METRO DE MADRID

PROGRAMA DE CONOCIMIENTOS

OFICIO 2025

ELECTRÓNICA E INFORMÁTICA

Para el nuevo proceso de ingreso en Metro de Madrid, se han creado un **CANAL** y un **GRUPO** de **Telegram** para informar, resolver dudas y compartir novedades en tiempo real.

El **CANAL** y el **GRUPO** ofrecerán actualizaciones sobre el proceso, mientras que el **GRUPO** además se permitirá la comunicación directa entre participantes para resolver inquietudes y compartir información relevante.

Se fomenta un ambiente de **respeto y colaboración**, asegurando interacciones constructivas para todas las personas interesadas. **¡Participa y mantente al tanto!**

Accede aquí:

PLANES DE FORMACIÓN OFICIALES EN ESPAÑA PARA LAS SIGUIENTES TITULACIONES DE FORMACIÓN PROFESIONAL:

1. **Técnico en Instalaciones de Telecomunicaciones**: Esta titulación de Grado Medio pertenece a la familia profesional de Electricidad y Electrónica. Los titulados en esta especialidad están capacitados para instalar, mantener y reparar sistemas de telecomunicaciones en viviendas y edificios, incluyendo redes de voz y datos, sistemas de seguridad y circuitos cerrados de televisión.

2. **Técnico en Sistemas Microinformáticos y Redes**: También de Grado Medio, esta titulación forma parte de la familia profesional de Informática y Comunicaciones. Los profesionales en este campo se encargan de instalar, configurar y mantener sistemas microinformáticos, así como redes locales en entornos pequeños y medianos, asegurando su correcto funcionamiento y seguridad.

3. **Técnico Superior en Mantenimiento Electrónico**: Esta titulación de Grado Superior pertenece a la familia profesional de Electricidad y Electrónica. Los titulados están preparados para desarrollar proyectos, gestionar y supervisar el montaje y mantenimiento de equipos y sistemas electrónicos, asegurando su funcionamiento y calidad.

4. **Técnico Superior en Administración de Sistemas Informáticos en Red**: De Grado Superior y perteneciente a la familia profesional de Informática y Comunicaciones, esta titulación capacita para configurar, administrar y mantener sistemas informáticos en red, garantizando su operatividad y seguridad.

5. **Técnico Superior en Sistemas de Telecomunicaciones e Informáticos**: También de Grado Superior y dentro de la familia profesional de Electricidad y Electrónica, esta titulación forma a profesionales para desarrollar proyectos, gestionar y supervisar el montaje y mantenimiento de infraestructuras comunes de telecomunicaciones y sistemas informáticos, asegurando su correcto funcionamiento y calidad.

Para obtener información detallada sobre los módulos profesionales de cada una de estas titulaciones, te recomiendo consultar el portal oficial de Formación Profesional del Ministerio de Educación y Formación Profesional de España:

- **Técnico en Instalaciones de Telecomunicaciones**: https://www.todofp.es/que-estudiar/familias-profesionales/electricidad-electronica/instalaciones-telecomunicaciones.html

- **Técnico en Sistemas Microinformáticos y Redes**: https://www.todofp.es/que-estudiar/familias-profesionales/informatica-comunicaciones/sistemas-microinformaticos-redes.html

- **Técnico Superior en Mantenimiento Electrónico**: https://www.todofp.es/que-estudiar/familias-profesionales/electricidad-electronica/mantenimiento-electronico.html

- **Técnico Superior en Administración de Sistemas Informáticos en Red**: https://www.todofp.es/que-estudiar/familias-profesionales/informatica-comunicaciones/admin-sist-informaticos-red.html

- **Técnico Superior en Sistemas de Telecomunicaciones e Informáticos**: https://www.todofp.es/que-estudiar/familias-profesionales/electricidad-electronica/sistemas-telecomunicaciones-informaticos.html

📢 AVISO IMPORTANTE SOBRE ESTE TEMARIO 📢

Este material se ofrece de forma gratuita y tiene como único propósito complementar el estudio individual del programa oficial de conocimientos. No sustituye ni reemplaza los contenidos oficiales, por lo que puede contener erratas o imprecisiones.

Conocimiento compartido y mejora colectiva

Este temario se basa en la idea de que el conocimiento debe ser libre, accesible y construido de forma colectiva. Entendemos la formación como un proceso en constante evolución, donde cada persona puede aportar, corregir y enriquecer el contenido. Si encuentras errores, tienes propuestas de mejora o deseas incluir información útil, tu colaboración es bienvenida. Este material está vivo y abierto, como reflejo de nuestros principios de Solidaridad, apoyo mutuo y empoderamiento Obrero. Aprender juntos, compartir saberes y mejorarlos es también una forma de luchar y avanzar hacia una formación más consciente y transformadora.

Te agradeceríamos que nos lo comuniques enviando un correo a:

soliinformacion@gmail.com

Este temario es fruto del gran esfuerzo y dedicación de los delegados y delegadas de Solidaridad Obrera, quienes han trabajado para elaborarlo y distribuirlo de manera altruista.

❤️🖤¡Gracias por tu confianza y colaboración!🖤❤️

📝 Ver uso de contenidos, fuentes y derechos de autor en la última página.

ÍNDICE

Ver uso de contenidos, fuentes y derechos de autor en la última página.

1. INSTALACIONES ELÉCTRICAS BÁSICAS

1.1. CONCEPTOS DE ELECTRICIDAD

Es un fenómeno: físico, químico, natural, que llena toda la estructura molecular de un cuerpo y se manifiesta a través de un flujo de electrones. Cuando una carga se encuentra en reposo produce fuerzas sobre otras situadas en su entorno. Si la carga se desplaza produce también fuerzas magnéticas. Hay dos tipos de carga eléctrica, llamadas positiva y negativa.

La electricidad está presente en algunas partículas subatómicas. La partícula fundamental más ligera que lleva carga eléctrica es el electrón, que transporta una unidad de carga. Los átomos, en circunstancias normales, contienen electrones, y a menudo los que están más alejados del núcleo se desprenden con mucha facilidad. En algunas sustancias, como los metales, proliferan los electrones libres. De esta manera, un cuerpo queda cargado eléctricamente gracias a la reordenación de los electrones.

Un átomo normal tiene cantidades iguales de carga eléctrica positiva y negativa; por lo tanto, es eléctricamente neutro. La cantidad de carga eléctrica transportada por todos los electrones del átomo, que por convención es negativa, está equilibrada por la carga positiva, localizada en el núcleo. Si un cuerpo contiene un exceso de electrones quedará cargado negativamente. Por lo contrario, con la ausencia de electrones, un cuerpo queda cargado positivamente, debido a que hay más cargas eléctricas positivas en el núcleo.

PRINCIPIOS FÍSICOS DE LA ELECTRICIDAD

Empezamos a explicar la electricidad a través de la física, concretamente de la unidad de materia. La materia está constituida por átomos.

LA ESTRUCTURA DEL ÁTOMO

Un átomo es la unidad más pequeña de materia y está compuesto de dos regiones. La primera es el pequeño núcleo atómico, que se encuentra en el centro del átomo y contiene partículas cargadas positivamente llamadas protones, y partículas neutras, sin carga, llamadas neutrones. La segunda, que es mucho más grande, es una "nube" de electrones, partículas de carga negativa que orbitan alrededor del núcleo. La atracción entre los protones de carga positiva y los electrones de carga negativa es lo que mantiene unido al átomo. La mayoría de los átomos tienen estos tres tipos de partículas subatómicas, protones, electrones y neutrones.

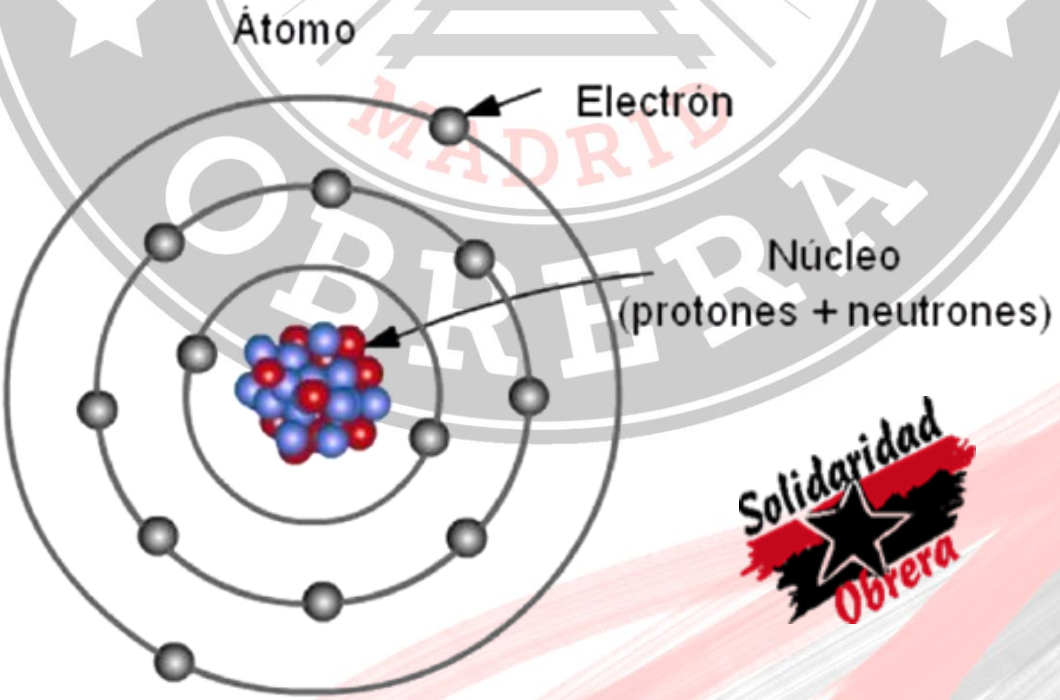
- **Electrones**, los mismos poseen carga eléctrica negativa (-) y se desplazan en una órbita elíptica al núcleo del átomo.
- **Protones**, estos se encuentran en el núcleo del átomo y poseen una carga eléctrica positiva (+).
- **Neutrones**, también se encuentran en el núcleo del átomo, y como su nombre lo indica posee carga neutra.

En su estado natural un átomo posee la misma cantidad de electrones que protones, obteniendo un átomo "neutro". Sin embargo, si el mismo poseyera más protones que electrones se lo denominaría Ion positivo, caso contrario sería un Ion negativo.

Teniendo en claro estos conceptos básicos podemos comprender el carácter eléctrico de la materia:

Imaginemos por un instante que poseemos un átomo en un **conductor metálico**, supongamos que ese átomo **A** posee un electrón que se ha movido hacia la órbita exterior del átomo, la atracción producida por los protones a ese electrón es mínima, mediante lo cual, si a este le proporcionamos suficiente energía, este electrón que se encuentra en la órbita o capa exterior (también llamado electrón de valencia) abandonara este átomo, pasando a llamarse electrón libre. Este electrón "libre" luego es adquirido por otro átomo (supongamos **B**), el cual previamente ha perdido un electrón, y así sucesivamente. Este proceso se denomina de "Ionización".

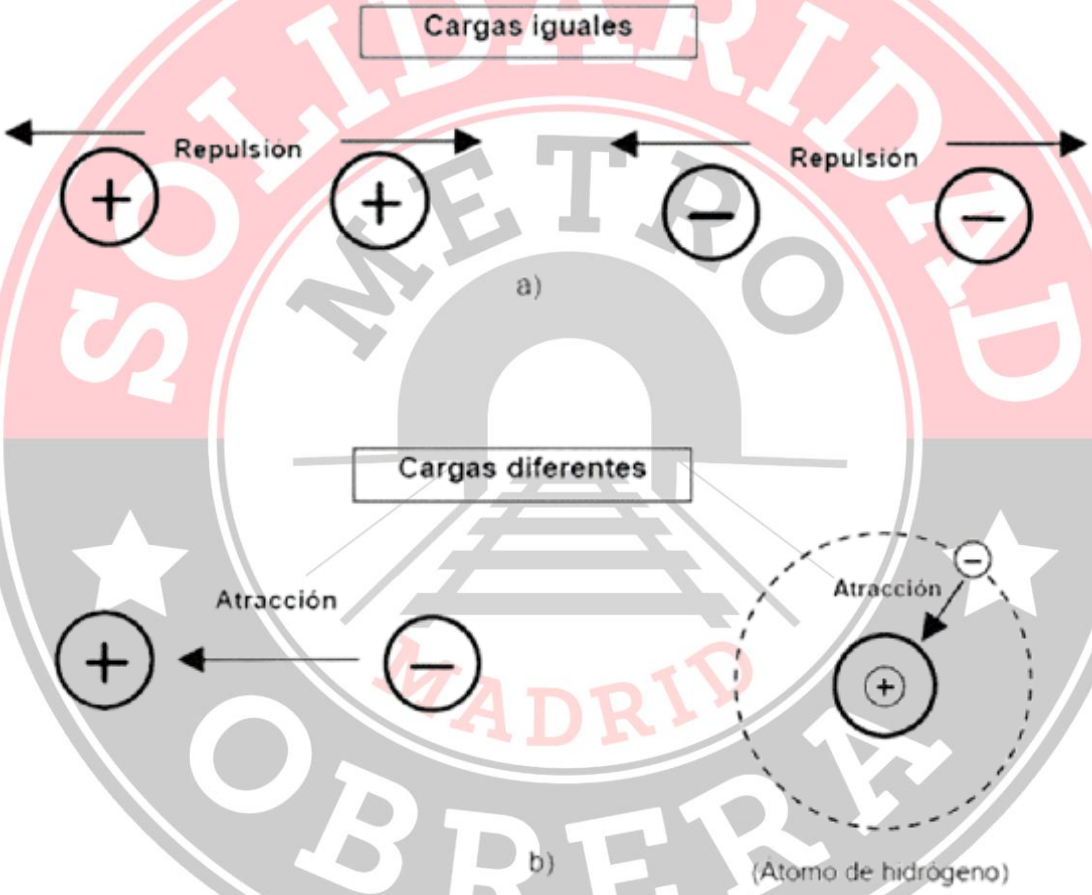
Este movimiento es el causante de la **corriente eléctrica**.



Inicialmente los átomos están equilibrados, es decir tienen una carga neutra, los protones y electrones se configuran de tal manera que se igualan las cargas. Para que los átomos manifiesten carga positiva o negativa se recurrirá a la eliminación de un protón o un electrón, esto da a lugar a dos posibilidades:

- **Catión o ión positivo:** Si al átomo le quitamos un electrón, su carga es positiva (+)
- **Anión o ión negativo:** Si al átomo le quitamos un protón, su carga es negativa (-)

El efecto que nos interesa en este artículo es el de **atracción o repulsión** entre átomos (análisis de las cargas) esto es el efecto que desarrolla un átomo sobre otro de igual carga o distinta carga.



Cuando disponemos de dos iones de igual carga (sea esta negativa o positiva), estos se repelerán, mientras que, si los iones son de cargas diferentes, se atraerán. Este efecto se denomina **Ley de Coulomb *.**

*** Nota:** Definición: **Ley de Coulomb**: Las cargas opuestas se atraen y las cargas iguales se repelen.

1.1.1. MAGNITUDES ELÉCTRICAS FUNDAMENTALES

1.1.1.1. Voltaje (V):

El **voltaje** o **tensión eléctrica** es la diferencia de potencial eléctrico entre dos puntos de un circuito. Representa la energía por unidad de carga eléctrica que impulsa el movimiento de los electrones a través de un conductor. Se mide en **voltios (V)** y su símbolo es V.
Matemáticamente, el voltaje se expresa como:

$$V = \frac{W}{Q}$$

donde:

- V es el voltaje en voltios (V)
- W es el trabajo o energía en julios (J),
- Q es la carga eléctrica en coulombs (C).

El voltaje es un parámetro fundamental en la electricidad y es responsable del flujo de corriente eléctrica en un circuito.

1.1.1.2. Corriente eléctrica (I):

El **amperio (A)** es la unidad de medida de la corriente eléctrica en el Sistema Internacional de Unidades. Se define como el flujo de carga eléctrica que pasa por un conductor en un segundo. Específicamente, un amperio equivale al paso de **un culombio (C) de carga por segundo**:

Donde:

$$1\,\mathrm{A} = 1\,\frac{\mathrm{C}}{\mathrm{s}}$$

- **A** = Corriente en amperios (A)
- **C** = Carga en culombios (C)
- **s** = Tiempo en segundos (s)

Un culombio corresponde aproximadamente a electrones en movimiento. Esta definición es fundamental en la electricidad, ya que describe el caudal de electrones que fluye en un circuito.

1.1.1.3. Resistencia eléctrica (R):

El **ohmio (Ω)** es la unidad de medida de la resistencia eléctrica en el Sistema Internacional de Unidades. La resistencia eléctrica se define como la oposición que presenta un material al paso de la corriente eléctrica. Matemáticamente, se expresa mediante la Ley de Ohm:

$$R = \frac{V}{I}$$

Donde:

- **R** = Resistencia en ohmios (Ω)
- **V** = Voltaje en voltios (V)
- **I** = Corriente en amperios (A)

Conclusión

Las unidades de medida del Sistema Internacional en electricidad (**voltio, amperio y ohmio**) son esenciales para comprender el comportamiento de los circuitos eléctricos y el funcionamiento de los dispositivos electrónicos. Cada una de estas unidades está interconectada a través de leyes fundamentales como la Ley de Ohm y la definición de potencia eléctrica. Su correcta comprensión permite diseñar, mantener y optimizar sistemas eléctricos en una amplia variedad de aplicaciones, desde pequeños dispositivos electrónicos hasta grandes sistemas de energía eléctrica industrial. Comprender estas unidades es el primer paso para dominar la electrónica y la ingeniería eléctrica.

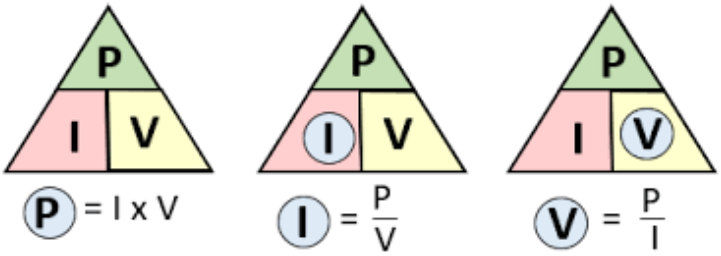
1.1.1.4. Potencia eléctrica (P):

La potencia eléctrica la podemos definir como la cantidad de energía eléctrica que se genera o se consume cada segundo.

Por ejemplo, la potencia de una lámpara o bombilla sería la cantidad de luz que emite por unidad de tiempo, en un timbre la cantidad de sonido que emite por unidad de tiempo, en un radiador la cantidad de calor que emite por unidad de tiempo. Se mide en vatios (w) y se representa con la letra P.

Una lámpara de 80w dará el doble de luz que una de 40w.

Su fórmula es:

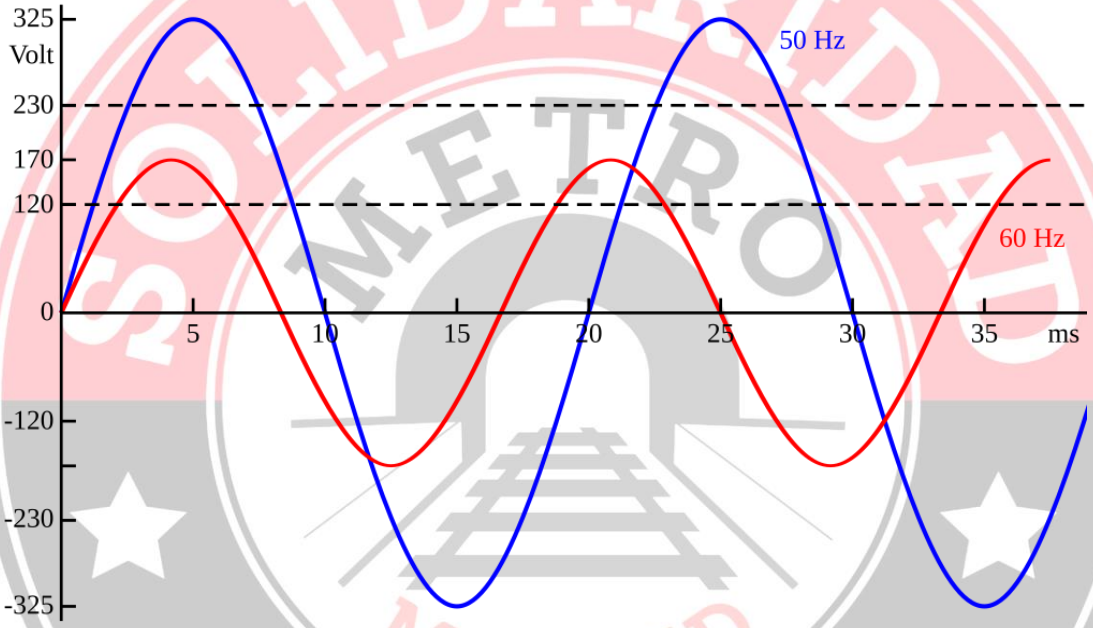


I: Intensidad en Amperios (A).

V: tensión en voltios (V).

1.1.1.5. Frecuencia (Hz):

La frecuencia de red es el valor nominal de las oscilaciones de corriente alterna (CA) en una red síncrona de área amplia transmitida desde una central eléctrica al usuario final.



