la llamada es cifrada cuando se usa 2G.

    - **Segunda generación, 2G**

Se conoce como telefonía móvil 2G a la segunda generación de telefonía móvil.

La telefonía móvil 2G no es un estándar o un protocolo sino que es una forma de marcar el cambio de protocolos de telefonía móvil analógica a digital.

La llegada de la segunda generación de telefonía móvil fue en los años 90 y su desarrollo deriva de la necesidad de poder tener un mayor manejo de llamadas en prácticamente los mismos espectros de radiofrecuencia asignados a la telefonía móvil, para esto se introdujeron protocolos de telefonía digital que además de permitir más enlaces simultáneos en un mismo ancho de banda, permitían integrar otros servicios, que anteriormente eran independientes, en la misma señal, como es el caso del envío de mensajes de texto o *página* en un servicio denominado *Short Message Service* (SMS) y una mayor capacidad de envío de datos desde dispositivos de fax y módem.

2G abarca varios protocolos distintos desarrollados por varias compañías.

- **Tercera generación, 3G**

3G es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (*Universal Mobile Telecommunications System* o servicio universal de telecomunicaciones móviles).

Los servicios asociados con la tercera generación proporcionan la posibilidad de transferir voz y datos no-voz (como la descarga de programas, intercambio de correos electrónicos, y mensajería instantánea).

- **Cuarta generación, 4G**

En telecomunicaciones, 4G son las siglas utilizadas para referirse a la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y precede a la próxima generación, la 5G.

Al igual que en otras generaciones, la Unión Internacional de Telecomunicaciones (UIT) creó un comité para definir las especificaciones. Este comité es el IMT-Advanced y en él se definen los requisitos necesarios para que un estándar sea considerado de la generación 4G. Entre los requisitos técnicos que se incluyen hay uno muy claro: las velocidades máximas de transmisión de datos deben estar entre 100 Mbit/s para una movilidad alta y 1 Gbit/s para movilidad baja.

**-SEGURIDAD EN LA RED:**

**-Confidencialidad:**

Es la propiedad que consiste en prevenir la divulgación de información a personas o sistemas no autorizados, es decir, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización.

Por ejemplo, una transacción realizada con una tarjeta de crédito en Internet requiere que el número de tarjeta de crédito es transmitida desde el comprador al comerciante, y del comerciante a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta de algún modo, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro mientras hay información confidencial en la pantalla,

cuando se publica información privada, cuando un ordenador con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Para garantizarla se utilizan mecanismos de cifrado y de ocultación de la comunicación. Digitalmente se puede mantener la confidencialidad de un documento con el uso de llaves asimétricas. Los mecanismos de cifrado garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje. Por esta razón, es necesario determinar durante cuánto tiempo el mensaje debe seguir siendo confidencial. No existe ningún mecanismo de seguridad absolutamente seguro.

**-Autentificación:**

La autenticación es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real. La autenticación de un objeto puede significar (pensar) la confirmación de su procedencia, mientras que la autenticación de una persona a menudo consiste en verificar su identidad en función de uno o varios factores.

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades identificadas con un identificador único (valga la

redundancia). Existen diferentes formas para autentificar una cuenta o usuario en la actualidad, siendo las más comunes las siguientes:

**·Autenticación clásica**

En un sistema Unix habitual cada usuario posee un nombre de entrada al sistema o login y una clave o password; ambos datos se almacenan generalmente en el fichero /etc/passwd. Este archivo contiene una línea por usuario donde se indica la información necesaria para que los usuarios puedan conectar al sistema y trabajar en él, separando los diferentes campos mediante ':'.

Al contrario de lo que mucha gente cree, Unix no es capaz de distinguir a sus usuarios por su nombre de entrada al sistema. Para el sistema operativo lo que realmente distingue a un usuario de otro es el UID del usuario en cuestión; el login es algo que se utiliza principalmente para comodidad de las personas.

Para cifrar las claves de acceso de sus usuarios, el sistema operativo Unix emplea un criptosistema irreversible que utiliza la función estándar de C crypt, basada en el algoritmo DES. Para una descripción exhaustiva del funcionamiento de crypt. Esta función toma como clave los ocho primeros caracteres de la contraseña elegida por el usuario (si la longitud de ésta es menor, se completa con ceros) para cifrar un bloque de texto en claro de 64 bits puestos a cero; para evitar que dos passwords iguales resulten en un mismo texto cifrado, se realiza una permutación durante el proceso de cifrado elegida de forma automática y aleatoria para cada usuario, basada en un campo formado por un número de 12 bits (con lo que conseguimos 4096 permutaciones diferentes) llamado *salt*. El cifrado resultante se vuelve a cifrar utilizando la contraseña del usuario de nuevo como clave, y permutando con el mismo salt, repitiéndose el proceso 25 veces. El bloque cifrado final, de 64 bits, se concatena con dos

bits cero, obteniendo 66 bits que se hacen representables en 11 caracteres de 6 bits cada uno y que, junto con el salt, pasan a constituir el campo password del fichero de contraseñas, usualmente /etc/passwd. Así, los dos primeros caracteres de este campo estarán constituidos por el salt y los 11 restantes por la contraseña cifrada.

Este modo de cifrado tiene diversos problemas, siendo el más común que las contraseñas, aunque indescifrables, mediante un programa crackeador que encripta palabras aleatorias sacadas de un diccionario, se pueden comparar los resultados, de forma que aparecerá una contraseña idéntica a la contraseña original.

**Shadow Password**

Otro método cada día más utilizado para proteger las contraseñas de los usuarios el denominado Shadow Password u oscurecimiento de contraseñas. La idea básica de este mecanismo es impedir que los usuarios sin privilegios puedan leer el fichero donde se almacenan las claves cifradas.

**Envejecimiento de contraseñas**

En casi todas las implementaciones de Shadow Password actuales se suele incluir la implementación para otro mecanismo de protección de las claves denominado envejecimiento de contraseñas (Password Aging). La idea básica de este mecanismo es proteger los passwords de los usuarios dándoles un determinado periodo de vida: una contraseña sólo va a ser válida durante un cierto tiempo, pasado el cual expirará y el usuario deberá cambiarla.

Realmente, el envejecimiento previene más que problemas con las claves problemas con la transmisión de éstas por la red: cuando conectamos mediante mecanismos como telnet, ftp o rlogin a un sistema Unix, cualquier equipo entre el nuestro y el servidor puede leer los paquetes que enviamos por la red, incluyendo aquellos que contienen nuestro nombre de usuario y nuestra contraseña.

**Otros métodos**

Algo por lo que se ha criticado el esquema de autenticación de usuarios de Unix es la longitud, para propósitos de alta seguridad, demasiado corta de sus claves; lo que hace años era poco más que un planteamiento teórico, actualmente es algo factible: sin ni siquiera entrar en temas de hardware dedicado, seguramente demasiado caro para la mayoría de atacantes, con un supercomputador es posible romper claves de Unix en menos de dos días.

Un método que aumenta la seguridad de nuestras claves frente a ataques de intrusos es el cifrado mediante la función conocida como bigcrypt() o crypt16(), que permite longitudes para las claves y los salts más largas que crypt y sin embargo, aunque se aumenta la seguridad de las claves, el problema que se presenta aquí es la incompatibilidad con las claves del resto de Unices que sigan utilizando crypt; este es un problema común con otras aproximaciones que también se basan en modificar el algoritmo de cifrado, cuando no en utilizar uno nuevo.

**-Autorización:**

En ingeniería de seguridad y seguridad informática, la autorización es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello. Los recursos incluyen archivos y otros objetos de dato, programas, dispositivos y funcionalidades provistas por

aplicaciones. Ejemplos de consumidores son usuarios del sistema, programas y otros dispositivos.

El proceso de autorización se usa para decidir si la persona, programa o dispositivo X tiene permiso para acceder al dato, funcionalidad o servicio Y.

La mayoría de los sistemas operativos multiusuarios modernos incluyen un proceso de autorización. Éste hace uso del proceso de autenticación para identificar a los consumidores. Cuando un consumidor intenta usar un recurso, el proceso de autorización comprueba que al consumidor le ha sido concedido permiso para usar ese recurso. Los permisos son generalmente definidos por el administrador de sistemas en algún tipo de «aplicación de políticas de seguridad», Los sistemas operativos monousuarios más antiguos solían tener sistemas de autenticación y autorización débiles o carecían por completo de ellos.

Se llama «consumidores anónimos» o «invitados» a aquellos consumidores a los que no se les ha exigido que se autentiquen. A menudo tienen muy pocos permisos. En un sistema distribuido, suele ser deseable conceder acceso sin exigir una identidad única.

Existe también el concepto de consumidores «confiables» (*trusted*). Los consumidores que se han autenticado y a los que se señalan como confiables se les permite acceso ilimitado a los recursos. Los consumidores «parcialmente confiables» e invitados están sujetos a autorización para usar los recursos protegidos. Las aplicaciones de políticas de seguridad de algunos sistemas operativos, conceden por defecto a todos los consumidores acceso completo a todos los recursos. Otros hacen lo opuesto, insistiendo en que el administrador lleve a cabo acciones deliberadas para permitir a cada consumidor el uso de cada recurso.