En gran parte del mundo es de 50 Hz,2 aunque en partes de América y partes de Asia suele ser de 60 Hz. El uso actual por país o región se proporciona en la lista de electricidad de red por país. Durante el desarrollo de los sistemas comerciales de energía eléctrica a fines del siglo XIX y principios del XX, se utilizaron muchas frecuencias (y voltajes) diferentes. La gran inversión en equipos en una frecuencia hizo que la estandarización fuera un proceso lento. Sin embargo, a principios del siglo XXI, los lugares que ahora usan la frecuencia de 50 Hz tienden a usar 220–240 V, y los que ahora usan 60 Hz tienden a usar 100–127 V. Ambas frecuencias coexisten hoy (Japón usa ambas) sin una gran razón técnica para preferir una y sin un deseo aparente de estandarización mundial completa.

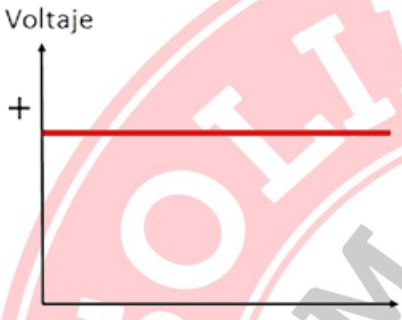
En la práctica, la frecuencia exacta de la red varía alrededor de la frecuencia nominal, reduciéndose cuando la red está muy cargada y acelerándose cuando la carga es ligera. Sin embargo, la mayoría de las empresas de servicios públicos ajustarán la frecuencia de la red a lo largo del día para garantizar que se produzca un número constante de ciclos. Esto es utilizado por algunos relojes para mantener con precisión su tiempo.

1.1.2. TIPOS DE CORRIENTE ELÉCTRICA

1.1.2.1. Corriente continua (DC):

La **corriente continua** es aquella en la que el flujo de cargas eléctricas se mantiene constante en una única única dirección. Utilizada en baterías, electrónica de consumo y paneles solares.

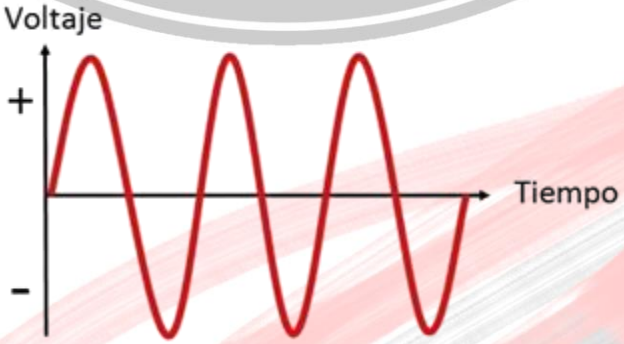
Esto significa que los electrones se desplazan siempre desde el polo negativo hacia el polo positivo del circuito, sin invertir su sentido de movimiento. La tensión o voltaje en un circuito de corriente continua también permanece constante, sin variaciones periódicas.



- Mantiene una dirección constante.
- Su voltaje es estable o varía uniformemente.
- Se encuentra en baterías, celdas solares y sistemas electrónicos.
- Es utilizada en dispositivos electrónicos sensibles y circuitos de baja potencia.
- Se transporta en distancias cortas debido a la caída de voltaje con la distancia.

1.1.2.2. Corriente alterna (AC):

La **corriente alterna** se caracteriza por un flujo de cargas eléctricas que cambia de dirección periódicamente. Esto significa que los electrones oscilan hacia adelante y hacia atrás dentro del conductor, debido a que la tensión alterna invierte su polaridad en intervalos regulares. La forma de onda más común de la corriente alterna es la senoidal, aunque existen otras formas como la triangular o cuadrada. Es la forma de electricidad utilizada en hogares e industrias debido a su facilidad de transporte y transformación.



- Cambia de dirección periódicamente.
- Su voltaje sigue un patrón senoidal con una frecuencia definida.
- Se usa en la distribución eléctrica doméstica e industrial.
- Es más eficiente para el transporte de electricidad a largas distancias debido a la facilidad con la que se puede transformar su voltaje mediante transformadores.

1.2. INSTALACIONES ELÉCTRICAS RESIDENCIALES Y COMERCIALES

Las instalaciones eléctricas se dividen en función de su uso y ubicación, existiendo diferencias en los materiales, la distribución de cargas y la normativa aplicada.

En el ámbito de la electricidad, existen diferentes tipos de instalaciones que se adaptan a las necesidades específicas de cada entorno. A continuación, se detallan algunos de los principales tipos de instalaciones eléctricas.

- **Instalaciones eléctricas residenciales**: Son aquellas destinadas a los hogares y viviendas. Estas instalaciones cubren la distribución de energía eléctrica para iluminación, electrodomésticos, enchufes, sistemas de climatización, entre otros.
- **Instalaciones eléctricas comerciales**: Se refieren a las instalaciones eléctricas en edificios comerciales, como oficinas, tiendas, centros comerciales y restaurantes. Estas instalaciones están diseñadas para cubrir las necesidades eléctricas de los negocios y pueden incluir sistemas de iluminación especializada, equipos de climatización y sistemas de seguridad.

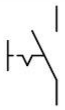
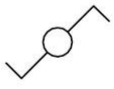
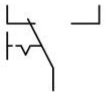
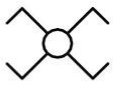
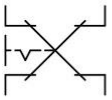
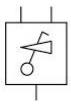
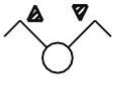
1.2.1. SÍMBOLOS NORMALIZADOS PARA LOS ESQUEMAS UNIFILARES Y MULTIFILARES

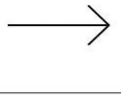
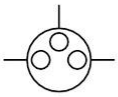
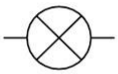
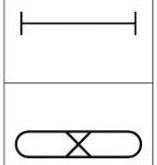
¿QUÉ ES LA SIMBOLOGÍA ELÉCTRICA?

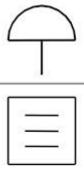
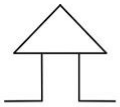
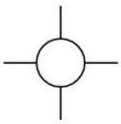
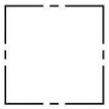
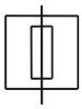
La Simbología Eléctrica es la representación gráfica de cada uno de los elementos eléctricos dentro de un circuito eléctrico o una instalación eléctrica.

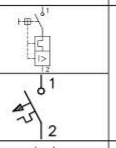
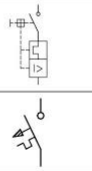
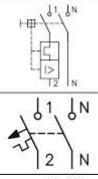
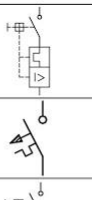
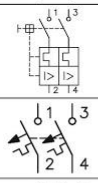
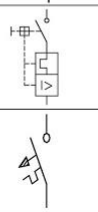
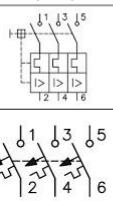
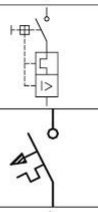
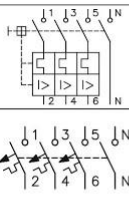
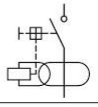
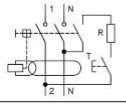
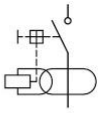
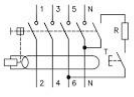
Los símbolos de circuitos eléctricos se utilizan para dibujar un diagrama esquemático. en otras palabras, es la representación gráfica que se realiza de cada elemento de un circuito o instalación eléctrica.

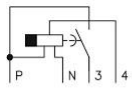
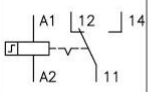
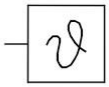
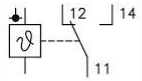
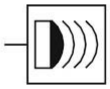
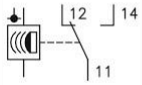
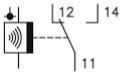
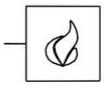
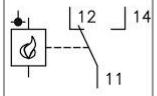
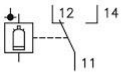
Los símbolos de conexiones eléctricas más utilizados para instalaciones domiciliarias. Para la representación de interruptores en circuitos unifilares de edificaciones, la norma UNE-EN 60617-11 define los siguientes símbolos.

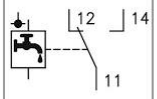
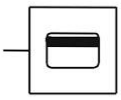
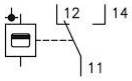
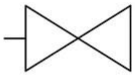
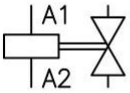
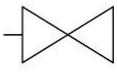
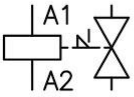
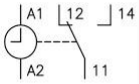
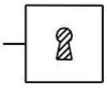
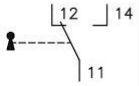
Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Interruptor	Empotrado en caja de mecanismo a una altura de 110 cm de pavimento y 15 cm del marco de la puerta (a excepción de cabeceros en dormitorios). A derecha o izquierda de éste pero siempre en el mismo lado del mecanismo de apertura de la puerta. Se prestará especial interés en la correcta fijación de la caja de mecanismo, debiendo estar nivelada y enrasada, de forma que permita que la placa de los mecanismos queden perfectamente adosadas al paramento. Los mecanismos deberán interrumpir la fase.
			Interruptor Bipolar	
			Interruptor de tirador	
			Interruptor doble	
			Conmutador	
			Conmutador de cruzamiento	
			Pulsador	
			Regulador	
			Interruptores de persianas	

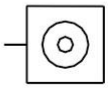
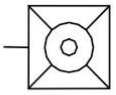
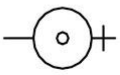
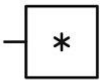
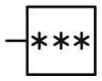
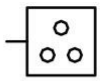
Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Clavija macho	Se admiten como dispositivos de conexión en carga hasta 16 A.
			Clavija hembra	
			Toma de corriente bipolar de 16 A con toma de tierra T	Se instalarán a 20 cm del pavimento, excepto en cocinas y baños, en donde la distancia será de 110 cm.
			Toma de corriente bipolar de 25 A con toma de tierra	La distancia al pavimento será de 70 cm.
			Toma de corriente trifásica con toma de tierra	Se instalará según necesidades de utilización.
			Punto de luz o lámpara	La sección mínima prevista para la alimentación de puntos de luz será de 1,5 mm^2. Todos los puntos de luz deberán disponer de conductor de protección, el cual será de la misma sección que el conductor de fase.
			Lámpara fluorescente	

Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Punto de luz autónomo	En viviendas se instalará encima del C.G.M.P. Se alimentará de C_1.
			Timbre	Se instalarán a una altura del techo de 30 cm. Empotrado en caja de mecanismo.
			Sirena	Se utiliza para avisos de alarmas técnicas. (incendio, gas, inundación.)
			Caja de registro	Su distancia al techo será de 20 cm. Las conexiones en su interior se realizarán mediante bornas.
			Cuadro general de mando y protección	Se instalará lo más próximo a la puerta de entrada. Se fijará a una altura del suelo comprendida entre 1,4 y 2 m.
			Caja general de protección	Se instalarán preferentemente sobre las fachadas exteriores de los edificios.
			Fusible	Se instalarán en bases apropiadas diseñadas especialmente a este fin.

Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Interruptor de control de potencia (ICP)	Se instalará antes de los dispositivos de protección, en caja precintable. Altura entre 1,4 y 2 m.
			Interruptor automático bipolar F+N (PIA) magnetotérmico	Los dispositivos generales e individuales de mando y protección, cuya posición de servicio será vertical, se instalarán en cuadros de distribución. Su poder de corte será suficiente para la intensidad de cortocircuito que pueda producirse en el punto de su instalación. Este poder de corte será como mínimo de 4,5 kA.
			Interruptor automático bipolar (PIA) magnetotérmico	
			Interruptor automático tripolar (PIA) magnetotérmico	
			Interruptor automático tetrapolar (PIA) magnetotérmico	
			Interruptor diferencial bipolar	Se instalarán en cuadros de distribución. Cuando se prevean corrientes no senoidales se emplearán diferenciales del tipo A.
			Interruptor diferencial tetrapolar	

Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Automático de escalera	Se instalará en carril o en fondo de caja, según necesidad.
			Telerruptor	Se instalará en carril o en fondo de caja, según necesidad.
			Termostato	Se instalará lejos de las fuentes de calor y de las corrientes de aire. Altura del suelo entre 1,5 y 1,7 m.
			Detector de movimientos (PIR)	Se instalará lejos de las fuentes de calor y de las corrientes de aire. Prestar atención al ángulo de cobertura.
			Emisor IR	Para el correcto funcionamiento, el emisor debe apuntar al receptor.
			Receptor IR	Su instalación dependerá del tipo de receptor (de techo, empotrar, etc.)
			Detector de incendios	En viviendas se instalarán preferentemente en cocina y pasillos distribuidores
			Detector de gas	***GAS*** / **Altura** Butano o propano / 0,30 m del suelo. Natural / 2,3 m del suelo

Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Detector de inundación	Se instalarán en cocinas, baños, lavaderos y en general en las zonas húmedas. La sonda se fijará a ras del suelo. Se recomienda asociar una electroválvula.
			Sonda de inundación	
			Relé accionado por tarjeta	Permite el control de acceso, y cargas (luces, motores, etc.)
			Electroválvula de agua	Se instalará a la entrada del suministro de agua.
			Electroválvula de gas (con rearme manual)	Se instalará a la entrada del suministro de gas.
			Reloj horario	Se instalará en cuadros de distribución.
			Dispositivo de seguridad con llave	Se instalará en accesos (p. ej. cierres comerciales, etc.)
			Limitador de sobretensiones	Se instalará en cuadros de distribución y en función del nivel de protección.

Simbología eléctrica normalizada				
Mecanismo	Símbolo		Significado	Condiciones de instalación
	Unifilar	Multifilar		
			Elemento calefactor	Cuando se trate de acumuladores eléctricos, deberán preverse las canalizaciones apropiadas, así como los sistemas de regulación y control.
			Lavadora	Se conectarán al circuito C_4 su sección será de 4 mm^2 y se protegerá con un PIA de 20 A. C_4 se puede subdividir en C_{41}, C_{42}, C_{43} .La sección de los circuitos, en este caso, será de 2,5 mm^2. Cada circuito estará protegido por un PIA de 16 A.
			Lavavajillas	
			Calentador eléctrico	
			Refrigerador o frigorífico	Circuito: C_2 Sección: 2,5 mm^2 Protección: 16 A. Base: 2P+T 16 A.
			Congelador	Circuito: C_2 Sección: 2,5 mm^2 Protección: 16 A. Base: 2P+T 16 A.
			Cocina eléctrica horno	Circuito: C_3 Sección: 6 mm^2 Protección: 25 A. Base: 2P+T 25 A.

1.2.1.1. DISEÑO DE INSTALACIONES ELÉCTRICAS RESIDENCIALES:

ESQUEMAS UNIFILARES.

El esquema unifilar eléctrico, como su nombre indica, es una representación gráfica simplificada de un circuito eléctrico en la que cada conductor, sin importar el número de hilos que lo compongan, se representa con una sola línea.

Aunque es menos detallado que un esquema multifilar, el unifilar resulta más funcional para proyectos de obra, ya que facilita la interpretación global del sistema eléctrico y su relación con la estructura del edificio o instalación.

Su simplicidad y eficacia permiten una representación gráfica clara de los circuitos eléctricos, enfocándose en mostrar de manera resumida y ordenada los componentes principales y conexiones básicas.

Como los esquemas unifilares reducen todos los conductores de un tramo a una sola línea, su correcta interpretación requiere familiaridad con este tipo de esquemas. Es indispensable conocer a fondo tanto la simbología estandarizada como los diferentes componentes eléctricos y sus requerimientos, ya que cada elemento determina la cantidad de conductores necesarios y su disposición.

El objetivo principal de un esquema unifilar es simplificar la comprensión y ejecución de los circuitos eléctricos, siendo un esquema fundamental para la planificación, ejecución y mantenimiento de las instalaciones eléctricas en edificios.

Además, los esquemas unifilares topográficos destacan la ubicación de elementos como interruptores, enchufes, luminarias, cuadros de distribución y canalizaciones. Por esta razón, son utilizados ampliamente en planos de planta y alzados arquitectónicos.

Por otro lado, los esquemas unifilares de cuadros eléctricos se utilizan para identificar las cargas y circuitos asociados. Indican el destino de cada circuito (por ejemplo, iluminación, tomas de corriente, motores o circuitos auxiliares), el tipo de protección, sección y canalización de los conductores, pero no ubican espacialmente los elementos de la instalación.

En definitiva, los esquemas unifilares son herramientas indispensables en la ingeniería eléctrica, constituyendo la base para la elaboración de los planos eléctricos.

ESQUEMAS MULTIFILARES

El esquema multifilar eléctrico es una herramienta de representación gráfica utilizada para mostrar de forma detallada todas las conexiones eléctricas de un circuito o instalación.

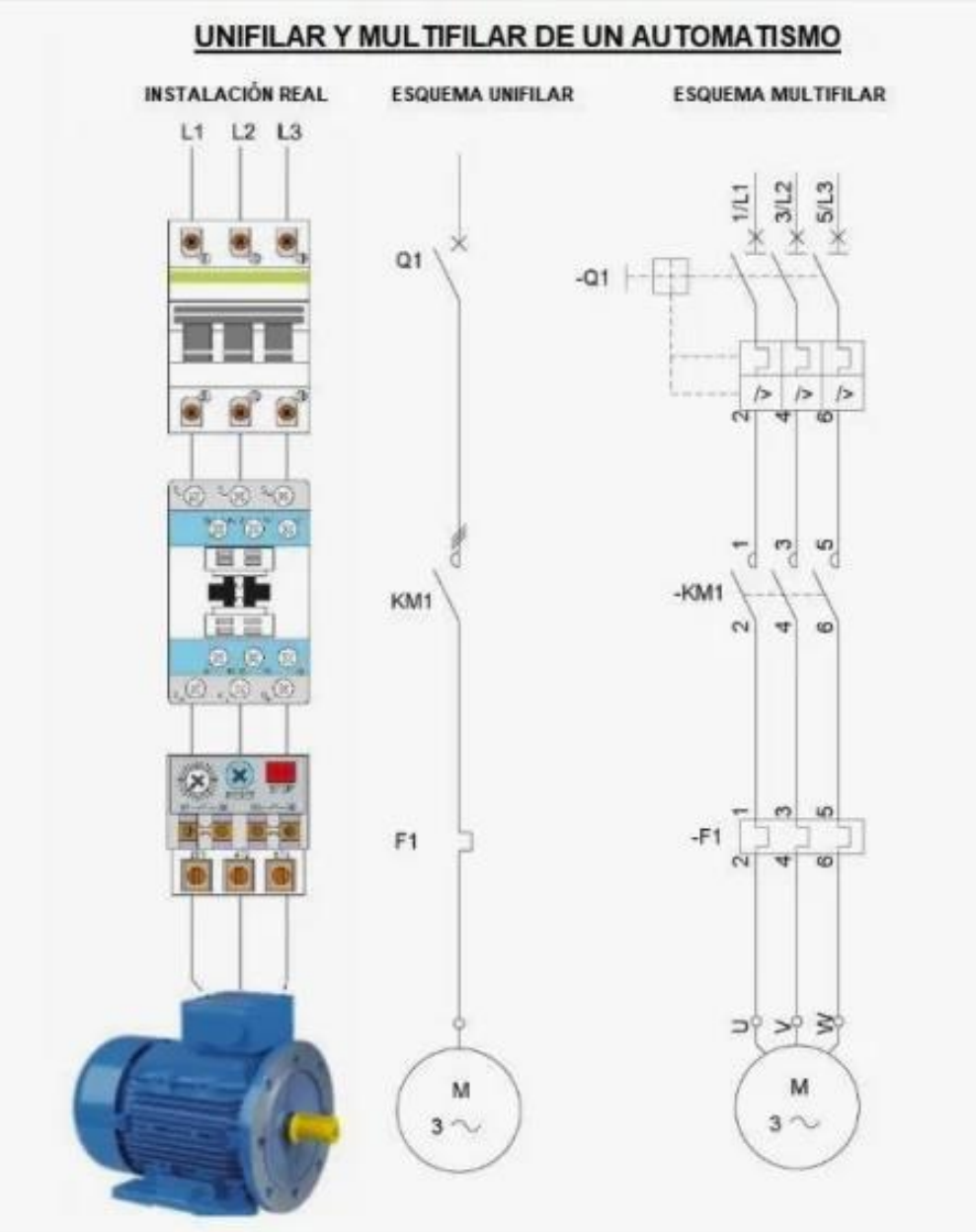
A través de este tipo de esquemas, se visualizan individualmente todos los conductores, elementos eléctricos (como interruptores, lámparas, motores, receptores), y sus relaciones eléctricas.

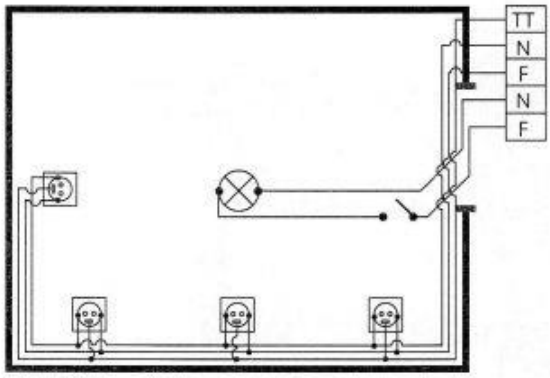
De todos los planos de las instalaciones eléctricas, el esquema mutifilar es una de las representaciones más completas y útiles en el diseño, análisis, instalación y mantenimiento de sistemas eléctricos.

No obstante, aunque estos esquemas pueden ser complejos y detallados, su utilidad en la práctica supera con creces sus limitaciones.