**-Integridad:**

Para un encargado de seguridad, la “integridad de los datos” puede definirse como la imposibilidad de que alguien modifique datos sin ser descubierto. Desde la perspectiva de la seguridad de datos y redes, la integridad de los datos es la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria. Si examinamos el concepto de “integridad”, podríamos concluir que no solo alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurado, revisión de códigos fuente por expertos, pruebas exhaustivas, etc.), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etc.).

Los ataques a la integridad de los datos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida. En el contexto del presente artículo, el ciclo de vida de los datos comprende las siguientes etapas:

- Introducción, creación y/o adquisición de datos.
- Procesamiento y/o derivación de datos.
- Almacenamiento, replicación y distribución de datos.
- Archivado y recuperación de datos.
- Realización de copias de respaldo y restablecimiento de datos.
- Borrado, eliminación y destrucción de datos.

**-Amenazas a la seguridad:**

**-Causas humanas:**

Ya antes de la existencia de Internet, existían los denominados Auténticos Programadores, brillantes ingenieros, físicos o matemáticos que decidieron dedicarse al mundo de las computadoras y que acabaron convirtiéndose en auténticos prodigios de la informática. Con la llegada de Internet y los ordenadores domésticos, el número de personas que deciden dedicarse al mundo del ordenador ha aumentado, existiendo actualmente los siguientes tipos de personas que podrían poner en riesgo la seguridad de nuestro ordenador:

·**Hackers:** son expertos en sistemas avanzados, centrándose en la actualidad en sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica, y suelen entran en ordenadores ajenos a distancia, aunque no suelen modificar ni llevarse nada de ellos. Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen hacker sea finalmente contratado por alguna importante empresa de seguridad.

·**Crackers:** es aquel hacker fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas. Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección, pero el problema no radica ahí, sino en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros. En la actualidad es habitual ver como se muestran los cracks de la mayoría de software de forma gratuita a través de Internet.

·**Lamers:** está formado por personas que quieren ser hackers pero que carecen de los conocimientos necesarios. Este es el grupo más peligroso, ya que usan diferentes técnicas de

hackeo, que encuentran en la red, de forma indiscriminada y sin control, con el único fin de autodenominarse hackers, para posteriormente reírse de la víctima.

·**Phreaker:** posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo, también tienen amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es una parte primordial a tener en cuenta, y emplean la informática para su procesado de datos.

·**Newbie:** es, básicamente, un novato del hackeo que va aprendiendo poco a poco y sin mofarse de la gente, todo lo contrario que los lamers.

·**Script kiddie:** internautas que descargan programas de hackeo sin tener conocimiento alguno sobre el tema. Son muy similares a los lamers.

**-Causas lógicas:**

Este tipo de riesgo suele ser uno de los más peligrosos y difíciles de detectar, ya que al alterar el funcionamiento normal del sistema y no detectarse a tiempo puede provocar daños irreparables a la información, a los usuarios e incluso al sistema físico.

·**Ciberplagas:** A veces también se les denomina como software malintencionado. Abarcan un conjunto diverso de programas (virus, gusanos, caballos de Troya, etc.) cuyos objetivos son adueñarse del control del sistema operativo con el fin de provocar, en la mayoría de los casos,

la destrucción de la información u otros tipos de daños a los sistemas informáticos. Entre estos programas destacan:

***Virus:** programas que modifican o alteran los ficheros. Hay dos tipos de virus, los benignos y los malignos. Los primeros sólo producen efectos molestos como la superposición de mensajes (el virus Marihuana), movimiento de figuras (virus de la Pelotita) o transposición de los caracteres de la pantalla (virus de la cascada de letras), mientras que los malignos pueden borrar ficheros de datos o alterar el funcionamiento de los programas.

***Caballos de Troya o troyanos:** son instrucciones introducidas en la secuencia de instrucciones de otros programas legales (de ahí su nombre) y que realizan funciones no autorizadas, destruyen ficheros o capturan información mientras simulan efectuar funciones correctas.

***Gusanos o worms:** programa que simplemente se va duplicando y ocupando memoria hasta que su tamaño desborda al sistema informático en que se instala, impidiéndole realizar ningún trabajo efectivo.