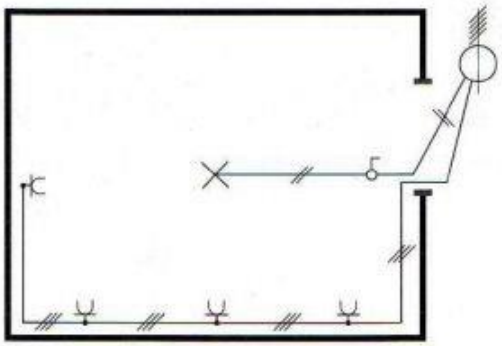
Aunque los diagramas multifilares no sitúan los elementos en el espacio real (paredes, techos, suelos) como lo haría un esquema topográfico, en ocasiones, se utiliza un esquema multifilar híbrido. Este esquema combina claridad técnica y ubicación práctica de los elementos eléctricos en el espacio.

Esta capacidad del esquema multifilar para adaptarse a diversas configuraciones lo hace imprescindible en cualquier proyecto de ingeniería eléctrica.





Plano Multifilar

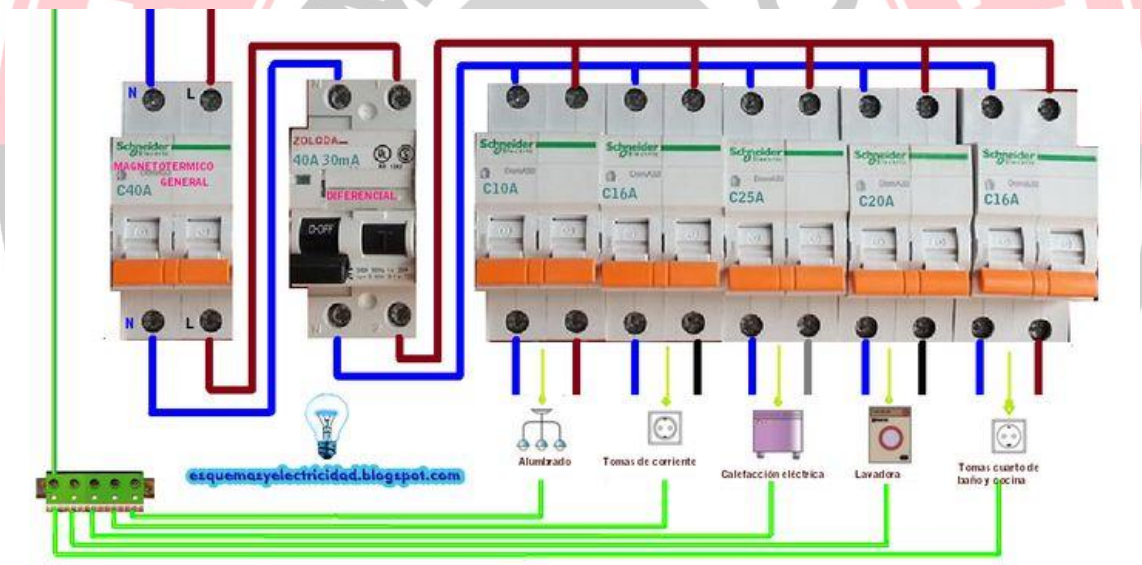


Plano Unifilar

1.3. ELEMENTOS DE UNA INSTALACIÓN ELÉCTRICA

1.3.1. CUADRO ELÉCTRICO:

Punto de distribución de energía, que contiene los dispositivos de protección.



Cuadro general de protección para una vivienda con grado de

El cuadro eléctrico es un elemento imprescindible en todo suministro de electricidad. Aunque normalmente solo echamos mano de él cuando nos saltan los plomos, es importante conocerlo, saber qué componentes básicos lo forman y para qué sirve cada uno. Esperamos que después de leer este post no te falte de nada :) (en este sentido).

¿QUÉ ES EL CUADRO ELÉCTRICO?

Aunque para personas no iniciadas, dependiendo de lo sofisticado de la instalación pueda parecer una especie de panel de control de una nave espacial, el cuadro de luz

no es tan complejo como lo pintan. Aunque, sin duda te permitirá controlar la electricidad de tu casa o tu negocio con la misma facilidad con la que Capitán Kirk controlaría la Enterprise.

El cuadro eléctrico, tanto en casas como en locales, suele estar en la parte de la entrada, por lo general protegido tras una portezuela de plástico (camuflada con más o menos gusto), llamado también armario eléctrico industrial. Puede que nunca tengas que acudir a él, pero para cuando se dé el caso, vamos a ponerte en situación presentándote sus elementos básicos y explicándote para qué sirven.

¿CÓMO FUNCIONA UN CUADRO ELÉCTRICO?

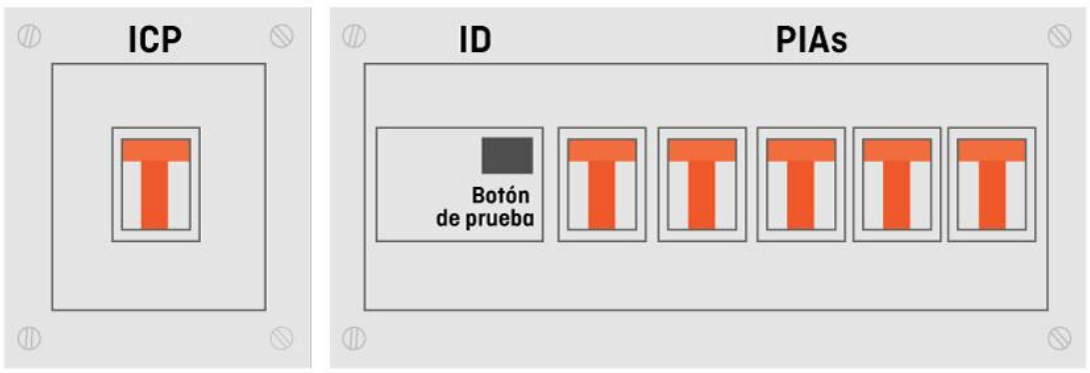
Su función principal es distribuir con seguridad la alimentación de energía eléctrica que llega desde la red hacia los circuitos auxiliares de la instalación eléctrica.

Dependiendo de cómo sean tu instalación y tu cuadro eléctrico, podrás usarlo para unas u otras funciones, pero en general desde aquí podrás desactivar toda la instalación o solo algunas partes, además de poder tomar medidas ciertas medidas de seguridad según convenga, sabiendo que el propio cuadro de luz cuenta con dispositivos como los diferenciales del cuadro eléctrico que protegen los circuitos eléctricos de tu instalación.

¿CUÁLES SON LOS COMPONENTES DEL CUADRO ELÉCTRICO?

En instalaciones domésticas por lo general encontramos un solo cuadro eléctrico, no así en instalaciones industriales o de grandes locales, en las que puede haber un cuadro principal alimentando uno o más cuadros secundarios.

A continuación, puedes ver el esquema del cuadro eléctrico estándar que hasta hace poco podíamos encontrar prácticamente en cualquier vivienda.

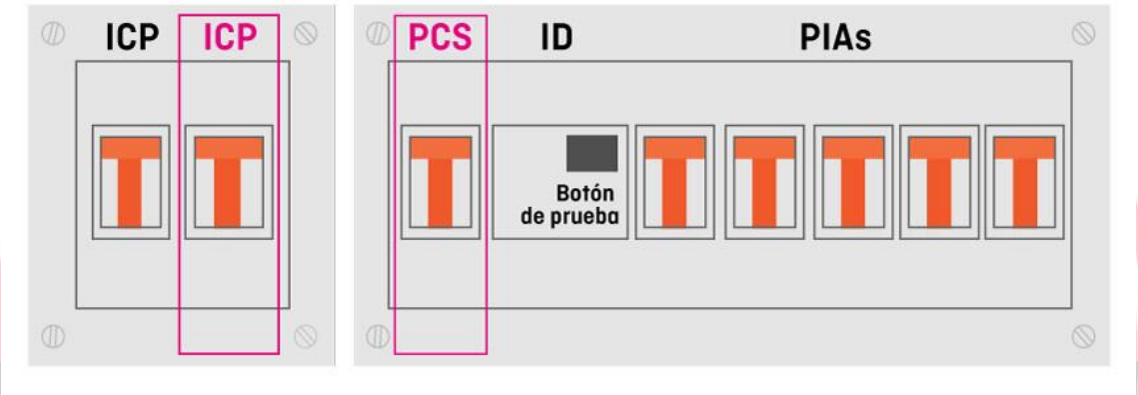


Suele contar con ICP (Interruptor de Control de Potencia), que es el que hace que “salten los plomos” cuando sobrepasas tu potencia contratada, apagando la instalación sobre todo por seguridad, o bien interrumpiendo el suministro eléctrico en caso de sobrecarga de la red, con el fin de evitar un mal mayor; ID (Interruptor Diferencial) que sirve para

desconectar la instalación, por ejemplo en caso de fuga, o derivaciones de corriente a tierra, interrumpiendo el suministro por seguridad.

Estos interruptores acostumbran a tener un Botón de prueba que permite comprobar el correcto funcionamiento de la instalación (y que los fabricantes aconsejan presionar una vez al mes); y por último PIAs (Pequeños interruptores automáticos) encargados de proteger cada uno de los circuitos interiores, de manera que puedas activar o desactivar de forma independiente iluminación, electrodomésticos o estancias. Es importante tener bien señalado cada circuito, ya que, si los interruptores saltan demasiado, puede significar que tengas demasiados aparatos en el mismo circuito o que exista una avería en alguno de ellos.

En este otro caso sería un modelo más reciente que podemos encontrar en instalaciones eléctricas relativamente nuevas:



En este caso, además de los componentes del ejemplo anterior, podemos encontrar el IGA (Interruptor General Automático), que sustituye al ICP en el cuadro (aunque este se incluye ahora en los nuevos contadores digitales) para controlar la potencia contratada y evitar sobrecargas y PCS (Protector Contra Sobretensiones), el dispositivo responsable de evitar que los aparatos eléctricos sufran daños derivados de posibles subidas de tensión.

1.3.1.1. CONDUCTORES ELÉCTRICOS

Los conductores eléctricos son materiales que permiten el flujo de la corriente eléctrica con baja resistencia. Se utilizan en instalaciones eléctricas para transportar energía desde la fuente de alimentación hasta los dispositivos de consumo. La elección del tipo de conductor depende de la aplicación, el nivel de tensión, las condiciones ambientales y los requisitos de seguridad.

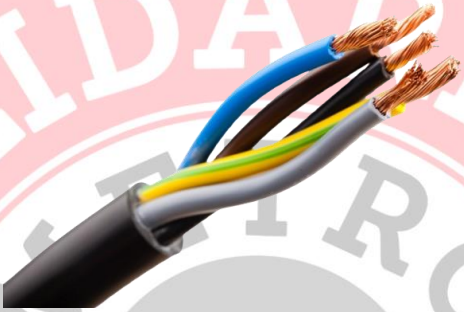
CLASIFICACIÓN DE LOS CONDUCTORES ELÉCTRICOS

Los conductores eléctricos pueden clasificarse según diferentes criterios, como el **material del conductor, la estructura del cableado, el aislamiento y la aplicación específica**.

SEGÚN EL MATERIAL DEL CONDUCTOR

El material del conductor influye en su capacidad de conducción, resistencia y aplicación.

1. **Cobre:**
    - Es el material más utilizado debido a su **alta conductividad** y resistencia mecánica.
    - Tiene **baja resistencia eléctrica**, lo que minimiza las pérdidas de energía.
    - Se emplea en **instalaciones eléctricas domésticas, industriales y de alta potencia**.



2. **Aluminio:**
    - Menos conductor que el cobre, pero **más ligero y económico**.
    - Se usa en **líneas de transmisión y distribución de energía eléctrica** debido a su menor peso.
    - Tiene mayor resistencia a la corrosión en aplicaciones exteriores.

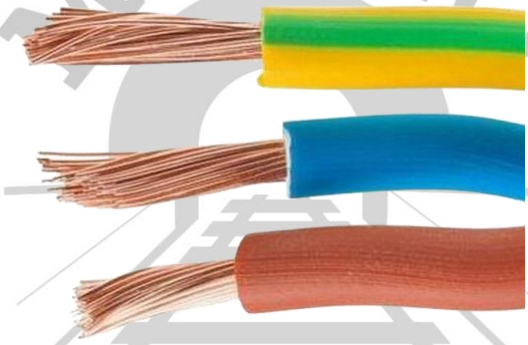
SEGÚN LA ESTRUCTURA DEL CABLEADO

Los conductores pueden presentarse en diferentes formas según su flexibilidad y resistencia mecánica.

1. **Conductores Sólidos (Hilos Únicos):**
    - Compuestos por un único hilo grueso de cobre o aluminio.

- Se utilizan en **instalaciones fijas** debido a su mayor rigidez.
- Ofrecen **menor resistencia eléctrica** pero menor flexibilidad.

2. **Conductores Trenzados o Multifilares:**
   - Formados por varios hilos finos trenzados juntos.
   - Mayor flexibilidad, lo que facilita su instalación en **zonas con movimiento o vibraciones**.
   - Se usan en **circuitos móviles, conexiones eléctricas flexibles y vehículos**.



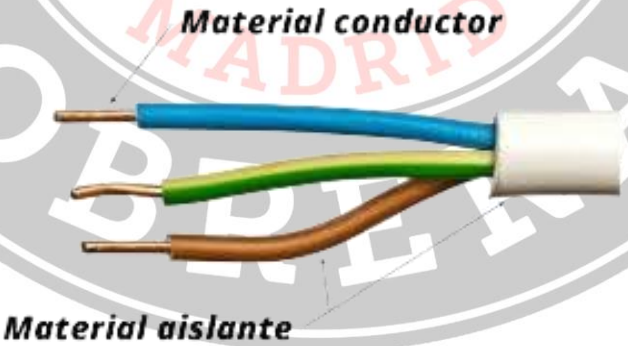
3. **Conductores Compactados:**
   - Combinan las ventajas de los conductores sólidos y trenzados.
   - Menor diámetro con mayor flexibilidad y conductividad.
   - Utilizados en **instalaciones de alta eficiencia energética**.

SEGÚN SU AISLAMIENTO

Los conductores pueden estar desnudos o aislados, dependiendo de la aplicación.

1. **Conductores Desnudos:**
   - No tienen recubrimiento aislante.
   - Se usan en **líneas de transmisión y distribución aérea**.
   - Deben instalarse con suficiente distancia entre ellos para evitar cortocircuitos.

2. **Conductores Aislados:**
   - Recubiertos con materiales como **PVC, XLPE, PE o goma**.
   - Se utilizan en **instalaciones domésticas, industriales y subterráneas**.
   - Protegen contra contactos accidentales y mejoran la durabilidad del conductor.



TIPOS DE AISLANTES Y RECUBRIMIENTOS:

1. **Policloruro de vinilo (PVC):**
   - Material más común en conductores eléctricos.
   - Alta resistencia mecánica y térmica.

- Usado en instalaciones domésticas e industriales.

2. **Polietileno Reticulado (XLPE):**

- Mayor capacidad de aislamiento térmico.
- Resistente a altas temperaturas y ambientes húmedos.
- Aplicado en cables de media y alta tensión.

3. **Etileno Propileno (EPR):**

- Resistente a la humedad y aceites.
- Utilizado en instalaciones submarinas y ambientes con alta humedad.

4. **Caucho de silicona:**

- Alta flexibilidad y resistencia al calor extremo.
- Empleado en equipos eléctricos de alto rendimiento.

5. **Libre de Halógenos (LSZH - Low Smoke Zero Halogen):**

- No emite gases tóxicos en caso de incendio.
- Recomendado en hospitales, aeropuertos y lugares con alta concentración de personas.

Los cables eléctricos están protegidos con materiales como PVC, XLPE o goma, los cuales garantizan seguridad y durabilidad en la instalación.

SEGÚN LA APLICACIÓN

Los conductores están diseñados para aplicaciones específicas según su entorno de uso.

1. **Conductores para Baja Tensión:**
   - Voltajes hasta **1000V en corriente alterna (CA)**.
   - Se emplean en **viviendas, oficinas y pequeñas industrias**.

2. **Conductores para Media Tensión:**
   - Voltajes entre **1kV y 36kV**.
   - Se usan en **redes de distribución y alimentación de grandes consumidores**.

3. **Conductores para Alta Tensión:**
    - Voltajes superiores a **36kV**.
    - Se utilizan en **líneas de transmisión de energía a largas distancias**.

4. **Conductores para Ambientes Especiales:**
    - **Ignífugos:** Resistentes al fuego para **salidas de emergencia y lugares públicos**.
    - **Resistentes a la humedad:** Para **ambientes marinos y subterráneos**.
    - **Libres de halógenos:** No generan gases tóxicos en caso de incendio.

Conclusión

La correcta selección del **tipo de conductor eléctrico** es esencial para garantizar la seguridad, eficiencia y durabilidad de una instalación eléctrica. Factores como la **conductividad, flexibilidad, aislamiento y aplicación** deben evaluarse antes de su instalación.

SEGÚN SU SECCIÓN

Las secciones de los circuitos de las viviendas deberán ser adecuadas para garantizar la **seguridad**, el **buen funcionamiento** y la **eficiencia** de la instalación.

La **sección adecuada de cada conductor se calcula tomando en cuenta diversos factores**, incluyendo la intensidad de corriente, la longitud, el tipo de conductor, el tipo de aislamiento y las condiciones de instalación.

La **ITC-BT-25** del REBT proporciona las **características de los circuitos de las viviendas**, indicando las secciones mínimas de cada uno de los diferentes circuitos en las instalaciones residenciales.

Estas secciones mínimas proporcionadas son para circuitos **en viviendas normales**, es decir, sin grandes longitudes. Para su cálculo, se tiene en cuenta:

– **La corriente del interruptor automático (IA)**: el REBT establece que la sección del conductor debe ser capaz de soportar la corriente nominal del IA sin sobrecalentarse.

– **Una caída de tensión máxima del 3%**: el REBT limita la caída de tensión en los circuitos a un máximo del 3% para garantizar un correcto funcionamiento de los equipos conectados.

– **Un factor de potencia (cos ϕ) de 1**: el REBT asume un caso simplificado donde el cos ϕ es igual a 1, lo que corresponde a una carga puramente resistiva (como resistencias calefactoras).

Por ello, para circuitos con **longitudes considerables**, el **cálculo de instalaciones en viviendas** supone comprobar si las secciones mínimas son suficientes. Además, puede ser necesario considerar factores adicionales como la temperatura ambiente, el método de instalación o la presencia de aislamientos térmicos en paredes.

Longitudes Máximas de los Circuitos de las Viviendas

La **guía técnica de la ITC-BT-25** proporciona una tabla que indica los valores máximos de longitud para los conductores eléctricos. Estos valores se determinan considerando la sección del conductor y la intensidad nominal del dispositivo de protección. El objetivo es el de mantener una **caída de tensión máxima del 3%**.

Esta tabla se basa en una **temperatura ambiente estimada de 40ºC** y un **factor de potencia de cos ϕ = 1**. En los casos donde las longitudes de los conductores superen los valores máximos especificados en la tabla, es necesario aumentar la sección mínima reglamentaria de los conductores. Con este ajuste aseguraremos que la caída de tensión no exceda del 3%.

Además, al aumentar la sección de los conductores, el **tubo** utilizado para la instalación debe ser adecuado conforme a las especificaciones de las tablas de la **ITC-BT-21**. Esto garantiza que los conductores tengan el espacio necesario para disipar el calor y que la instalación cumpla con el REBT.

Sección del conductor (mm^2)	Intensidad nominal del dispositivo de protección (A)			
	10	**16**	**20**	**25**
1,5	24 m			
2,5	41 m	25 m		
4		41 m	33 m	
6			49 m	39 m

1.3.2. PROTECCIÓN Y SEGURIDAD ELÉCTRICA

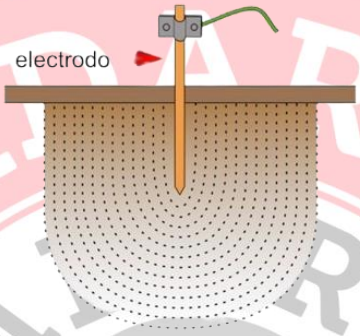
La seguridad en instalaciones eléctricas es esencial para prevenir accidentes y fallos que puedan ocasionar daños materiales o personales.

1.3.2.1. SISTEMAS DE PROTECCIÓN ELÉCTRICA

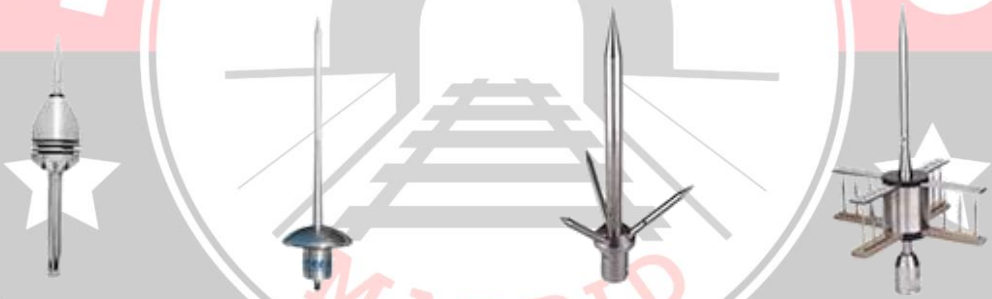
1. **Interruptores magnetotérmicos**: Protegen contra sobrecargas y cortocircuitos.