***Electronic Mail Bombs:** son programas relacionados con el correo electrónico y permiten generar órdenes de envío de correos desde uno o varios orígenes a un solo destinatario, generando una gran cantidad de órdenes y mensajes, con el fin de bloquear su funcionamiento e impidiendo, por ejemplo, atender pedidos o responder consultas. A este efecto se le conoce como denegación de servicios.

**-Copias ilegales:** cada vez circulan más por la red todo tipo de programas que permiten la copia de otros programas, música, tarjetas de televisión, CDs, películas, etc. Todo ello ocasiona un fraude a los derechos de autor y a los beneficios de empresas editoras, cinematográficas, discográficas, de TV, etc., que se elevan a miles de millones anuales, y que ponen en peligro el futuro de algunos sectores económicos dedicados al ocio.

**-Causas físicas:**

**·Obsolescencia de los soportes de almacenamiento:** la rápida evolución de las tecnologías de almacenamiento (tarjetas perforadas, cintas magnéticas, casetes, discos magnéticos, discos compactos, etc.) implica que, al pasar el tiempo, la información grabada en un determinado soporte sea prácticamente irrecuperable al no disponerse de los sistemas de lectura adecuados. El trasvase de ingentes cantidades de información de un tipo de soporte a otro implica una gran cantidad de tiempo de sistema y elevados costes económicos, por lo que muchas veces no se hace.

**·Amenazas naturales:** las instalaciones de procesos de datos se encuentran sometidas a todo tipo de amenazas y catástrofes (terremotos, riadas, tormentas, incendios, etc.) que pueden provocar la interrupción del funcionamiento y, en muchos casos, la destrucción del sistema.

**·Problemas eléctricos y electromagnéticos:** los fallos del suministro eléctricos y las radiaciones electromagnéticas pueden alterar el funcionamiento de los equipos y los datos almacenados de forma magnética.

·**Sabotajes y actos terroristas:** la concentración de la información y el control de numerosos sistemas, (tráfico aéreo, ferroviario, comunicaciones, sistemas energéticos, etc.) en los centros de proceso de datos los hace especialmente vulnerables a este tipo de actos que buscan paralizar la sociedad. Por lo tanto los CPD se convierten en objetivos de primer orden para grupos revolucionarios o terroristas.

**-Legislación en la red:**

Para hacer de Internet un lugar más seguro, existen una serie de leyes que velan por nuestra seguridad. Entre ellas, destacan las siguientes:

·**LOPD (Ley Orgánica de Protección de Datos):** su objetivo es garantizar las libertades públicas y derechos de las personas físicas. Está regulada por la Agencia Española de Protección de Datos.

·**LPI (Ley de Protección de Datos):** sus objetivos son: conocer el marco jurídico español sobre la propiedad intelectual, afianzar conceptos y principios básicos relacionados con la propiedad intelectual, conocer las buenas prácticas de gestión del software como activo dentro de una organización y sensibilizar sobre las sanciones impuestas por la Administración para el cese de las actividades ilícitas respecto a los Derechos de Autor.

·**LSSICE (Ley de Servicios de la Sociedad de la Información y Comercio Electrónico):** La LSSICE se aplica al comercio electrónico y a otros servicios de Internet cuando sean parte

de una actividad económica. Establece unos criterios y medidas reguladoras aplicables a todas las actividades que realicen por medios electrónicos y tengan carácter comercial o persigan un fin económico. Se aplica tanto a las páginas web en las que realicen actividades de comercio electrónico como a aquellas se suministren información u ofrezcan servicios (incluso gratuitos) para los usuarios, cuando constituyan una actividad económica para el titular del sitio web.

**·LAECSP (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos):**
Su principal objetivo es reconocer y garantizar el derecho del ciudadano a relacionarse por medios electrónicos con las Administraciones Públicas. Por otra parte se pretende impulsar el uso de los servicios electrónicos en la Administración creando las condiciones necesarias, y de manera indirecta ejercer con ello un efecto arrastre sobre la sociedad de la información en general.

Debido a esto, las Administraciones Públicas tienen la obligación de posibilitar el acceso a todos sus servicios electrónicos, incluyendo registros, pago, notificaciones y la consulta del estado de tramitación de sus procedimientos desde el 31 de diciembre de 2009.

**·Ley de Firma Electrónica:** esta ley se encarga de definir los siguientes conceptos:

***Firma electrónica:** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

***Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de

manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

***Firma electrónica reconocida:** es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

**Adopción de medidas de seguridad**

- **Protección**

**-Antivirus:** Surgió en la misma época en la que comenzaron a detectarse los primeros "Virus de PC" en los 90. Hoy por hoy constituya en el producto básico de la seguridad informática, no se debe tener ningún equipo conectado a Internet sin ningún programa que ofrezca una buena protección contra programas malignos.