2. **Interruptores diferenciales**: Detectan fugas de corriente y evitan descargas eléctricas.

3. **Puesta a tierra**: Conduce cargas eléctricas no deseadas hacia el suelo.



4. **Pararrayos**: Protegen contra descargas eléctricas atmosféricas.



5. **Fusibles**: Dispositivos de protección que evitan el paso de corriente excesiva.

1.4. NORMATIVA APLICABLE A INSTALACIONES ELÉCTRICAS

Las **normativas eléctricas** establecen las regulaciones y estándares de seguridad, eficiencia y fiabilidad en el diseño, instalación y mantenimiento de sistemas eléctricos en entornos residenciales, comerciales e industriales. Su aplicación garantiza la protección de las personas, los equipos y las infraestructuras, reduciendo riesgos como cortocircuitos, incendios y descargas eléctricas.

1.4.1. PRINCIPALES NORMATIVAS ELÉCTRICAS

1.4.1.1. NORMATIVA IEC (COMISIÓN ELECTROTÉCNICA INTERNACIONAL):

La **Normativa IEC (Comisión Electrotécnica Internacional)** establece estándares globales para la seguridad y eficiencia de las instalaciones y dispositivos eléctricos. Su objetivo principal es garantizar la compatibilidad, seguridad y calidad en los sistemas eléctricos, promoviendo regulaciones que faciliten la interoperabilidad de equipos en distintos países.

Los estándares IEC abarcan áreas como la protección contra sobrecargas, el diseño de instalaciones eléctricas, la certificación de componentes electrónicos y las normativas para la eficiencia energética. También regulan la seguridad en la manipulación de sistemas eléctricos y establecen criterios para minimizar riesgos de fallos eléctricos en entornos residenciales, comerciales e industriales.

Esta normativa es adoptada por diversos países y sirve de referencia para la creación de regulaciones locales, asegurando un marco técnico confiable para la industria eléctrica y electrónica.

1.4.1.2. REGLAMENTO ELECTROTÉCNICO DE BAJA TENSIÓN (REBT):

Aplicado en muchos países para regular las instalaciones en edificios residenciales e industriales.

Es la normativa que establece los requisitos técnicos y de seguridad que deben cumplir las instalaciones eléctricas de baja tensión en España. Su objetivo principal es garantizar la seguridad de las personas y los bienes, así como la eficiencia energética y el correcto funcionamiento de las instalaciones eléctricas.

CARACTERÍSTICAS PRINCIPALES DEL REBT

1. **Ámbito de aplicación:**

   - Se aplica a todas las instalaciones eléctricas de **baja tensión** (menores o iguales a 1000V en corriente alterna y 1500V en corriente continua).

- Afecta a instalaciones en **viviendas, edificios, locales comerciales, industrias y espacios públicos**.

2. **Estructura y contenido:**

   - Se compone de un **reglamento general** y varias **instrucciones técnicas complementarias (ITC-BT)**, que desarrollan aspectos específicos como protección, dimensionamiento de conductores, puesta a tierra y eficiencia energética.

3. **Objetivos principales:**

   - Garantizar la **seguridad de las personas y bienes** ante riesgos eléctricos.
   - Asegurar la **eficiencia energética** en las instalaciones eléctricas.
   - Regular los **procedimientos de inspección, verificación y mantenimiento** de las instalaciones.

PRINCIPALES ASPECTOS REGULADOS POR EL REBT

1. **Diseño y ejecución de instalaciones eléctricas**

   - Criterios para el diseño y cálculo de instalaciones de baja tensión.
   - Selección de materiales y equipos conforme a normas de calidad y seguridad.

2. **Protecciones eléctricas**

   - Protección contra sobrecargas y cortocircuitos mediante interruptores automáticos y fusibles.
   - Protección diferencial para evitar contactos eléctricos indirectos y directos.

3. **Instalaciones en diferentes entornos**

   - Requisitos para instalaciones en viviendas, industrias, locales comerciales y locales de pública concurrencia.
   - Normativas para instalaciones en lugares con riesgo de explosión (ATEX).

4. **Puesta a tierra y seguridad**

   - Sistemas de protección contra descargas eléctricas.
   - Requisitos para la instalación de sistemas de puesta a tierra y pararrayos.

5. **Eficiencia energética y sostenibilidad**

   - Normativas para reducir el consumo de energía en edificios.
   - Uso de iluminación eficiente y energías renovables en instalaciones eléctricas.
   -

IMPORTANCIA DEL REBT EN LAS INSTALACIONES ELÉCTRICAS

- **Obligatorio**: Todas las instalaciones eléctricas nuevas y reformas deben cumplir con el REBT.
- **Garantiza la seguridad**: Minimiza riesgos eléctricos en instalaciones residenciales, comerciales e industriales.
- **Control y supervisión**: Establece requisitos para inspecciones periódicas y certificaciones eléctricas.

El **REBT** es la referencia fundamental para el diseño, instalación y mantenimiento de sistemas eléctricos de baja tensión en España.

1.4.1.3. CÓDIGO ELÉCTRICO NACIONAL (NEC):

El **Código Eléctrico Nacional (NEC)** es una normativa de seguridad utilizada principalmente en Estados Unidos para regular el diseño, instalación y mantenimiento de sistemas eléctricos. Su objetivo es garantizar la seguridad en las instalaciones eléctricas residenciales, comerciales e industriales, reduciendo riesgos de incendios, descargas eléctricas y fallos en los equipos.

El NEC establece especificaciones sobre el uso de conductores, protección contra sobrecargas, sistemas de puesta a tierra, dispositivos de protección y distancias mínimas de seguridad. Además, regula el uso de materiales y métodos adecuados para garantizar la eficiencia y confiabilidad de las instalaciones eléctricas.

Si bien es de aplicación en Estados Unidos, muchos países adoptan sus lineamientos como referencia para sus propias normativas eléctricas, asegurando estándares de seguridad y eficiencia en la distribución y consumo de energía eléctrica.

1.4.1.4. NORMAS DE EFICIENCIA ENERGÉTICA:

Las **Normas de eficiencia energética en instalaciones eléctricas residenciales y comerciales** establecen directrices para optimizar el consumo de energía y reducir pérdidas eléctricas. Su objetivo es garantizar el uso racional de la electricidad mediante la implementación de tecnologías eficientes, el diseño adecuado de las instalaciones y la aplicación de estrategias de ahorro energético.

Entre sus principales lineamientos se encuentran:

- **Uso de dispositivos de bajo consumo**, como bombillas LED, electrodomésticos con certificación energética y sistemas de climatización eficientes.
- **Optimización del cableado eléctrico**, evitando pérdidas por sobrecalentamiento y reduciendo caídas de tensión.
- **Implementación de sistemas de automatización y control**, como sensores de movimiento y temporizadores para la gestión inteligente de la iluminación y el consumo eléctrico.

- **Incorporación de fuentes de energía renovable**, como paneles solares fotovoltaicos, para reducir la dependencia de la red eléctrica convencional.
- **Cumplimiento de normativas internacionales**, como IEC y NEC, que regulan los estándares de eficiencia en el diseño y operación de instalaciones eléctricas.

Estas normas buscan no solo reducir el impacto ambiental, sino también mejorar la seguridad y reducir los costos de operación en edificios residenciales y comerciales, promoviendo un uso más sostenible de la electricidad.

1.4.1.5. NORMAS DE PREVENCIÓN DE RIESGOS LABORALES:

Las **Normas de prevención de riesgos laborales en instalaciones eléctricas residenciales y comerciales** están diseñadas para garantizar la seguridad de los trabajadores y usuarios al manipular sistemas eléctricos. Su principal objetivo es prevenir accidentes como descargas eléctricas, cortocircuitos, incendios y fallos estructurales en la red eléctrica.

Entre las medidas clave se incluyen:

- **Uso de equipos de protección personal (EPP)**, como guantes aislantes, gafas de seguridad y calzado dieléctrico.
- **Implementación de sistemas de protección**, como interruptores diferenciales, puesta a tierra y fusibles.
- **Cumplimiento de distancias de seguridad** en tableros eléctricos y cableados para evitar contactos accidentales.
- **Mantenimiento y revisión periódica** de las instalaciones para detectar fallos antes de que representen un peligro.
- **Capacitación del personal** en procedimientos de trabajo seguro, identificación de riesgos y respuesta ante emergencias eléctricas.

Estas normas están reguladas por organismos nacionales e internacionales, como la **Normativa IEC, el Código Eléctrico Nacional (NEC) y reglamentos de seguridad laboral**, asegurando un entorno seguro en la instalación y mantenimiento de sistemas eléctricos.

1.4.2. APLICACIÓN DE LA NORMATIVA EN PROYECTOS ELÉCTRICOS

- Uso de materiales certificados y homologados.
- Diseño de instalaciones de acuerdo con las regulaciones vigentes.
- Cumplimiento de distancias de seguridad y limitaciones de carga.
- Documentación y registro de inspecciones técnicas.
- Capacitación y certificación del personal encargado de instalaciones eléctricas.

El cumplimiento de normativas garantiza la seguridad de las instalaciones y previene problemas legales y técnicos.

2. ELECTRÓNICA APLICADA

2.1. INTRODUCCIÓN A LA ELECTRÓNICA

La electrónica es la rama de la física y la ingeniería que estudia y aplica el comportamiento de los electrones en distintos dispositivos y sistemas. Su importancia radica en su presencia en la mayoría de los dispositivos tecnológicos modernos, desde teléfonos móviles hasta sistemas industriales avanzados.

Se puede clasificar en:

- **Electrónica analógica**: Maneja señales continuas.
- **Electrónica digital**: Trabaja con señales discretas, principalmente binarias.
- **Electrónica de potencia**: Se enfoca en el control de la energía eléctrica.
- **Electrónica de telecomunicaciones**: Se especializa en la transmisión y recepción de señales.

2.2. COMPONENTES ELECTRÓNICOS BÁSICOS

Los circuitos electrónicos están compuestos por distintos elementos que cumplen funciones específicas. Algunos de los principales son:

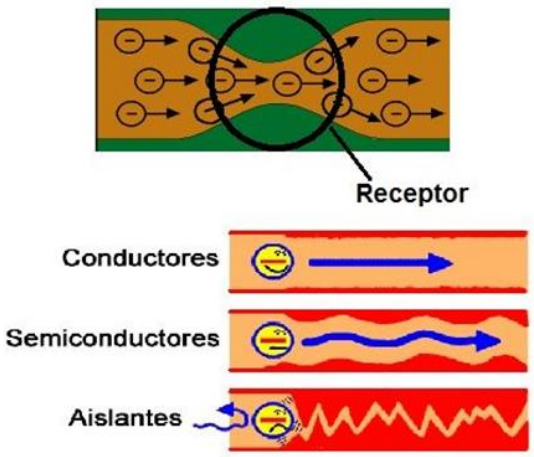
2.2.1. RESISTENCIAS:

La resistencia eléctrica es la oposición (dificultad) al paso de la corriente eléctrica. Sabemos que la corriente eléctrica es el paso (movimiento) de electrones por un circuito o, a través de un elemento de un circuito (receptor). Según lo dicho podemos concluir que **"la corriente eléctrica es un movimiento de electrones".**

Dependiendo del tipo, material y sección (grosor) de cable o conductor por el que tengan que pasar los electrones les costará más o menos trabajo. Un buen conductor casi no le ofrecerá resistencia a su paso por él, un aislante les ofrecerá tanta resistencia que los electrones no podrán pasar a través de él. Ese esfuerzo que tienen que vencer los electrones para circular, es precisamente la **Resistencia Eléctrica**. Luego lo veremos más detalladamente.

Además, estos electrones cuando llegan algún receptor, como por ejemplo una lámpara, para pasar a través de ella les cuesta más trabajo, es decir, también les ofrece resistencia a que pasen por el receptor.

Como ves, en un circuito eléctrico encontramos resistencia en los propios cables o conductores y en los receptores (lámparas, motores, etc.).



Veamos esto mediante la fórmula de la Ley de Ohm, formula fundamental de los circuitos eléctricos:

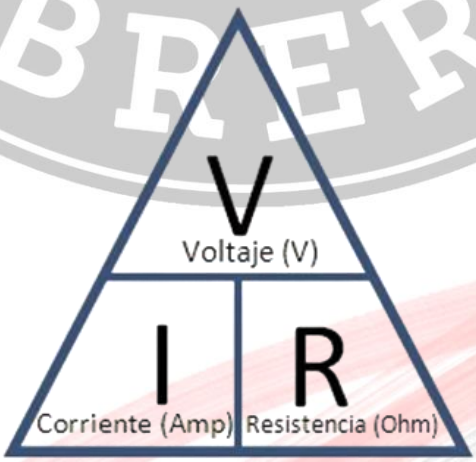
Esta fórmula nos dice que la Intensidad o Intensidad de Corriente Eléctrica (I) que recorre un circuito o que atraviesa cualquier elemento de un circuito, es igual a la Tensión (V) a la que está conectado, dividido por su Resistencia (R). Esta fórmula nos sirve para calcular la resistencia de un elemento dentro de un circuito o la del circuito entero.

Según esta fórmula en un circuito o en un receptor que esté sometido a una tensión constante (por ejemplo, a la tensión de una pila de 4V) la intensidad que lo recorre será menor cuanto más grande sea su resistencia.

Comprobado: la resistencia se opone al paso de la corriente, a más R menos I, según la Ley de Ohm.

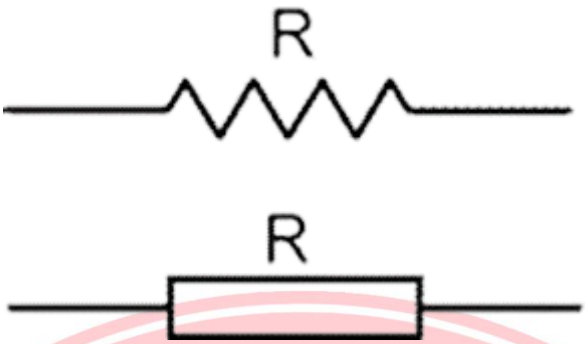
Todos los elementos de un circuito tienen resistencia eléctrica. La resistencia eléctrica se mide en Ohmios (Ω) y se representa con la letra R.

En un circuito de corriente continua podemos calcular la resistencia despejándola de la fórmula de la ley de ohm:



V en voltios e I en amperios nos dará la resistencia en Ohmios (Ω).

Para el símbolo de la resistencia eléctrica, dentro de los circuitos eléctricos, podemos usar dos diferentes:



Da igual usar un símbolo u otro.

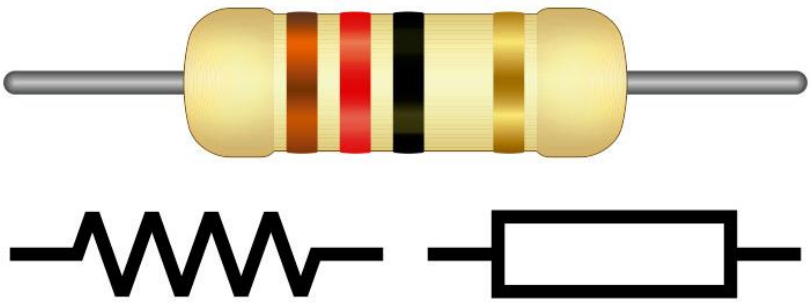
Aunque en los circuitos pequeños la resistencia de los conductores se considera la mayoría de las veces cero, cuando hablamos de circuitos donde los cables son muy largos, debemos calcular el valor de la resistencia del conductor entre un extremo y el otro del cable. Más adelante veremos cómo se hace.

Ya sabemos que los elementos de un circuito tienen resistencia eléctrica, pero lógicamente unos tienen más que otros.

A parte de la resistencia de los receptores también hay unos elementos que se colocan dentro de los circuitos y que su única función es precisamente esa, oponerse al paso de la corriente u ofrecer resistencia al paso de la corriente para limitarla y que nunca supere una cantidad de corriente determinada. Son muy usados en electrónica.

Un elemento de este tipo también se llama también Resistencia Eléctrica. A continuación, vemos como se calcula su valor Y algunas de las más usadas.

Como se calcula su valor

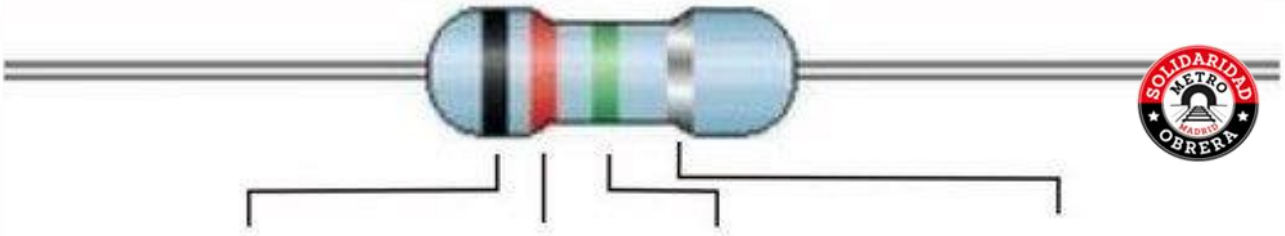


De este tipo de resistencias, las que se usan para limitar la corriente en un circuito o por parte de él, es de las que vamos a hablar a continuación. Hay muchos tipos diferentes y se fabrican de materiales diferentes.

El valor de una resistencia de este tipo viene determinado por su código de colores. Vemos en la figura anterior varias resistencias, y como las resistencias vienen con unas franjas o bandas de colores. Estas franjas, mediante un código, determinan el valor que tiene la resistencia.

Código de Colores Para Resistencias

Para saber el valor de una resistencia tenemos que fijarnos que tiene 3 bandas de colores seguidas y una cuarta más separada. Las 3 primeras bandas nos dicen su valor, la cuarta banda nos indica la tolerancia, es decir el valor + - el valor que puede tener por encima o por debajo del valor que marcan las 3 primeras bandas.



Color	1ra. Banda	2da. Banda	3ra. Banda Multiplicador	Tolerancia %
Negro	0	0	x1	
Cafe	1	1	x10	
Rojo	2	2	x100	2%
Naranja	3	3	x1000	
Amarillo	4	4	x10000	
Verde	5	5	x100000	
Azul	6	6	x1000000	
Violeta	7	7	x10000000	
Gris	8	8	x100000000	
Blanco	9	9	x1000000000	
				Dorado 5%
				Plata 10%

Circuitos Básicos

El Valor real de una resistencia lo podemos averiguar mediante el polímetro, aparato de medidas eléctricas, incluida el valor de la resistencia eléctrica. También con el Fluke usado por la mayoría de los electricistas.

Valor de la Resistencia entre 2 Puntos de un cable

Ya sabemos que para calcular el valor de la resistencia de un elemento dentro de un circuito se hace mediante la ley de ohm R = V/I. Pero a veces es necesario calcular la resistencia de un cable desde un extremo a otro.

Imaginemos que queremos calcular la resistencia que tendrá el paso de la corriente entre dos puntos de un circuito en el que solo hay cable. Ya dijimos que en los cables casi no hay resistencia, pero en algunos casos hay que calcular la resistencia que tiene el

cable, sobre todo en distancias largas o en bobinas de cables. Para estos casos la fórmula para hallar la resistencia es:

$$R = \rho \frac{L}{s}$$

Donde L es la longitud del cable, S la sección del cable y p es la resistividad del conductor o cable, un valor que nos da el fabricante del cable. La L se pone en metros, la Sección o diámetro en mm cuadrados y la resistencia nos dará en ohmios.

+

Tipos de Resistencias

En función de su funcionamiento tenemos:

- **Resistencias fijas:** Son las que presentan un valor que no podemos modificar.

- **Resistencias variables:** Son las que presentan un valor que nosotros podemos variar codificando la posición de un contacto deslizante. A este tipo de resistencia variables se le llama Potenciómetro.

- **Resistencias especiales:** Son las que varían su valor en función de la estimulación que reciben de un factor externo (luz, temperatura...). Por ejemplo, las LDR son las que varían su valor en función de la luz que incide sobre ellas.

TIPOS DE RESISTORES

Película de carbón
- 5%, 10%
- Barato
- Propósito general

Óxido metálico
- Mayor potencia

Película metálica
- Precisión 1%
- Alto desempeño

Alambre
- Alta potencia, Alta corriente

SMD para circuitos impresos

Alta Potencia

2.2.2. CONDENSADORES:

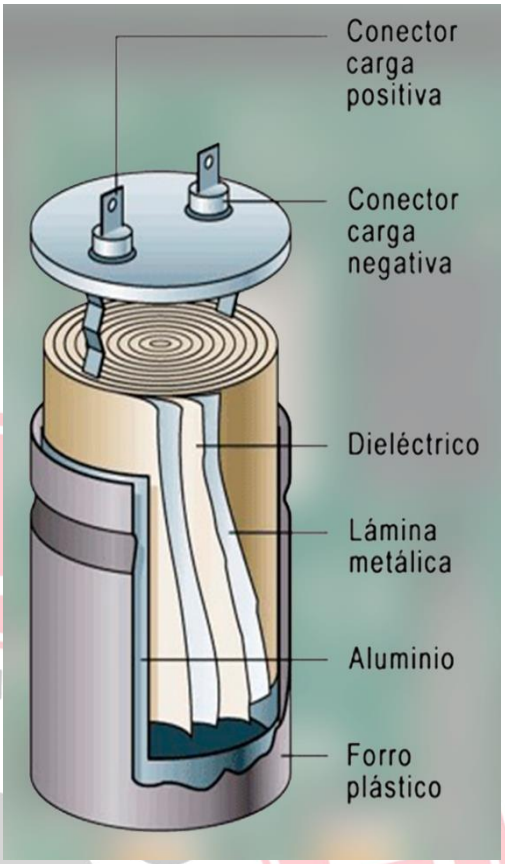
INTRODUCCIÓN A LOS CONDENSADORES

Los condensadores son componentes eléctricos pasivos que almacenan energía en un campo eléctrico. Están compuestos por dos placas conductoras separadas por un material dieléctrico, el cual impide el paso directo de corriente, pero permite la acumulación de carga en las placas.

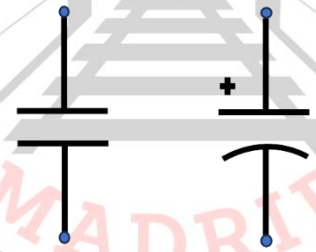
PARTES DE UN CONDENSADOR

Un condensador está compuesto por los siguientes elementos principales:

1. **Placas Conductoras**: Son las superficies metálicas encargadas de almacenar la carga eléctrica. Estas placas pueden estar hechas de aluminio, cobre u otros metales conductores.
2. **Dieléctrico**: Es el material aislante que separa las placas conductoras. Puede estar compuesto de cerámica, mica, papel, plástico o incluso aire, dependiendo del tipo de condensador.
3. **Terminales**: Son los puntos de conexión eléctrica que permiten integrar el condensador a un circuito. Generalmente, se encuentran soldados a las placas conductoras.
4. **Cubierta o Encapsulado**: En muchos condensadores, especialmente los comerciales, se emplea una cubierta protectora hecha de plástico o metal para proteger los elementos internos de la humedad, el polvo y otros factores ambientales.



¿CUÁL ES EL SÍMBOLO DEL CAPACITOR?



El **símbolo del capacitor** en los esquemas eléctricos es esencial para representar este componente de manera clara. Se utiliza un par de líneas paralelas, que simbolizan las placas del condensador, con una curva o líneas onduladas entre ellas para indicar el dieléctrico. Este símbolo proporciona una representación visual rápida y reconocible en los diagramas eléctricos.

¿CÓMO FUNCIONA UN CAPACITOR?

El funcionamiento de un **capacitor** o **condensador** se basa en el principio de almacenamiento de carga eléctrica. Un condensador está compuesto por dos placas conductoras separadas por un material dieléctrico. Aquí te explicaré paso a paso cómo se produce este proceso:

1. **Almacenamiento de carga:** Cuando se aplica un voltaje a través de las placas del condensador, se inicia un proceso de carga. Las cargas positivas se acumulan en una de las placas, mientras que las cargas negativas se acumulan en la otra. Este movimiento de electrones crea un campo eléctrico entre las placas.

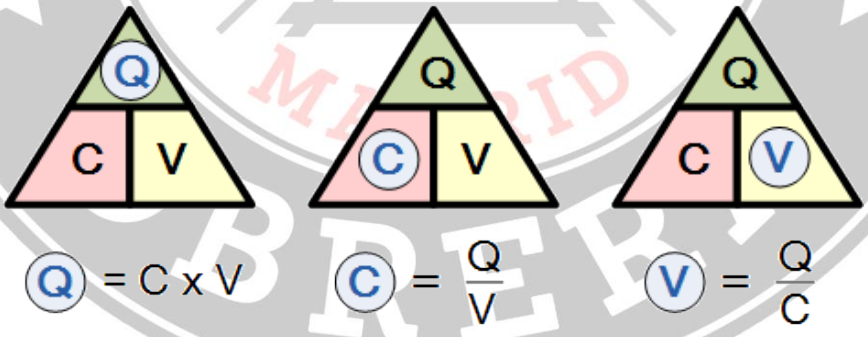
2. **Campo eléctrico:** El campo eléctrico generado por las cargas almacenadas es esencial en el funcionamiento del condensador. Este campo puede almacenar energía en forma de carga eléctrica, actuando como un reservorio temporal.
3. **Almacenamiento de energía:** A medida que se acumulan más cargas en las placas, la capacidad del condensador para almacenar energía eléctrica aumenta. Esta energía queda almacenada en el campo eléctrico creado entre las placas.
4. **Liberación de energía:** Cuando se conecta el condensador a un circuito, la energía almacenada se libera. Las cargas fluyen desde una placa a la otra, generando una corriente eléctrica en el circuito conectado.
5. **Descarga:** Después de la liberación de energía, el condensador se descarga gradualmente hasta que su carga eléctrica se reduce a cero. Este proceso puede repetirse múltiples veces, dependiendo de la aplicación específica del condensador en el circuito.

El funcionamiento del condensador es fundamental en diversas aplicaciones electrónicas. Desde su uso en filtros de señales hasta la estabilización de voltajes, los condensadores desempeñan un papel crucial en la optimización y control de circuitos eléctricos. Su capacidad para almacenar y liberar energía de manera eficiente los convierte en componentes esenciales en el diseño electrónico.

PRINCIPIO DE FUNCIONAMIENTO

El funcionamiento de un condensador se basa en el almacenamiento de carga eléctrica cuando se conecta a una fuente de voltaje. Cuando se aplica una diferencia de potencial entre sus placas, los electrones se acumulan en una de ellas, generando un campo eléctrico que almacena energía.

La cantidad de carga (*Q*) almacenada en un condensador es proporcional al voltaje (*V*) aplicado, según la ecuación:



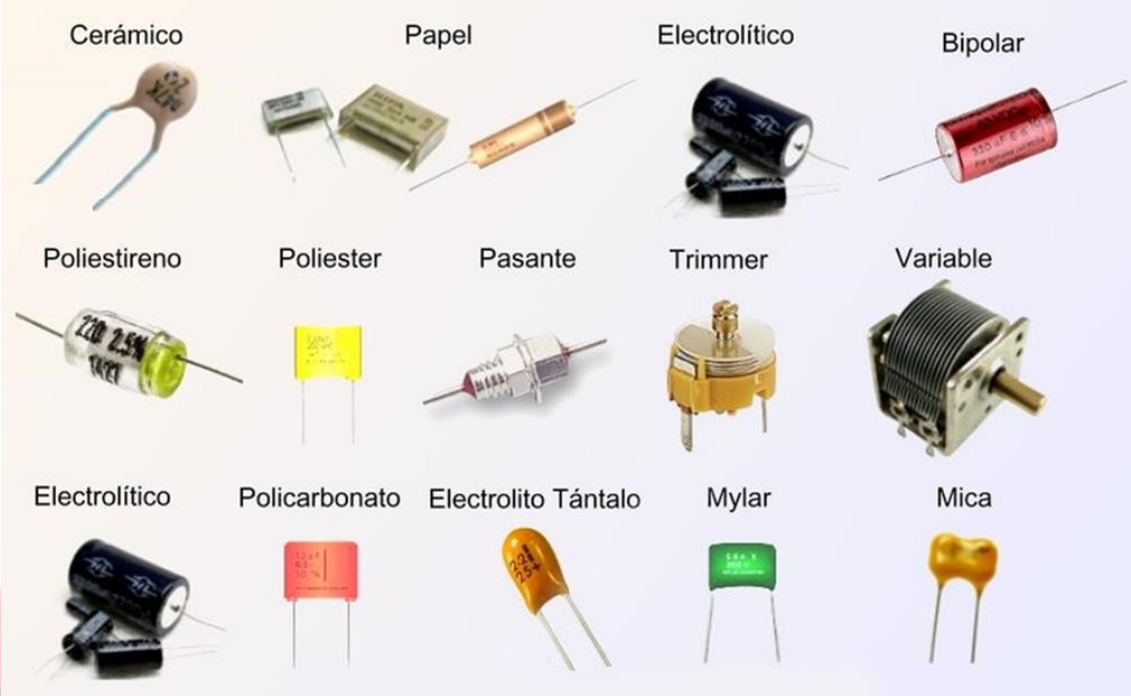
Donde *C* es la capacitancia, medida en faradios (F), y representa la capacidad del condensador para almacenar carga.

¿CUÁL ES LA UNIDAD DE MEDIDA DE LOS CAPACITORES?

La **unidad de medida de los capacitores** es el **faradio (F)**, en honor al científico Michael Faraday. Sin embargo, debido a la magnitud de los valores típicos, se utilizan subunidades como el microfaradio (µF) y el picofaradio (pF). Estas unidades reflejan la capacidad del condensador para almacenar carga.

TIPOS DE CAPACITORES

Existen diversos **tipos de condensadores** diseñados para adaptarse a diferentes aplicaciones. Entre ellos se incluyen los electrolíticos, cerámicos, de tantalio y variables. Cada tipo tiene sus propias características y ventajas, lo que permite a los ingenieros elegir el componente más adecuado para sus diseños.



Electrolíticos:

- **Electrolíticos de Aluminio:** Destacan por su alta capacidad y son comúnmente utilizados en fuentes de alimentación y amplificadores.
- **Electrolíticos de Tántalo:** Con un tamaño más pequeño que los de aluminio, son ideales en dispositivos electrónicos compactos y aplicaciones de alta frecuencia.

Cerámicos

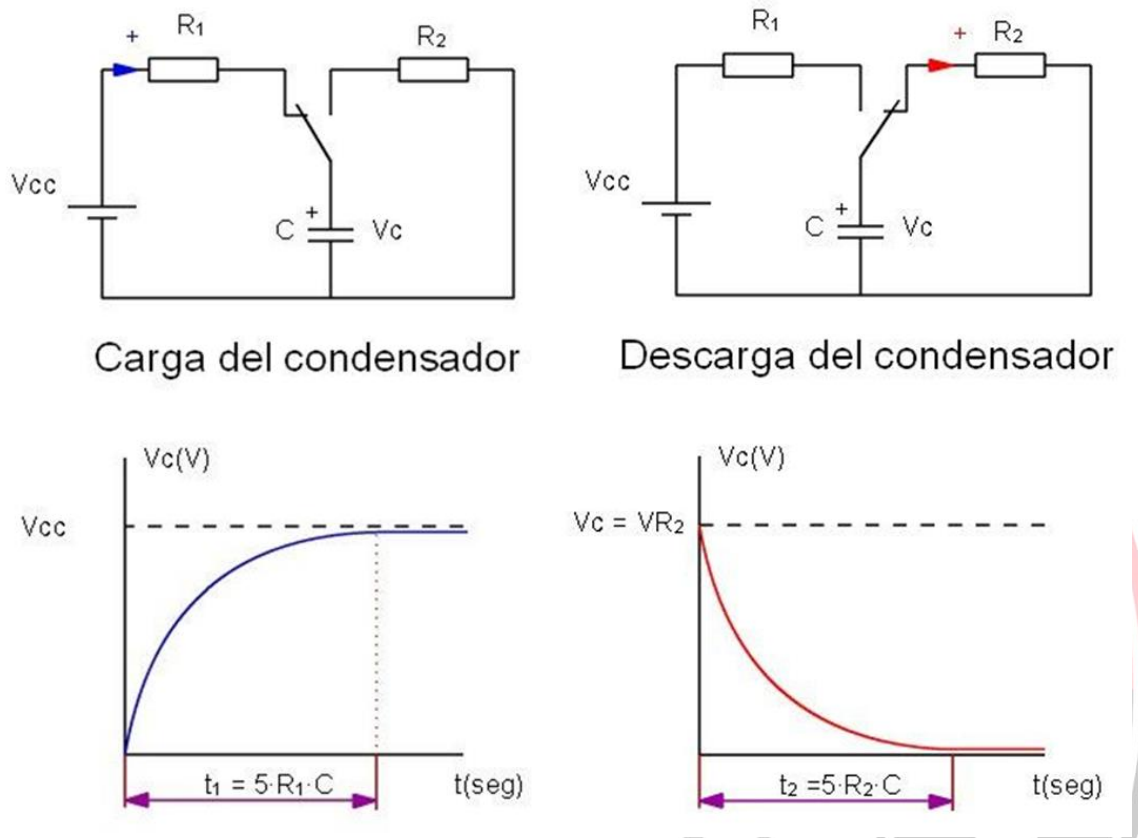
- **Multicapa:** Ofrecen estabilidad y se utilizan en aplicaciones de alta frecuencia, como en circuitos integrados y microcontroladores.
- **Monocapa:** Más simples y económicos, se emplean en aplicaciones de baja frecuencia.

Variables:

- **Capacitores de Ajuste:** Se utilizan para sintonizar circuitos y ajustar frecuencias en radios y transmisores.
- **Capacitores de Trimmer:** Ajustables con herramientas, son útiles en prototipos y ajustes finos de circuitos.

La elección del tipo de capacitor depende de factores como la aplicación específica, la frecuencia de operación, el espacio disponible y las características eléctricas requeridas. Cada tipo tiene sus propias ventajas y limitaciones, permitiendo a los diseñadores seleccionar el componente más adecuado para sus proyectos electrónicos.

CARGA Y DESCARGA DE UN CONDENSADOR



CARACTERÍSTICAS PRINCIPALES

Los condensadores presentan varias características fundamentales:

- **Capacitancia (C)**: Capacidad de almacenar carga eléctrica.
- **Tensión de Trabajo**: Voltaje máximo que puede soportar sin dañarse.
- **Tolerancia**: Variación permitida en la capacitancia nominal.
- **Resistencia Serie Equivalente (ESR)**: Indica las pérdidas internas del condensador.
- **Tiempo de Respuesta**: Determina la velocidad de carga y descarga en circuitos.

CÓMO LEER EL VALOR DE UN CAPACITOR

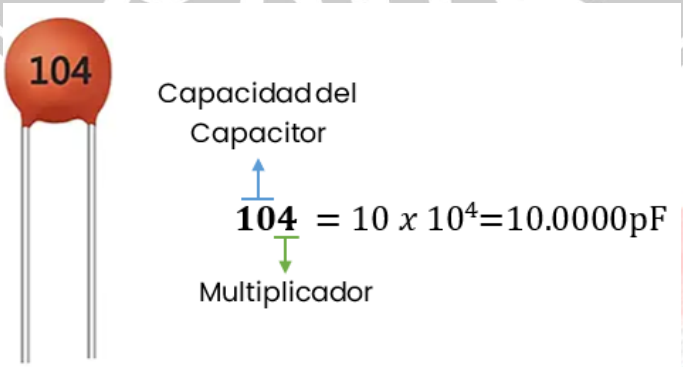
Leer el valor de un **capacitor** puede realizarse de varias maneras, y aquí te explico dos de las más comunes:

MARCAS IMPRESAS O GRABADAS:

- Algunos capacitores tienen el **valor impreso** directamente en su carcasa. Puedes encontrar números que indican la capacitancia en microfaradios (µF) o picofaradios (pF). A veces, también se incluyen letras que representan la tolerancia.
- **Ejemplo:** Si ves «10uF 450V», el capacitor tiene una capacitancia de 4.7 microfaradios y un voltaje nominal de 450 voltios.

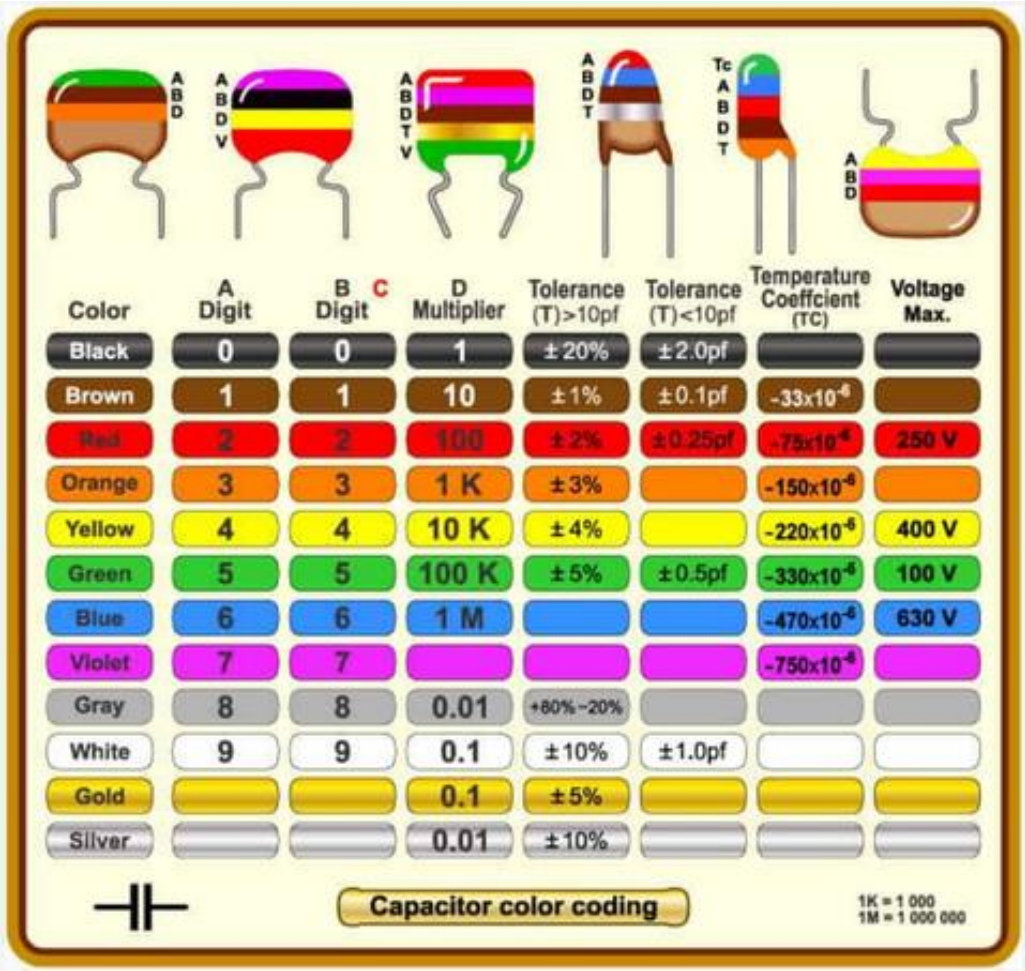
En el caso de un capacitor cerámico, el número «104» representa su valor de capacitancia en picofaradios (pF). Este número se interpreta de la siguiente manera:

- El primer y segundo dígito, en este caso, son «10». Esto indica que la capacitancia del capacitor es de 10 picofaradios.
- El tercer dígito, «4», es el multiplicador. Este número indica la cantidad de ceros que se agregan al valor. En este caso, el multiplicador «4» significa que se agregan cuatro ceros al valor, lo que equivale a multiplicar por 10,000.

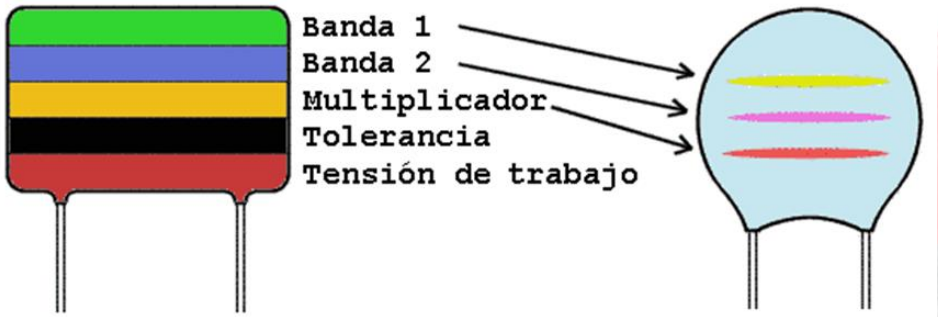


Por lo tanto, «104» en un capacitor cerámico significa que su valor de capacitancia es de 10 picofaradios (10 pF) multiplicado por 10,000, lo que da un total de 100,000 picofaradios, o lo que también se puede expresar como 0.1 microfaradios (0.1 µF).

CODIFICACIÓN DE COLOR DEL CONDENSADOR



Los condensadores tienen un código de colores, similar al de las resistencias, para calcular el valor de su capacidad, pero OJO en picofaradios (10-12 Faradios).



El primer color, nos dice el valor de la primera cifra de la capacidad el **segundo** el de la segunda y el **tercero** el del factor de multiplicación, que es 10 elevado al número del código del color.

El **cuarto** color nos indica la tolerancia, el porcentaje que puede variar del valor teórico (el sacado de los 3 primeros colores) de su capacidad. Por ejemplo 10%, 20%, etc.

Si un condensador tiene un valor de 1000pF y una tolerancia del 10%, quiere decir que el valor real puede oscilar entre un 10% más o un 10% menos.

Podría valer entre 900 y 1100 pF, aunque normalmente se ajustan bastante al valor teórico, en este caso 1000pF.

El **quinto** color nos indica la tensión de trabajo del condensador, es decir tensión a la que se carga.

El valor de los colores viene en una tabla, iguales a los de las resistencias, que puedes ver aquí: Código Colores Resistencia.

Sabiendo el valor de los colores, veamos un ejemplo:

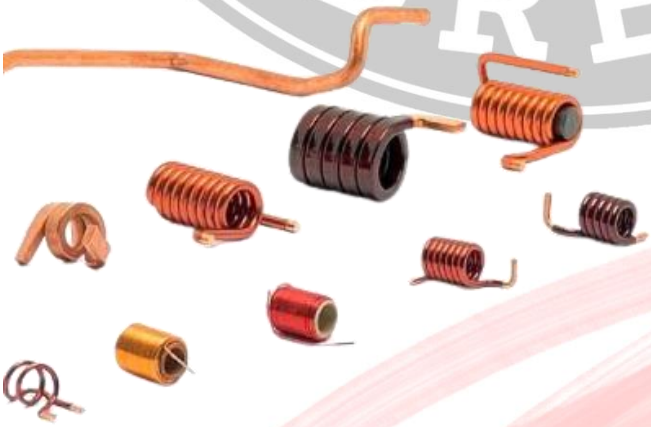
¿Qué valor tendría un condensador con los siguientes colores verde-azul-naranja?