Un programa antivirus analiza información de muy diverso tipo, y en caso de que el sistema se encuentre infectado por algún código maligno procede a su desinfección o eliminación según la configuración que permita cada software.Cabe destacar que ell mecanismo de interceptación debe ser específico para cada sistema operativo o componente sobre el que se va a implantar el antivirus.

Preventores: Los programas que previenen la infección, quedan residentes en la memoria de la computadora todo el tiempo y monitorean algunas funciones del sistema.

Identificadores: Estos productos antivirus identifican programas malignos específicos que infectan al sistema.

Descontaminadores: Sus características son similares a los productos identificadores, con la diferencia que su principal función es descontaminar a un sistema que ha sido infectado, eliminando el programas malignos y retomando el sistema a su estado original por lo que tiene que ser muy preciso en la identificación de los programas malignos contra los que descontaminan.

Cada programa maligno tiene un código de "firma" que lo identifica, por lo cual es detectado por el antivirus. Algunos antivirus tienen la capacidad de detectar programas que no están en su base de datos. Esto se realiza por medio del sondeo del sistema en busca de síntomas clásicos de infección, como por ejemplo fechas extrañas en archivos, programas residentes en la memoria, una configuración extraña del sistema. El problema de esto es que puede dar "falsos positivos" es decir, puede dar por infectado un fichero que en realidad no lo está. Podemos destacar algunos softwares antivirus como McAfee o AVG.

**-Cortafuegos**: El cortafuegos o firewall una parte del sistema que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Todos los mensajes que entran o salen pasan a través del cortafuegos, que examina cada mensaje y bloquea los que no cumplen los criterios de seguridad especificados.

Es importante recordar que un cortafuegos no elimina problemas de virus del ordenador, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicionales para tu ordenador o red. Podemos distinguir entre cortafuegos de hardware (se compran como producto

independiente y protegen de ataques del mundo exterior) y de software, el más utilizado, que controla intentos de acceder a tu ordenador desde el exterior.

- **Recuperación**

-Copias de seguridad.

Una Copia de Seguridad, o Backup en inglés, es un duplicado de nuestra información más importante, que realizamos para salvaguardar los archivos de nuestro ordenador, por si acaso ocurriese algún problema que nos impidiese acceder a los originales que tenemos en él.

Para usuarios de Windows, para realizar una copia de seguridad vamos Inicio y luego, selecciona Panel de control > Sistema y mantenimiento > Copia de seguridad y restauración.

**-Información en la nube**

La “nube” , cloud computing en inglés, es un modelo que traslada parte de tus archivos y programas a un conjunto de programas a los cuales se puede acceder a través de internet. Todo lo que ocurre dentro de la nube es totalmente transparente para ti y no necesitas conocimiento técnico para utilizarla.

Actualmente, estamos haciendo un uso constante de “la nube constante, cuando, por ejemplo, accedemos a nuestro correo a través de páginas web como Gmail o Outlook.

La nube ofrece un gran número de ventajas, como es el hecho de poder acceder a ella desde varios dispositivos o el de poder tener “concentrados” todos nuestros archivos. Aún así, presenta notables desventajas, como son el hecho de que sin internet no podemos acceder a ella o la falta de seguridad y privacidad.

**-SAN**

La red SAN (Storage Area Network) es una red que permite adjuntar dispositivos de almacenamiento de computadoras remotas como un conjunto de discos, como si fuesen dispositivos locales. Las SANs todavía no son comunes fuera de grandes corporaciones. Estas redes permiten duplicar el aprovechamiento del almacenamiento, reducir a la mitad los gastos de almacenamiento e impulsar la productividad de todo el negocio, a la vez que disfruta de un alto rendimiento y disponibilidad.

Es una subred de alta velocidad, donde todos los sistemas de almacenamiento están disponibles para todos los servidores de la red LAN o WAN.

**-Conexiones seguras y cifradas:**

**·DNI Electrónico:**

El DNI electrónico es un documento emitido por la Dirección General de la Policía . Este documento permite acreditar físicamente la identidad personal de su titular y de una forma electrónica e inequívoca.

En enero de 2015 se puso en marcha el DNI 3.0 . Un documento de alta seguridad que combina las más novedosas medidas de seguridad con la última tecnología aplicada a la identificación de los ciudadanos.

**·Certificados digitales:**

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las

instituciones puedan ofrecer servicios seguros a través de Internet. Además, este permite la firma electrónica de elementos y cifrar información.

**·HTTPS:**

Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto),es un protocolo de aplicación basado en el protocolo HTTP. Éste permite una transferencia segura de datos de hipertexto.