Verde = 5; **Azul** = 6, **Naranja** = 3; por lo tanto, tendrá una capacidad = 56 x 103 picofaradios = 56000 pF = 56 nF.

Conclusión

En conclusión, los condensadores son elementos esenciales en el diseño de circuitos electrónicos. Desde su función básica de almacenar energía hasta la variedad de tipos disponibles, comprender estos componentes es vital para cualquier ingeniero o entusiasta de la electrónica. Al conocer el símbolo, el funcionamiento y las características clave, podrás seleccionar y utilizar condensadores de manera efectiva en tus proyectos.

2.2.3. INDUCTORES O BOBINAS:

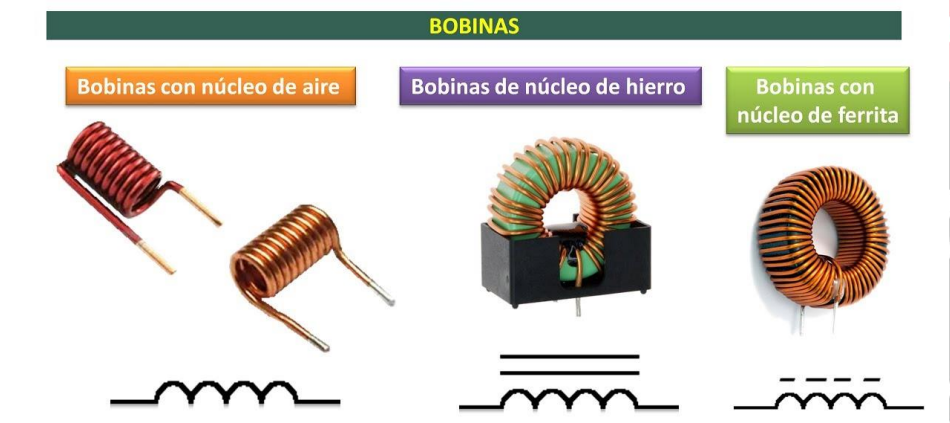


Un inductor o bobina es un componente pasivo de un circuito eléctrico que, debido al fenómeno de la auto inducción, almacena energía en forma de campo magnético. Un inductor está constituido usualmente por una cabeza hueca de una bobina de conductor, típicamente alambre o hilo de cobre esmaltado. Existen inductores con núcleo de aire o con núcleo de un material ferroso, para incrementar su capacidad de magnetismo.

Las Bobinas se caracterizan por retrasar el paso de la corriente que la atraviesa, su unidad de medida es el Henrio aunque se utilizan sus unidades como el microhenrio y milihenrio, se presentan en diversas formas desde un simple alambre espirado con núcleo o sin el, hasta haciendo parte de un transformador o en un encapsulado plástico o de cera.

Las Bobinas que vienen en encapsulado se identifican usualmente con el mismo código de colores de las resistencias, en otros casos llevan grabado el valor en números, en las Bobinas de alambre el valor viene determinado por el numero de espiras y el diámetro del alambre.

Algunas Bobinas utilizan un núcleo que puede ser de hierro o de ferrita o no contar con uno, las Bobinas son utilizadas ampliamente en fuentes de alimentación en donde en conjunto con condensadores y resistencias forman filtros para evitar ruidos eléctricos, también son muy usadas en circuitos de radio para formar osciladores de las distintas bandas de la radio.

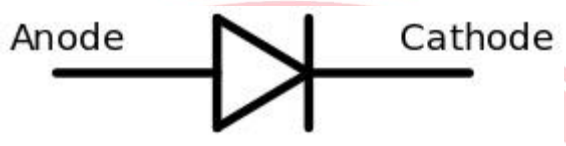


2.2.4. DIODOS:

Un diodo es un componente electrónico de dos terminales que permite la circulación de la corriente eléctrica a través de él en un solo sentido, bloqueando el paso si la corriente circula en sentido contrario, no solo sirve para la circulación de corriente eléctrica, sino que este la controla y resiste. Esto hace que el diodo tenga dos posibles posiciones: una a favor de la corriente (polarización directa) y otra en contra de la corriente (polarización inversa).

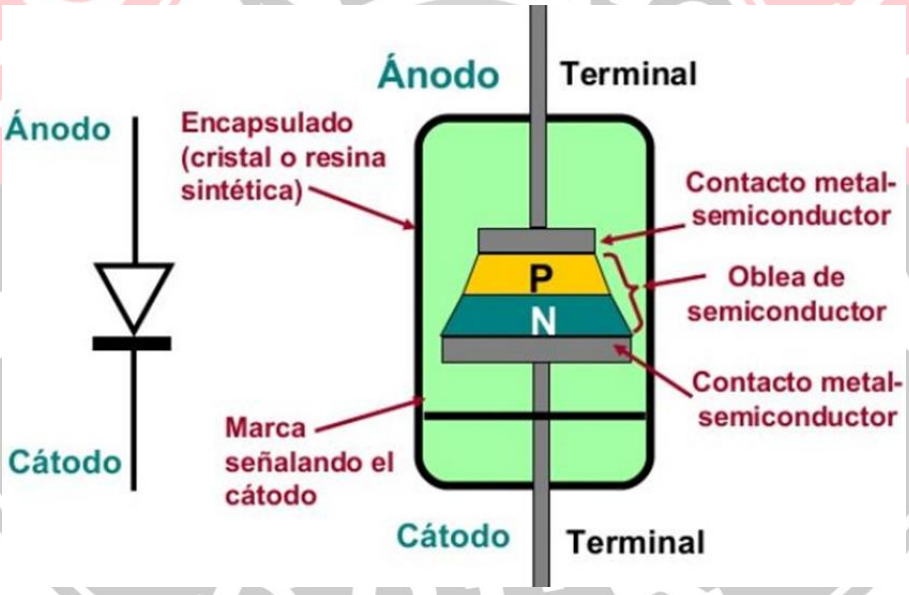
SÍMBOLO DEL DIODO

El símbolo eléctrico del diodo es un triángulo equilátero con una línea que pasa por uno de sus vértices en con la misma longitud y paralelo al lado opuesto. Su forma es similar a una flecha.



Como curiosidad la dirección en la que apunta el símbolo es la contraria en la que se desplaza la corriente.

La unión de estas dos regiones es la que define el comportamiento del diodo. Además, es en cada una de estas regiones es donde se conecta cada terminal del dispositivo.



Estructura del diodo.

Este término generalmente se usa para referirse al diodo semiconductor, el más común en la actualidad; consta de una pieza de cristal semiconductor conectada a dos terminales eléctricos. El diodo de vacío (que actualmente ya no se usa, excepto para tecnologías de alta potencia) es un tubo de vacío con dos electrodos: una lámina como ánodo, y un cátodo.

De forma simplificada, la curva característica de un diodo (I-V) consta de dos regiones: por debajo de cierta diferencia de potencial, se comporta como un circuito abierto (no conduce), y por encima de ella como un circuito cerrado con una resistencia eléctrica muy pequeña. Debido a este comportamiento, se les suele denominar rectificadores, ya

que son dispositivos capaces de suprimir la parte negativa de cualquier señal, como paso inicial para convertir una corriente alterna en corriente continua. Su principio de funcionamiento está basado en los experimentos de Lee De Forest.

Los primeros diodos eran válvulas o tubos de vacío, también llamados válvulas termoiónicas constituidos por dos electrodos rodeados de vacío en un tubo de cristal, con un aspecto similar al de las lámparas incandescentes. El invento fue desarrollado en 1904 por John Ambrose Fleming, empleado de la empresa Marconi, basándose en observaciones realizadas por Thomas Alva Edison.

Al igual que las lámparas incandescentes, los tubos de vacío tienen un filamento (el cátodo) a través del cual circula la corriente, calentándolo por efecto Joule. El filamento está tratado con óxido de bario, de modo que al calentarse emite electrones al vacío circundante los cuales son conducidos electrostáticamente hacia una placa, curvada por un muelle doble, cargada positivamente (el ánodo), produciéndose así la conducción. Evidentemente, si el cátodo no se calienta, no podrá ceder electrones. Por esa razón, los circuitos que utilizaban válvulas de vacío requerían un tiempo para que las válvulas se calentaran antes de poder funcionar y las válvulas se quemaban con mucha facilidad.

Lo más importante que debemos de entender en este tipo de componentes son las múltiples formas en que podemos polarizarlos, ya que, dependiendo de esto se compararán de una forma u otra, por ejemplo:

POLARIZACIÓN

En este tipo de componentes cuyo material en su estructura es un semiconductor de tipo **N** y tipo **P**, generan una barrera que impide el flujo de electrones entre ambos materiales.

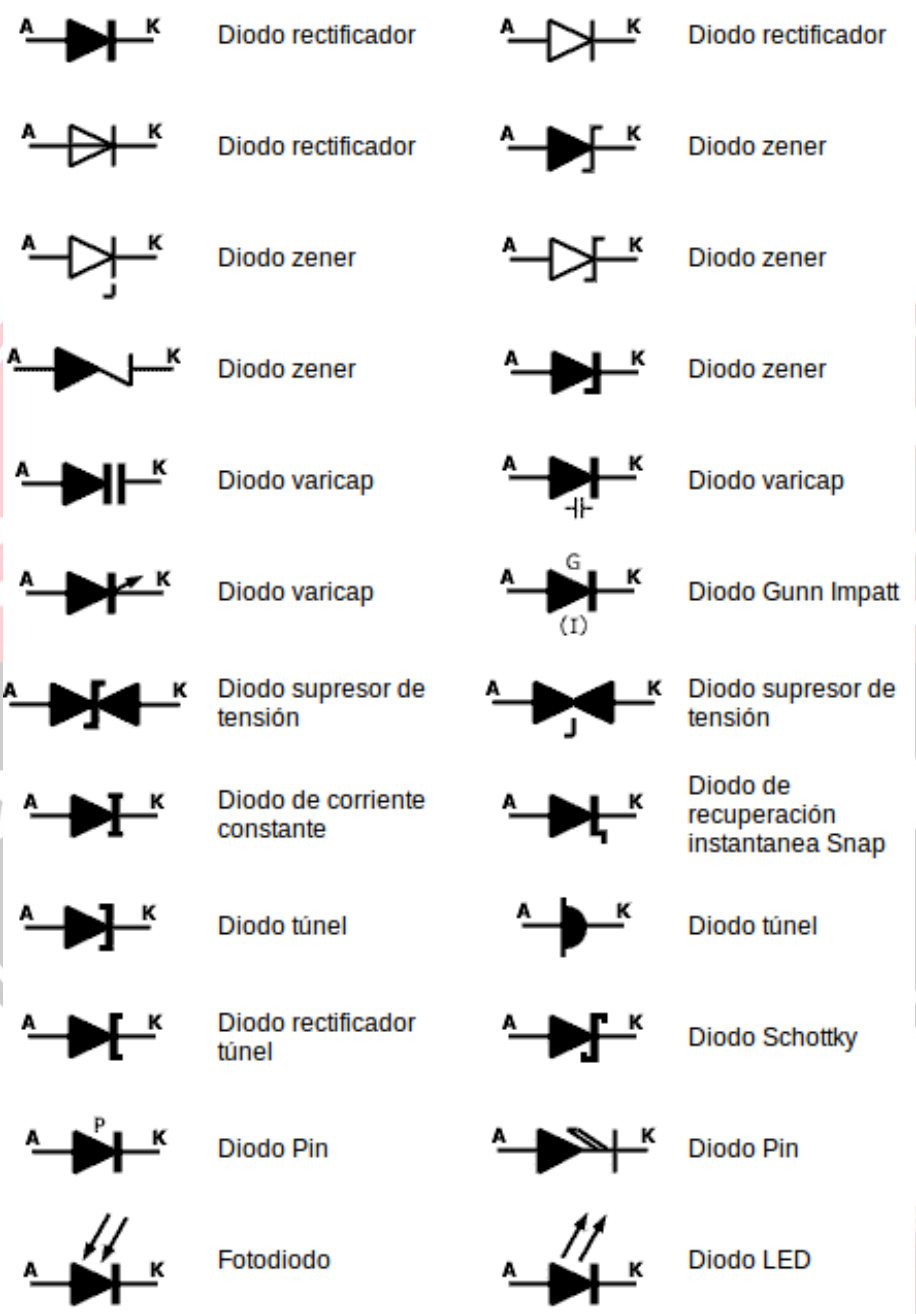
Dicha barrera se llama zona de empobrecimiento y es la razón por la que un diodo puede funcionar como un conductor o un aislante.

Para poder vencer esta barrera el diodo debe ser expuesto a una diferencia de potencial entre sus terminales, a esta acción se le conoce como polarización y puede manifestarse según los tres tipos siguientes:

- **Sin polarización**, indica que el diodo no tiene aplicado ningún **voltaje** entre sus terminales.
- **Polarización en directa**, indica que el diodo tiene un diferencial aplicado en sus terminales, y si, este voltaje es suficientemente grande, los portadores libres vencerán la barrera de empobrecimiento y el diodo entrará en conducción.
- **Polarización en inversa**, indica que el diodo tiene una diferencia de potencial aplicada entre sus terminales:
    - El positivo está conectado al material tipo **N**
    - Y el negativo conectado al tipo **P**

- Esto hace que la zona de empobrecimiento sea mayor e impide el flujo de corriente, lo que causa que el diodo se comporte como un circuito cerrado.

2.2.5. TIPOS DE DIODOS



Existen varios tipos de diodos, que pueden diferir en su aspecto físico, impurezas, uso de electrodos y algunos con características eléctricas específicas para alguna aplicación especial.

CLASIFICACIÓN Y TIPOS DE DIODOS

- **DIODOS TERMOIÓNICOS Y DE ESTADO GASEOSO**

Este tipo de diodos pueden considerarse como el principio de todo, no son precisamente semiconductores y son conocidos más popularmente como tubos de vació, pero dieron paso a la electrónica moderna que todos conocemos hoy en día.

Estos dispositivos consisten en un arreglo de electrodos que se encuentran dentro de un vidrio al vacío y que en un principio eran muy parecidos a un foco incandescente.

Hoy en día los materiales más usados por los fabricantes de diodos son el Silicio y el Germanio, de los cuales el Silicio es el preferido debido a sus bajos costos de refinación y el alto grado de pureza que se pueden alcanzar.

- **DIODO DETECTOR O DE BAJA SEÑAL**

Hemos hablado que la mayoría de los fabricantes utilizan el Silicio por su abundancia, y por qué, relativamente es más fácil de refinar, sin embargo, cuando hablamos de altas frecuencias el Germanio resulta ser el material más utilizado.

Y es precisamente de lo que está hecho el diodo detector, el cual es un tipo de diodo caracterizado por:

- Tener una unión PN pequeña
- Una excelente respuesta a altas frecuencias y con señales pequeñas

Esto debido a que su unión requiere de un menor voltaje para que el diodo entre en conducción. Su uso está presente en receptores de radio donde separan las señales de alta frecuencia o portadora de las señales de baja frecuencia o las señales audibles.

Diodo detector o de baja señal

- **DIODO RECTIFICADOR**

El diodo rectificador es uno de los más usados en la industria y su funcionamiento es muy interesante, son utilizados principalmente en las fuentes de voltaje de corriente directa para separar los semiciclos de las ondas sinusoidales y así poder obtener señales de un solo signo que son más fáciles de filtrar para eliminar el rizado y obtener un voltaje continuo.

Dentro de los diodos rectificadores podemos sub dividirlos en las siguientes clasificaciones:

RECTIFICADORES DE MEDIA ONDA

Es un circuito de un solo diodo al cual se le aplica un voltaje variable o corriente alterna, por ejemplo:

- Una señala senoidal en sus terminales y durante el primer semiciclo estará polarizado en directa permitiendo el paso de la señal.
- Y se mantendrá en inversa durante el segundo semiciclo impidiendo el flujo de corriente.

PUENTE DE DIODOS O RECTIFICADOR DE ONDA COMPLETA

Para lograr la rectificación de onda completa se emplean:

- Al menos 2 diodos
- Y en el caso del puente rectificador son 4 diodos

Ya que al tener conectados esta cantidad de diodos se logra que a la salida del circuito se tengan los dos semiciclos de la señal senoidal.

Esto resulta más eficiente ya que si pensamos en el área bajo la curva de la señal senoidal, con esta configuración se mantiene prácticamente intacta, claro desde el punto ideal.

RECORTADORES

Como su nombre lo indica, son una red de diodos que recortan una parte de la señal sin alterar el resto de la señal de entrada, el recortador más simple es el rectificador de media onda que vimos previamente, se construye usando un diodo y un resistor únicamente.

- **DIODOS DE POTENCIA**

El diodo de potencia está muy ligado a los diodos rectificadores incluso podría decirse que son aquellos que se utilizan en los puentes de diodos para fuentes de alimentación de alta potencia y altas temperaturas. La mayoría de los diodos de potencia se construyen de Silicio por su alto valor nominal de corriente, temperatura y voltaje pico en inversa (PIV).

La alta demanda de corriente requiere que la unión p-n se a mayor para disminuir la resistencia eléctrica cuando el diodo se polariza en directa, ya que, si la resistencia crece la perdida de potencia seria mayor aumentando la temperatura en los materiales.

Para aumentar la capacidad de corriente en los diodos los puedes conectar en paralelo y el valor nominal del PIV conectándolos en serie.

- **DIODO ZENER**

Es un tipo de diodo que cuenta con la característica especial de mantener un voltaje constante entre sus terminales, los diodos Zener tienen un dopaje especial que permite polarizarlo en inversa y mantenerlo en la región Zener de la curva característica del diodo.

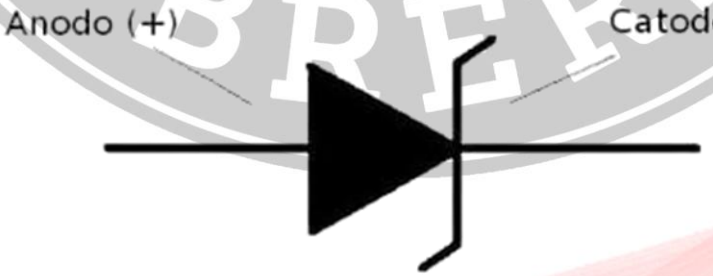
En dicha zona la corriente del diodo ID es igual a la corriente de saturación en inversa Iz provocando que el voltaje en las terminales del diodo no cambie mientras no supere la zona Zener, ya que al superar dicha zona el diodo puede entrar en la zona de ruptura y quemarse.

Si variamos el nivel de dopado en los materiales, también variaremos su ubicación en la zona Zener, por lo tanto, el potencial Zener se reduce si el nivel de dopado aumenta el nivel de impurezas en los materiales.

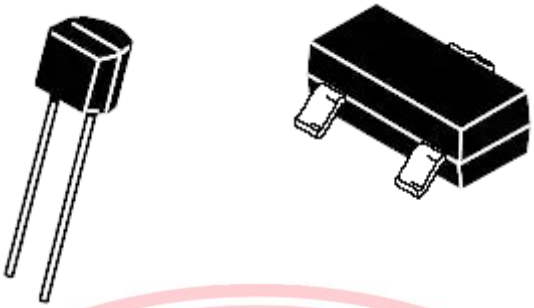
Esto permite la existencia de diodos Zener que soportan potenciales desde 1.8 Volts hasta aproximadamente 200 Volts, soportando potencias desde un cuarto de watts hasta unos cincuenta watts.

Si polarizamos en directa un diodo Zener, este se comportará idealmente igual a cualquier otro diodo.

Diodo Zener



- **DIODO VARACTOR (VARICAP)**



Los diodos varactores son conocidos también como varicap, VVC (capacitancia variable dependiente de voltaje) o de sintonización. Los diodos varactores son considerados capacitores semiconductores dependientes del voltaje.

Este tipo de diodo depende de la capacitancia que se manifiesta en la unión p-n cuando es polarizado en inversa. En condiciones de polarización en inversa existe una región de carga no recuperada en ambos lados de la unión de los materiales p-n que en conjunto forman la región de empobrecimiento.

Esta característica de capacitancia hace ideales a este tipo de diodo para aplicaciones como elementos de sintonía en receptores de radio, televisión, osciladores, multiplicadores, amplificadores, generadores de frecuencias FM e incluso existe una variante de estos diodos de nombre SNAP empleados en circuitos de UHF y microondas.

Diodo Varactor

- **DIODO EMISOR DE LUZ LED**

El diodo LED es un tipo de diodo que emite luz visible al energizarse, recordemos que en cualquier unión p-n polarizada en directa dentro de la estructura y principalmente cerca de la unión p-n hay una recombinación de huecos y electrones.

Esta recombinación, necesita que la energía adquirida por los electrones sea liberada y se transforme en otro estado, en todas las uniones n-p de los semiconductores una parte de esta energía se libera en forma de calor y otra en forma de fotones y depende del tipo de material semiconductor la energía se liberara en mayor o menor proporción.

En los diodos de Silicio y Germanio es mayor el porcentaje de energía liberado en forma de calor que en forma de fotones, por lo tanto, no vemos ningún destello durante su

operación o cuando lo polarizamos en directa, esto hace que no sean elementos adecuados para la fabricación de leds.

Existe una combinación de elementos que con los cuales se pueden generar luz visible y su voltaje en directa varia, por ejemplo:

- El azul se crea a partir de GaN con voltaje en directa de 5 volts.
- El verde se crea a partir de GaP con voltaje en directa de 2.2 volts
- El rojo se crea a partir de GaAsP con voltaje en directa de 1.8

Físicamente, los LEDs tienen una superficie metálica conductora externa conectada al material tipo p la cual es más pequeña para permitir la salida del máximo de fotones de energía luminosa cuando el LED es conectado en directa.

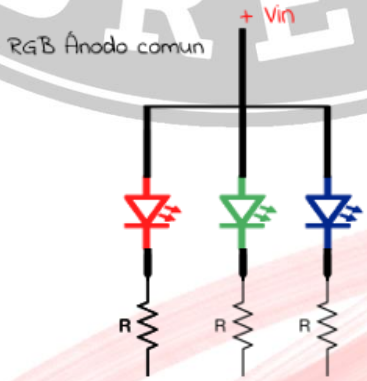
Diodo emisor de luz led

- **DIODO LED RGB**

Aun que es un tipo de LED, es importante que conozcas que existe un LED que emite luz en 3 diferentes tonalidades Rojo, Verde y Azul, de allí las siglas RGB.

Siempre he mencionado que este componente se comporta como si tuvieras 3 LED conectados con un ánodo o catado común, según sea el caso.

Además, es muy interesante y sumamente colorido hacer proyectos escolares con este tipo de LED, ya que a través de un tren de impulsos, puedes generar hasta 16 millones de tonalidades entre muchas otras cosas, por ejemplo, las tiras de LED RGB son de las más vendidas, porque son sumamente vistosas.



LED RGB conectado en ánodo común

- **LED INFRARROJO**

Los diodos emisores de luz infrarroja están construidos principalmente por Arseniuro de Galio en estado sólido que emiten un flujo radiante cuando se conecta en directa.

Cuando la región de la unión se polariza en directa, los electrones de a región n se recombinan con los huecos excedentes de la región p en una región de recombinación situada entre los materiales p y n, esta recombinación provoca que el diodo emita una radiación de energía en forma de fotones, los cuales se reabsorben en la estructura o abandonan el dispositivo en forma de energía radiante.

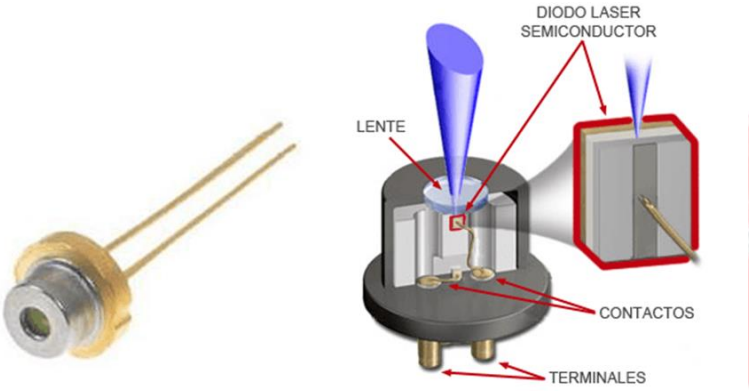
Emisor de un led infrarrojo

- **DIODO EMISOR DE LUZ LÁSER**

Este tipo de diodo como otros emisores de luz irradian energía tras la recombinación de los electrones con los huecos de los materiales extrínsecos p y n de su estructura.

Estos LEDs irradian una poderosa luz invisible para el ojo humano, pero, que está fuertemente concentrada, también son conocidos como láseres de inyección o ILD's y son usados en muchas aplicaciones como:

- En los lectores de CD, DVD, Blueh-ray, HD-DVD
- Interconexiones ópticas en los circuitos integrados,
- Y en impresoras láser, etc.



- **DIODO ESTABILIZADOR**

Más que un diodo se trata de un conjunto de diodos conectados en serie y polarizado en directa, con el propósito de estabilizar el voltaje a tensiones bajas tal y como lo haría un diodo Zener.

- **DIODO TÚNEL ESAKI**

En 1958 Leo Esaki presentó el diodo túnel, y es por ello que lo conocemos como diodo Esaki y tiene una característica que lo diferencia de prácticamente todos los otros diodos.

Un diodo túnel posee una región de resistencia interna negativa, en esta región un incremento del voltaje terminal reduce la corriente del diodo.

El diodo túnel se fabrica dopando los materiales semiconductores que forman la unión p-n a un nivel de 100 o varios miles de veces más al de un diodo semiconductor típico.

La región de empobrecimiento en un diodo túnel es muy pequeña y hace que los portadores la penetren a velocidades que exceden por mucho a los diodos convencionales, por lo que los hacen ideales en aplicaciones de alta velocidad, por ejemplo:

- Computadoras donde se necesitan conmutaciones de nanosegundos o picosegundos.

- **DIODO PIN**

Los diodos PIN son aquellos semiconductores que tienen una estructura de 3 capas, las capas externas son de material tipo p y n, mientras la capa intermedia es un material intrínseco, de allí recibe el nombre de PIN, donde:

- **P -** por el material tipo p
- **I -** por el material intrínseco
- **N -** por el material tipo N

Sin embargo, en la práctica comúnmente la capa intrínseca se cambia por un material tipo P de alta resistividad o por una capa tipo n igualmente de alta resistividad.

Los diodos tipo PIN principalmente son utilizados como conmutadores de alta frecuencia o como resistencias variables por voltaje, ya que, la velocidad en la que tardan los portadores libres en atravesar la unión, es sumamente elevada.

Diodo PIN

- **DIODO BACKWARD**

Este diodo es una variación del diodo Zener y el diodo túnel, este diodo también es llamado back diode o diodo hacia atrás, está construido de Germanio y se caracteriza por mantener una mejor conducción al ser polarizado en inversa que al ser conectado en directa.

Diodo BACKWARD

- **DIODO DE BARRERA SCHOTTKY**

El diodo Schottky también es conocido como barrera superficial o portadores calientes y es un dispositivo con una rápida respuesta a altas frecuencias y de bajo ruido.

Inclusive, lo podemos encontrar en fuentes de alimentación de alto voltaje y baja corriente, también lo podemos encontrar en la lógica TTL Schottky para computadoras.

Su construcción es bastante diferente a la convencional p-n y se trata de la unión de un metal semiconductor, donde;

- El material semiconductor normalmente es Silicio tipo n y en algunas ocasiones tipo p
- Mientras que el metal puede ser:
  - Molibdeno
  - Platino
  - Cromo
  - O tungsteno.

Esta estructura causa que en ambos materiales el electrón sea el portador mayoritario y los huecos sean insignificantes.

Cuando los materiales se unen los electrones del material tipo n fluyen de inmediato al material metálico estableciendo un flujo de portadores mayoritarios y como tienen un nivel de energía cinética mayor a los electrones que ya se encuentran en el metal, se llaman portadores calientes.

Diodo de barrera SCHOTTKY

- **DIODO SHOCKLEY**

Este tipo de componentes se caracteriza por tener dos estados estables, a diferencia de lo que hemos visto, por ejemplo:

- Un estado estable se encuentra en el bloque o alta impedancia
- El otro esta durante la conducción o baja impedancia

Quizá encuentres literatura donde se confunde con el diodo anteriormente descrito Schottky, no obstante, este componente posee:

- Cuatro capas de tipo N y P
- Las cuales están formadas alternadamente

Diodo Shockley

- **FOTODIODOS**

Los fotodiodos se construyen a partir de la unión de elementos semiconductores p-n y su región de operación se limita a la polarización en inversa.

Los fotodiodos vienen con un tipo de ventana transparente que permite el paso de la luz a la unión p-n, permitiendo que la energía de las ondas luminosas o fotones lleguen a la estructura atómica de los elementos.

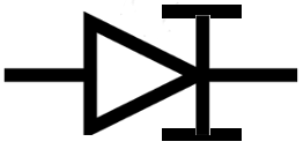
Lo anterior da como resultado un incremento de portadores minoritarios y corriente inversa, por lo tanto, si la luz aumenta la corriente en inversa también crecerá, se utilizan mucho en sistemas de iluminación, sistemas de seguridad, contadores de objetos, etc.

Fotodiodos

- **DIODO DE CORRIENTE CONSTANTE**

Este tipo de diodo es conocido también por muchos como diodo de regulación, a pesar de ser un JFET, entra en esta categoría debido a sus características similares a la mayoría de componentes descritos anteriormente.

Este componente permite el flujo de corriente a través de su estructura hasta alcanzar un nivel adecuado, para posterior estabilizarse en un nivel especifico.



Diodo de corriente constante

- **DIODO DE RECUPERACIÓN DE PASO (SRD)**

Este componente es conocido como:

- Diodo de separación rápida
- Diodo de almacenamiento de carga
- Diodo con memoria
- también puedes encontrarlo como chasquido

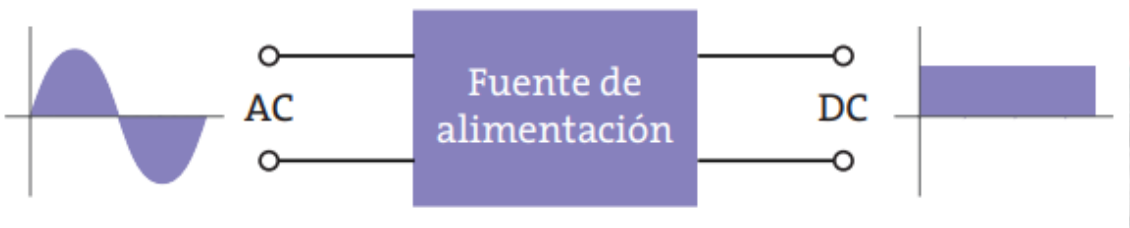
Es muy curioso, ya que puede generar pulsos muy cortos y almacenar carga eléctrica durante la conducción, es sumamente utilizado en electrónica de microondas como generador de pulsos y como amplificador paramétrico.

Diodo de recuperación SDR

APLICACIONES Y USOS DE LOS DIODOS, CIRCUITOS RECTIFICADORES

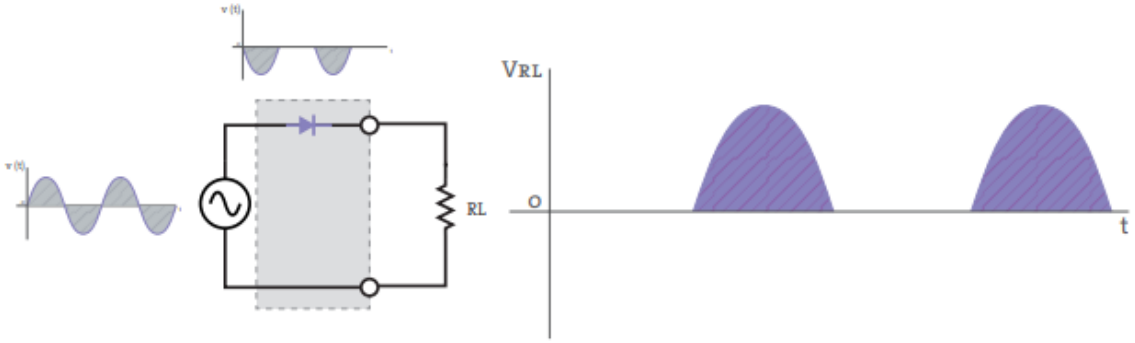
Como hemos visto, en función del tipo de diodo las aplicaciones son muy variadas, utilizándose en iluminación, demoduladores de radio, protectores de sobretensión o puertas lógicas (dispositivo electrónico esenciales en la construcción de microchips), pero una de las más comunes es en las fuentes de alimentación donde actúan como rectificadores de onda.

La mayoría de los circuitos electrónicos contienen un circuito que es una fuente de alimentación. Como el suministro de la energía eléctrica es en corriente alterna, esta se debe convertir en corriente continua. Para esta función son empleados los rectificadores. Veremos aquí un par de circuitos con diodos para rectificar una onda senoidal.



Rectificador de media onda

El rectificador más simple se realiza mediante la utilización de un diodo conectado en serie una carga que recibirá la tensión continúa. La carga la llamaremos RL. Este rectificador obtiene su nombre debido a que a través de él se obtiene la mitad positiva de la tensión alterna de entrada.

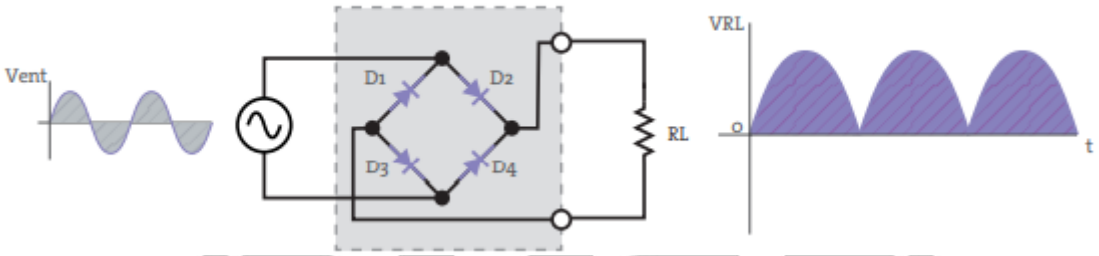


Como vemos en el circuito, sobre la resistencia obtenemos una señal de media onda. El diodo funciona como llave; cerrándose para el semiciclo positivo y abierta para el semiciclo negativo.

Rectificador de onda completa

En este caso usaremos un puente de diodos. Este tipo de rectificador invierte la

mitad negativa de la tensión de entrada. De esta manera tendremos ambos semiciclos en la zona positiva en la resistencia de carga.



2.2.6. TRANSISTORES:

Se llama transistor (del inglés: *transfer resistor*, "resistor de transferencia") a **un tipo de dispositivo electrónico semiconductor**, capaz de modificar una señal eléctrica de salida como respuesta a una de entrada, sirviendo como amplificador, conmutador, oscilador o rectificador de la misma.

Es un tipo de dispositivo **de uso común en numerosos aparatos**, como relojes, lámparas, tomógrafos, celulares, radios, televisores y, sobre todo, como componente de los circuitos integrados (chips o microchips).

Los transistores tienen su origen en la necesidad de controlar el flujo de la corriente eléctrica en diversas aplicaciones, como parte de la evolución del campo de la electrónica. Su antecesor directo fue un aparato inventado por Julius Edgar Lilienfeld en Canadá en 1925, pero no sería hasta mediados de siglo cuando podría implementarse usando materiales semiconductores (en lugar de tubos al vacío).

Los primeros logros en este sentido consistieron en la ampliación de la potencia de una señal eléctrica a partir de conducirla a través de dos puntales de oro aplicados a un cristal de germanio.

El nombre de transistor fue propuesto por el ingeniero estadounidense John R. Pierce, a partir de los primeros modelos diseñados por los Laboratorios Bell. **El primer transistor de contacto apareció en Alemania en 1948**, mientras que el primero de alta frecuencia fue inventado en 1953 en los Estados Unidos.

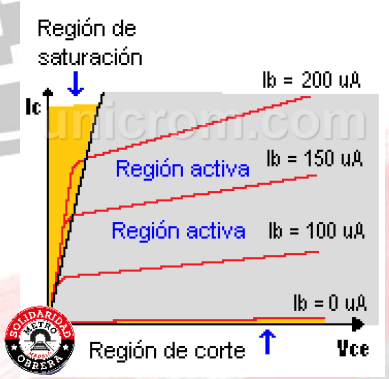
Estos fueron los primeros pasos hacia la explosión electrónica de la segunda mitad del siglo XX, que permitieron, entre muchas otras cosas, el desarrollo de las computadoras.

En la construcción de los transistores hoy en día se emplean materiales como germanio (Ge), silicio (Si), arseniuro de galio (GaAs) o aleaciones de silicio y germanio o silicio y aluminio. Dependiendo del material usado, el dispositivo podrá resistir una cantidad determinada de tensión eléctrica y una temperatura máxima de calentamiento por resistencia.

2.2.6.1. ¿CÓMO FUNCIONA UN TRANSISTOR?

Los transistores **operan sobre un flujo de corriente**, operando como amplificadores (recibiendo una señal débil y generando una fuerte) o como interruptores (recibiendo una señal y cortándole el paso) de la misma. Esto ocurre dependiendo de cuál de las tres posiciones ocupe un transistor en un determinado momento, y que son:

- **En activa.** Se permite el paso de un nivel de corriente variable (más o menos corriente).
- **En corte.** No deja pasar la corriente eléctrica.
- **En saturación.** Deja pasar todo el caudal de corriente eléctrica (corriente máxima).



la

En este sentido, **el transistor funciona como una llave de paso** de una tubería: si está totalmente abierto deja entrar todo el caudal del agua, si está cerrado no deja pasar nada, y en sus posiciones intermedias deja pasar más o menos agua.

Ahora bien: todo transistor se compone de tres elementos: base, colector y emisor. La primera es la que media entre el emisor (por donde entra el caudal de corriente) y el colector (por donde sale el caudal de corriente). Y lo hace, a su vez, activada por una corriente eléctrica menor, distinta de la que modulada por el transistor.

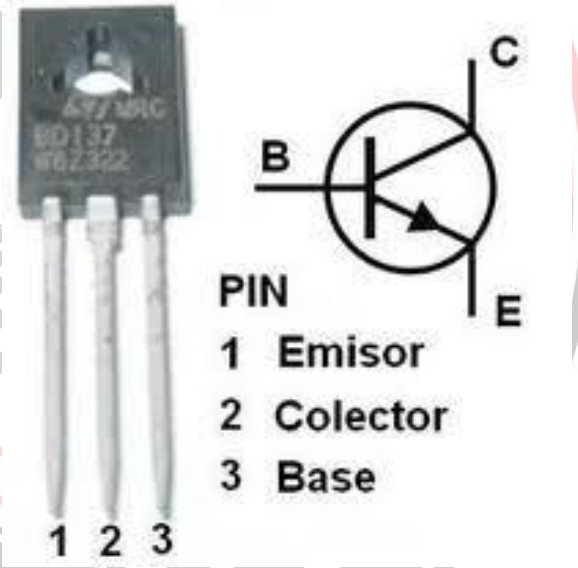
De esta manera, si la base no recibe corriente, el transistor se ubica en posición de corte; si recibe una corriente intermedia, la base abrirá el flujo en determinada cantidad; y si la base recibe la suficiente corriente, entonces se abrirá del todo el dique y pasará el total de la corriente modulada.

Se entiende así que el transistor **opera como un modo de controlar la cantidad de electricidad** que pasa en determinado momento, permitiendo así la construcción de relaciones lógicas de interconexión.

2.2.6.2. COMPONENTES DE LOS TRANSISTORES

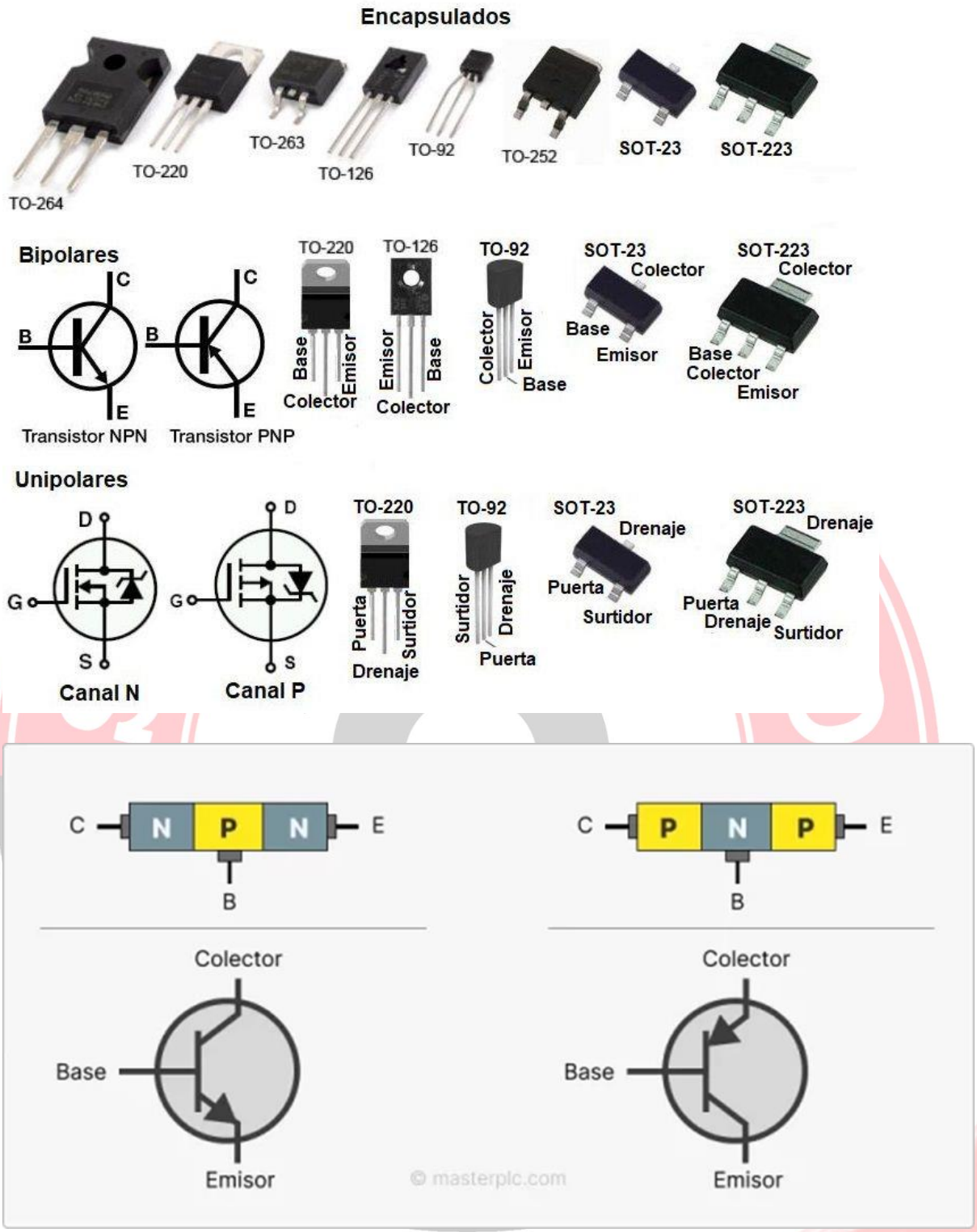
Los transistores se componen esencialmente de tres patillas o cables, cada uno encargado de una labor diferente y que se denominan:

- **Emisor**. Desde donde entra el flujo eléctrico al interior encapsulado del transistor.
- **Base**. La que modula el flujo entre emisor y colector.
- **Colector**. Hacia donde fluye la corriente una vez que ha sido modulada por la base.