Es utilizado principalmente por cualquier tipo de servicio que requiera el envío de datos personales y/o contraseñas.

Certificado electrónico

Es un documento electrónico expedido por una Autoridad de Certificación y Contiene la información necesaria para firmar electrónicamente e identificar a su propietario con sus datos: nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide.

**-Navegación privada:**

La diferencia respecto a la navegación normal es que no se guarda la siguiente información:

-Cookies: al cerrar la ventana desaparecen.

-Caché web: no permanece ningún archivo.

-Historial del navegador (que no de búsquedas de Google).

-Datos para la función “autocompletar” de formularios.

-Otros datos del navegador: contraseñas, listas de descargas, etc.

No obstante, la navegación privada no sirve para evitar el código de seguimiento de Google Analytics y para desactivar el historial de búsqueda, pues este se guarda en la nube y Google

lo guardará siempre a no ser que desactives tu cuenta. La navegación privada tampoco evita ataques relacionados con la seguridad.

Actualmente, tanto Google Chrome como Mozilla Firefox permiten la navegación privada.
El Filtro de suplantación de identidad (phishing) ofrece una nueva tecnología dinámica para protegerte del fraude en el Web y del riesgo de robo de datos personales. Las estafas conocidas como "phishing" normalmente intentan atraerte para que visites sitios web falsos donde se puede recopilar tu información personal o de tarjeta de crédito para fines delictivos. Esta forma de robo de identidad está aumentando rápidamente en Internet. Consulta opciones generales del filtro anti-phishing.

**Filtro de Suplantación de Identidad (Phishing Filter):**

La suplantación de identidad (phishing) en línea es un método de robo de identidad mediante el que se te engaña para que reveles tu información personal o financiera en línea. Los estafadores emplean webs falsas o correos en los que imitan a diversas empresas (generalmente las bancarias ) con el fin de robar información personal identificable como nombres de usuario, contraseñas, números de tarjetas de crédito...
El Filtro de Suplantación de identidad de Microsoft protege a los usuarios de Windows de sitios web fraudulentos, actuando de dos formas:

-Funciona en segundo plano mientras te desplazas por el Web, analiza las páginas Web y determina si son sospechosas.

-El Filtro de suplantación de identidad comprueba los sitios que visita en una lista dinámica

actualizada de sitios de suplantación de identidad notificados. Si se existe una coincidencia, el filtro avisará con una señal roja, advirtiendo de que la navegación no es segura.

·**Bloqueador de elementos emergentes:** puedes cambiar el modo en que los sitios web supervisan tu actividad en línea ajustando la configuración de privacidad de Internet Explorer. Por ejemplo, puedes decidir qué cookies se van a almacenar, cómo y cuándo los sitios pueden usar tus datos de ubicación y bloquear mensajes emergentes no deseados.

·**Java/JavaScript:** JavaScript no crea applets ni aplicaciones independientes. En su forma más habitual, JavaScript está en documentos HTML y puede proporcionar niveles de interactividad en las páginas web que no se pueden conseguir con HTML simple.

Diferencias clave entre Java y JavaScript

- Java es un lenguaje de programación OOP, mientras que JavaScript es un lenguaje de scripts OOP.
- Java crea aplicaciones que se ejecutan en una máquina o explorador virtual, mientras que el código JavaScript sólo se ejecuta en un explorador.
- El código Java necesita compilación, mientras que el código JavaScript está en todo el texto.
- Necesitan diferentes plugins.

·**Filtrado Active X:** ActiveX es una tecnología de Microsoft para el desarrollo de páginas dinámicas. Tiene presencia en la programación del lado del servidor y del lado del cliente,

aunque existan diferencias en el uso en cada uno de esos dos casos.

Son pequeños programas que se pueden incluir dentro de páginas web y sirven para realizar acciones de diversa índole. Por ejemplo hay controles ActiveX para mostrar un calendario, para implementar un sistema de FTP, etc. Son un poco parecidos a los Applets de Java en su funcionamiento, aunque una diferencia fundamental es la seguridad, pues un Applet de Java no podrá tomar privilegios para realizar acciones malignas (como borrarnos el disco duro) y los controles ActiveX sí que pueden otorgarse permisos para hacer cualquier cosa. Los controles ActiveX son particulares de Internet Explorer.

·**Configuración de las Cookies:** son una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Sus principales funciones son:

***Llevar el control de usuarios:** cuando un usuario introduce su nombre de usuario y contraseña, se almacena una galleta para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo, una galleta no identifica a una persona, sino a una combinación de computadora de la clase de computacion-navegador-usuario.

* **Conseguir información sobre los hábitos de navegación del usuario**, e intentos de spyware (programas espía), por parte de agencias de publicidad y otros. Esto puede causar problemas de privacidad y es una de las razones por la que las cookies tienen sus detractores.

## FUENTES DE INFORMACIÓN Y REFERENCIACIÓN DE LAS MISMAS

### Fundamentos de las redes

- Proceso de comunicación

  https://es.wikipedia.org/wiki/Protocolo_de_comunicaciones

- Redes de ordenadores

  https://es.wikipedia.org/wiki/Red_de_computadoras

### Origen de las redes y modelos de referencia

https://es.scribd.com/doc/28065286/Origenes-de-Las-Redes-Alambricas-e-Inalambricas

- Modelo de referencia OSI

  https://es.wikipedia.org/wiki/Modelo_OSI

- Familia de protocolos de Internet: TCP/IP

  https://es.wikipedia.org/wiki/Modelo_TCP/IP

### Protocolo IP

- Direcciones IP

  https://es.wikipedia.org/wiki/Dirección_IP

    - Direcciones IPv4

      https://es.wikipedia.org/wiki/Dirección_IP#Direcciones_IPv4
    - Direcciones IPv6

      https://es.wikipedia.org/wiki/Dirección_IP#Direcciones_IPv6
    - IP estática

      http://es.ccm.net/faq/569-seguridad-ip-estatica-o-dinamica
    - IP dinámica

      https://es.wikipedia.org/wiki/Dirección_IP#IP_din.C3.A1mica
    - Direcciones públicas

      http://windowsespanol.about.com/od/RedesYDispositivos/f/IP-Publica-IP-Privada.htm
    - Direcciones privadas

      https://es.wikipedia.org/wiki/Dirección_IP#Direcciones_privadas
- Subredes

  https://es.wikipedia.org/wiki/Subred
- Puerta de enlace o Gateway

  http://www.puertadeenlace.com/faq/general/46-que-es-una-puerta-de-enlace-gateway
- DNS

  http://www.xatakamovil.com/conectividad/como-funciona-internet-dns
- Dirección MAC

  https://es.wikipedia.org/wiki/Dirección_MAC

**Tipos de redes**

- Según su área de cobertura
    - Red de área extensa, WAN

      https://es.wikipedia.org/wiki/Red_de_área_amplia
    - Red de área metropolitana, MAN

      https://es.wikipedia.org/wiki/Red_de_área_metropolitana
    - Red de área local, LAN

      https://es.wikipedia.org/wiki/Red_de_área_local
    - Red de área personal, PAN

      https://es.wikipedia.org/wiki/WPAN
- Según su tipología
    - Bus

      https://es.wikipedia.org/wiki/Red_en_bus
    - Anillo

      https://es.wikipedia.org/wiki/Red_en_anillo
    - Estrella

      https://es.wikipedia.org/wiki/Red_en_estrella
    - Árbol

      https://es.wikipedia.org/wiki/Red_en_%C3%A1rbol
    - Híbrida

      https://es.wikipedia.org/wiki/Topología_híbrida
- Según su nivel de acceso o privacidad
    - Red pública

      http://www.eveliux.com/mx/concepto-de-red-publica-y-red-privada.html

    - Red privada

      http://www.eveliux.com/mx/concepto-de-red-publica-y-red-privada.html

    - VPN (red privada virtual)

      https://es.wikipedia.org/wiki/Red_privada_virtual

- Según su relación funcional

    - Cliente-Servidor

      https://es.wikipedia.org/wiki/Cliente-servidor

    - Redes entre iguales, P2P

      https://es.wikipedia.org/wiki/Peer-to-peer

- Según su tecnología física de conexión

    - Redes cableadas

      http://teoriasobreredes.blogspot.com.es/p/blog-page.html

        - Fast Ethernet

          https://es.wikipedia.org/wiki/Fast_Ethernet

        - Gigabit Ethernet

          https://es.wikipedia.org/wiki/Gigabit_Ethernet

        - 10 Gigabit Ethernet

          https://es.wikipedia.org/wiki/10_Gigabit_Ethernet

    - Redes inalámbricas

      http://teoriasobreredes.blogspot.com.es/p/blog-page.html

        - Wi-Fi

          https://es.wikipedia.org/wiki/Wifi

        - Bluetooth

          https://es.wikipedia.org/wiki/Bluetooth

        - Infrarrojos

          https://es.wikipedia.org/wiki/Red_por_infrarrojos

**La red Internet**

- Orígenes de internet

  https://es.wikipedia.org/wiki/Internet#Origen

- Servicios de internet

  http://www.uclm.es/profesorado/ricardo/internet/index_archivos/inet_servicios.htm

- La web

  https://es.wikipedia.org/wiki/World_Wide_Web

- Evolución de la web

    - Web 1.0 o web estática

      https://es.wikipedia.org/wiki/Web_1.0

    - Web 2.0 o web social

      https://es.wikipedia.org/wiki/Web_2.0

    - Web 3.0 o web semántica

      https://es.wikipedia.org/wiki/Web_3.0

**Tecnologías de acceso a Internet**

- Acceso cableado

  http://recursostic.educacion.es/usuarios/web/ayudas/54-conexiones-a-internet-bis

- Acceso inalámbrico

  https://es.wikipedia.org/wiki/Punto_de_acceso_inalámbrico

- Acceso móvil

  https://facua.org/es/guia.php?Id=142&capitulo=1258

Línea telefónica

- RTC

  http://wikitel.info/wiki/RTC

- RDSI

  https://es.wikipedia.org/wiki/Red_digital_de_servicios_integrados

- ADSL

  http://definicion.de/adsl/

Cable o HFC

https://es.wikipedia.org/wiki/Híbrido_de_Fibra_Coaxial

Fibra óptica hasta el hogar

https://es.wikipedia.org/wiki/Fibra_hasta_la_casa

Internet por satélite

https://www.euskaltel.com/CanalOnline/empresas/internet/internet-en-casa/internet-por-satelite-empresa

WIMAX y LMDS

http://www.engisip.com/tecno_lmds-wimax.asp

Red eléctrica

https://es.wikipedia.org/wiki/Red_eléctrica

Conexión por telefonía móvil

- Primera generación, 1G

  https://es.wikipedia.org/wiki/Telefonía_móvil_1G
- Segunda generación, 2G

  https://es.wikipedia.org/wiki/Telefonía_móvil_2G
- Tercera generación, 3G

  https://es.wikipedia.org/wiki/Telefonía_móvil_3G
- Cuarta generación, 4G

  https://es.wikipedia.org/wiki/Telefonía_móvil_4G

**Seguridad en la red**

- Confidencialidad

  https://es.wikipedia.org/wiki/Seguridad_de_la_información
- Autentificación

  https://es.wikipedia.org/wiki/Autenticación
- Autorización

  https://es.wikipedia.org/wiki/Autorizaci%C3%B3n
- Integridad

https://es.wikipedia.org/wiki/Integridad_de_datos

- Disponibilidad

http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServDisponibilidad.php

Amenazas a la seguridad

http://recursostic.educacion.es/observatorio/web/fr/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=5

- Causas humanas
- Causas lógicas
- Causas físicas

Legislación en la red

- LOPD

  http://www.lopd-proteccion-datos.com/ley-proteccion-datos.php
- LPI

  http://noticias.juridicas.com/base_datos/Admin/rdleg1-1996.html
- LSSI-CE

  http://www.tyd.es/pdfs/Obligaciones%20LSSI%20resumen.pdf
- LAECSP

  http://www.cenatic.es/laecsp/

- Ley de firma electrónica

  http://noticias.juridicas.com/base_datos/Admin/l59-2003.html

Adopción de medidas de seguridad

- Protección
  - Antivirus

    https://es.wikipedia.org/wiki/Antivirus
  - Cortafuegos

    http://computerhoy.com/noticias/internet/cortafuegos-informaticos-que-son-que-sirven-26747
- Recuperación
  - Copias de seguridad
  - Información en la nube
  - SAN

Conexiones seguras y cifradas

- DNIe

  https://www.dnielectronico.es/PortalDNIe/
- Certificados digital

  https://es.wikipedia.org/wiki/Certificado_digital
- HTTPS

  https://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure
- Certificado electrónico

ttps://www.sede.fnmt.gob.es/certificados/persona-fisica

Configuración segura del navegador

- Navegación privada

https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=es

- Filtro contra la suplantación de identidad, Phishing

https://es.wikipedia.org/wiki/Phishing

- Bloqueador de elementos emergentes

https://support.microsoft.com/es-es/help/17479/windows-internet-explorer-11-change-security-privacy-settings

- Java/JavaScript

  http://www.campusmvp.es/recursos/post/Java-y-JavaScript-son-lo-mismo.aspx
- Filtrado Active X:

  https://es.answers.yahoo.com/question/index?qid=20110522083231AAuNjbY

- Configuración de las cookies:

  https://es.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)