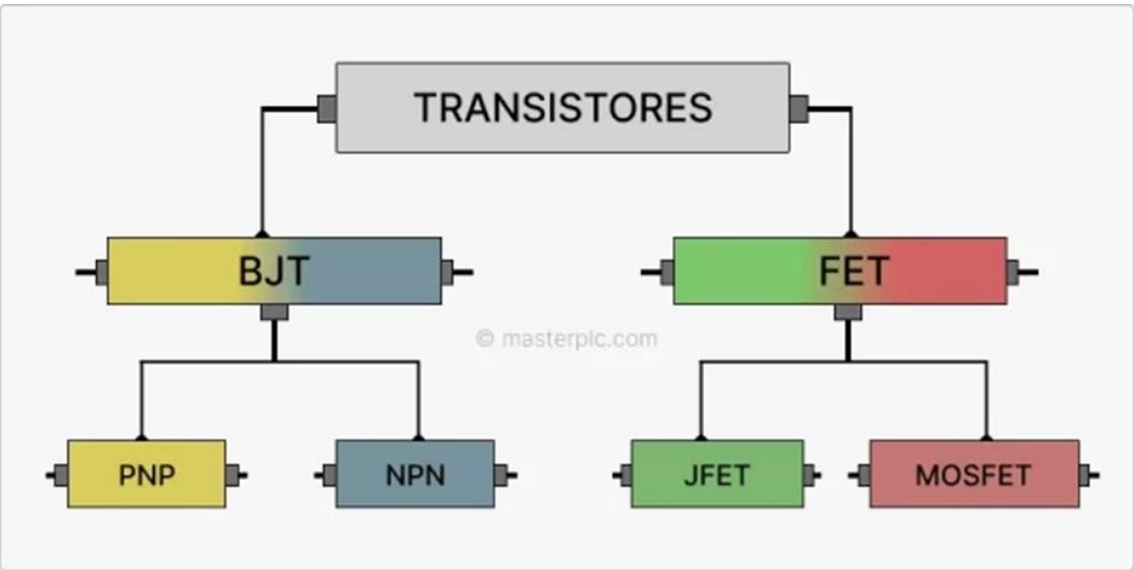


2.2.6.3. TIPOS DE TRANSISTORES

En electrónica, los **transistores** son componentes semiconductores fundamentales que amplifican o conmutan señales eléctricas. Se pueden clasificar de varias maneras según su estructura, funcionamiento y aplicación. Aquí te dejo los tipos principales:



Tipos de Transistores



Clasificación de los transistores

1. Según su estructura y material semiconductor

- **Transistores Bipolares de Unión (BJT - Bipolar Junction Transistor)**

Los transistores de unión generalmente se denominan transistores de unión bipolar (BJT). El término 'Bipolar' significa que tanto los electrones como los huecos son necesarios para conducir la corriente y el término 'Unión' significa que contiene una Unión PN (dos uniones, de hecho).

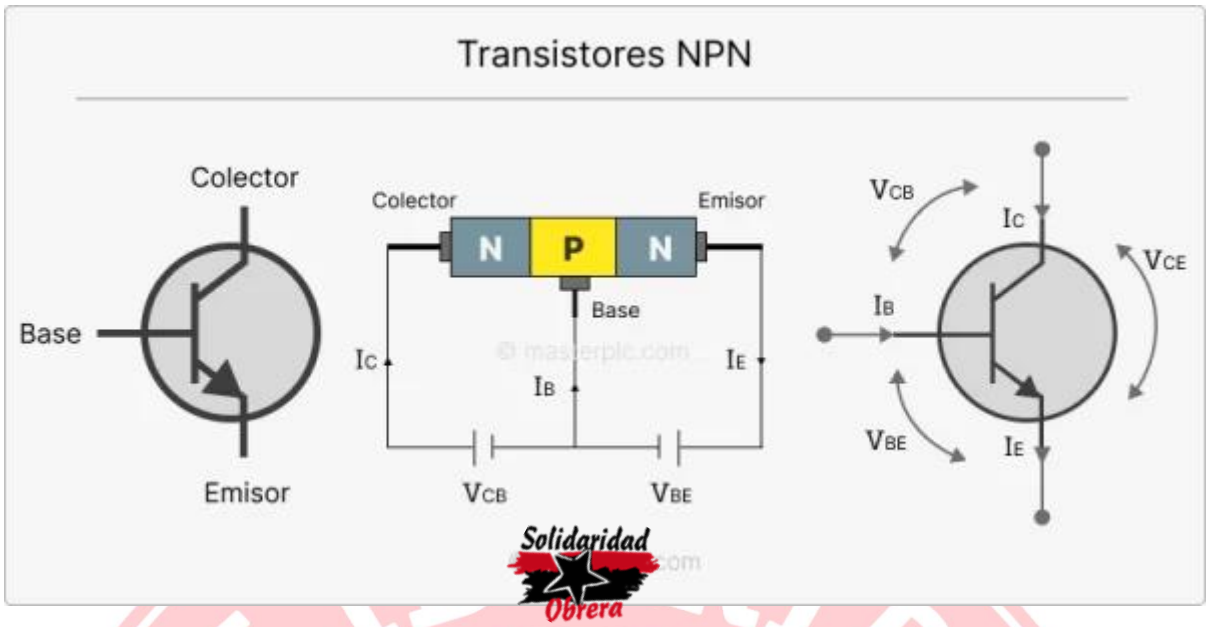
Los BJT tienen tres terminales denominados Emisor (E), Base (B) y Colector (C). Los transistores BJT se clasifican en transistores NPN y PNP según la construcción.

- Tipos: **NPN y PNP**
- Funcionamiento: Controlan la corriente entre el colector y el emisor mediante una corriente de base.
- Aplicaciones: Amplificadores, osciladores, conmutadores.

1. Transistor NPN

El transistor NPN consta de dos materiales semiconductores de tipo N y están separados por una capa delgada de semiconductor de tipo P.

Los símbolos y la estructura de los transistores NPN.

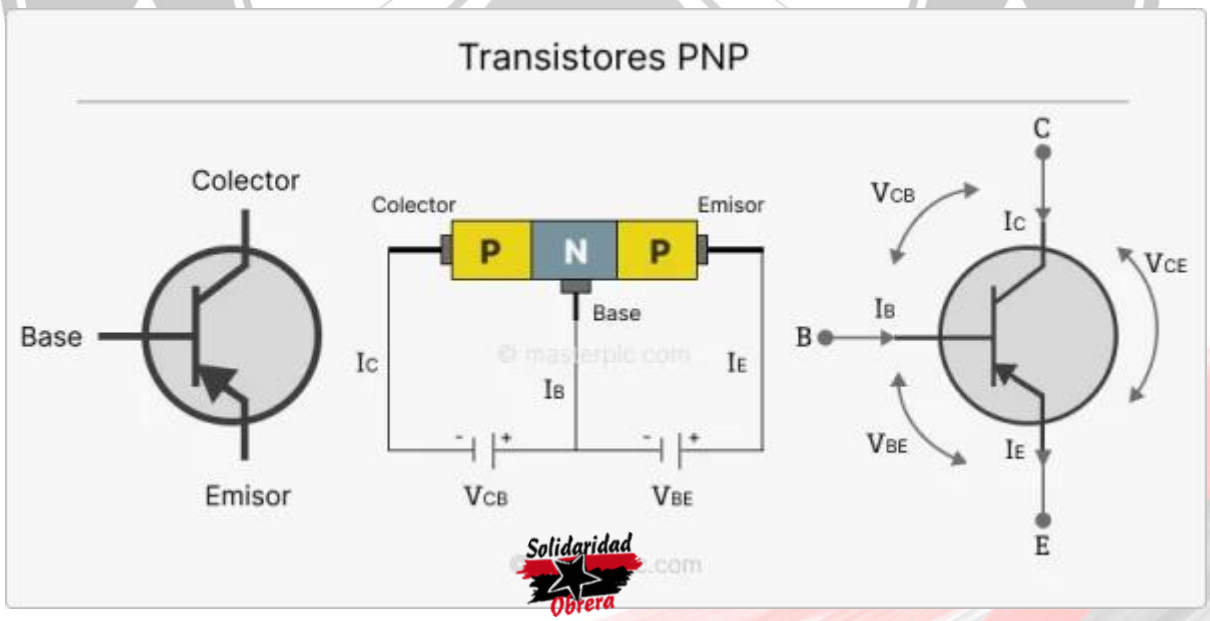


Transistores NPN

2. Transistor PNP

Los PNP es otro tipo de transistores de unión bipolar (BJT). Los transistores PNP contienen dos materiales semiconductores de tipo P y están separados por una capa delgada de semiconductor de tipo N.

El transistor PNP está ENCENDIDO cuando la terminal de la base se baja con respecto al emisor. El símbolo y la estructura del transistor PNP se muestran a continuación.

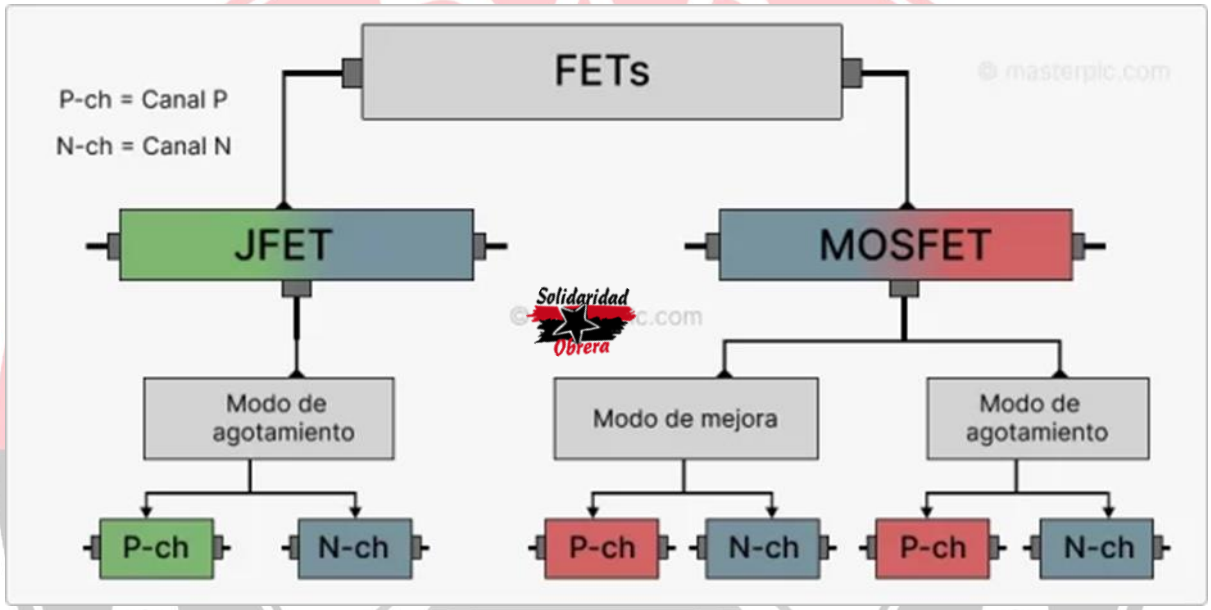


Transistores PNP

- **Transistores de Efecto de Campo (FET - Field Effect Transistor)**

El transistor de efecto de campo (FET) es otro tipo importante de transistor. Básicamente, el FET también tiene tres terminales (como BJT). Los tres terminales son: Puerta (G), Drenaje (D) y Fuente (S).

Los transistores de efecto de campo se clasifican en transistores de efecto de campo de unión (JFET) y transistores de efecto de campo de puerta aislada (IG-FET) o transistores de efecto de campo de semiconductores de óxido metálico (MOSFET).

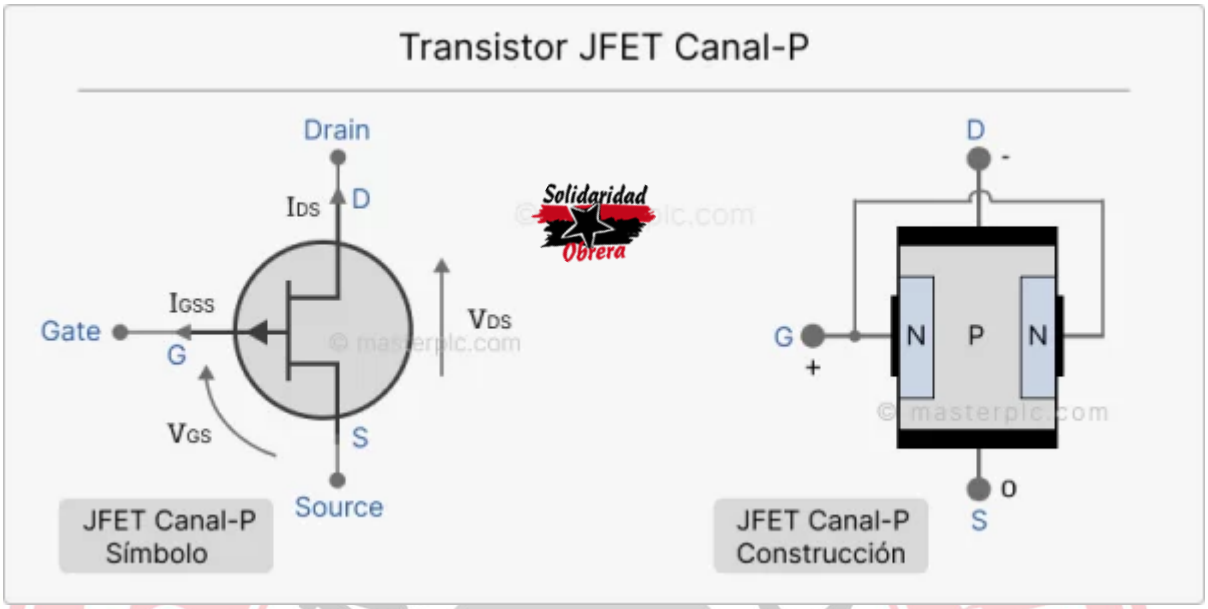


Tipos de transistores FET

- Tipos:
  - **Junction FET (JFET)** (Canal N y Canal P)
  - **Metal-Oxide-Semiconductor FET (MOSFET)** (Canal N y Canal P)
- Funcionamiento: Controlan la corriente mediante un voltaje aplicado a la compuerta.
- Aplicaciones: Electrónica digital, fuentes de alimentación, amplificadores de potencia.

1. JFET de canal P

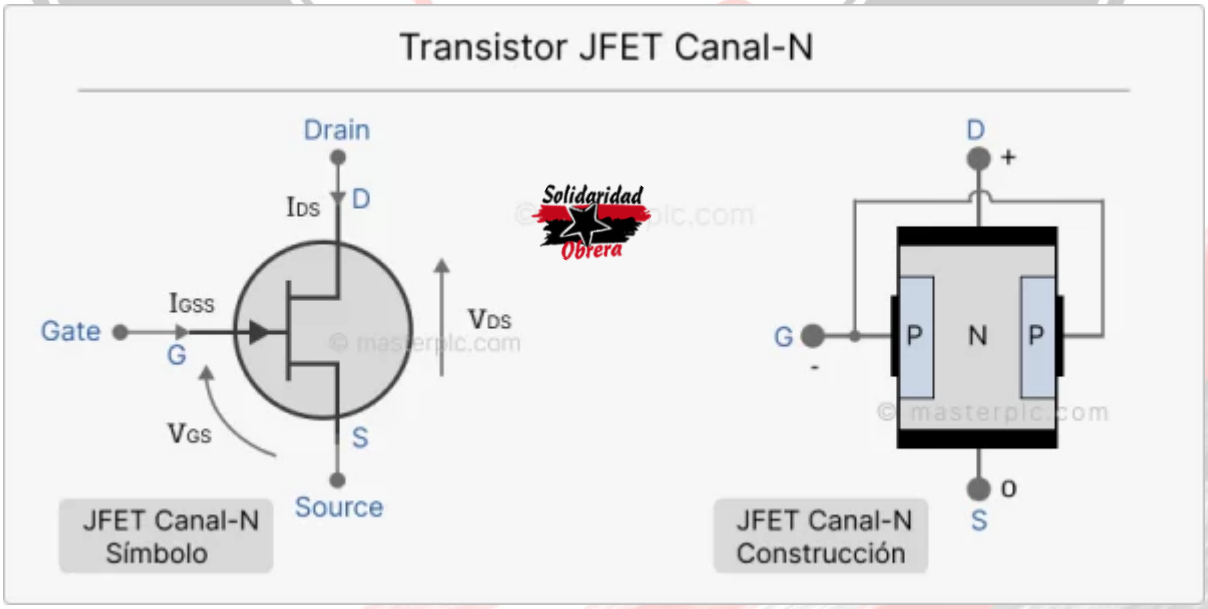
En este tipo de JFET, el flujo de corriente se debe a los agujeros. El canal entre la fuente y el drenaje se llama P-Channel. Los símbolos para los JFET de canal P se dan a continuación.



Transistor JFET Canal-P

2. JFET de canal N

En JFET de canal N, el flujo de corriente se debe a los electrones. Cuando se aplica voltaje entre la puerta y la fuente, se forma un canal entre la fuente y el drenaje para el flujo de corriente. Este canal se llama N–Channel.



Transistor JFET Canal-N

- **Transistores de Alta Movilidad de Electrones (HEMT - High Electron Mobility Transistor)**
    - Basados en materiales como **GaAs o GaN**.
    - Aplicaciones: Radiofrecuencia (RF), telecomunicaciones, sistemas de radar.

2. Según su aplicación específica

- **Transistores de conmutación rápida**
    - Diseñados para operar a alta velocidad en circuitos digitales.
- **Transistores de Potencia**
    - Manejan altas corrientes y voltajes.
    - Tipos:
        - **MOSFET de Potencia**
        - **BJT de Potencia**
        - **IGBT (Insulated Gate Bipolar Transistor)** → Combinación de BJT y MOSFET, usado en motores eléctricos e inversores.
- **Transistores Darlington**
    - Dos BJTs en un solo encapsulado para mayor ganancia de corriente.
- **Transistores Fototransistores**
    - Sensibles a la luz, usados en sensores y sistemas ópticos.

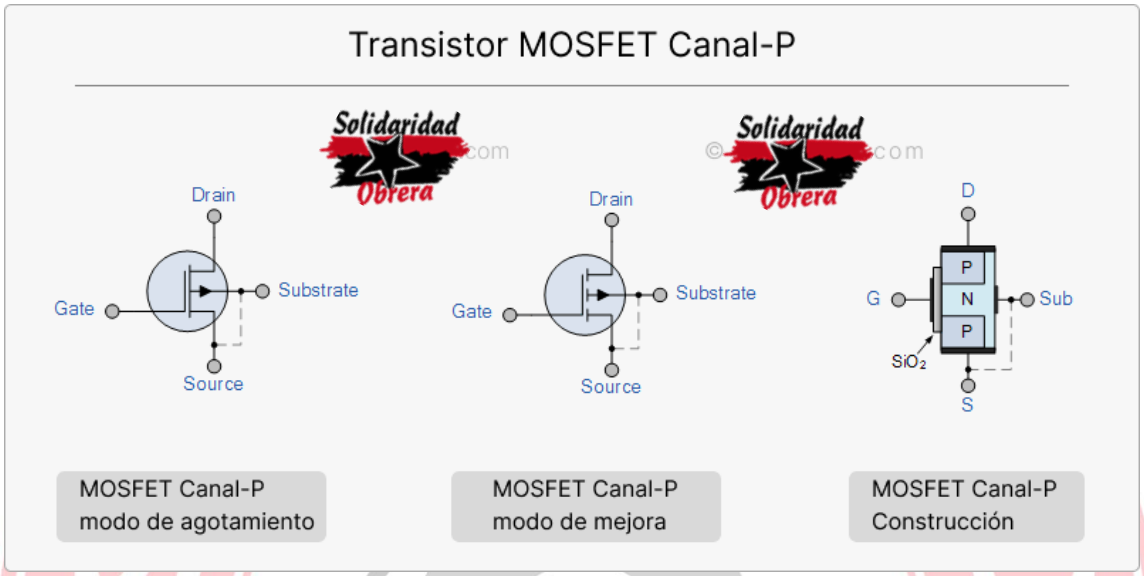
1. MOSFET

El transistor de efecto de campo semiconductor de óxido de metal (MOSFET) es el más utilizado y el tipo más popular entre todos los transistores. El nombre «Óxido de metal» indica que la región de la puerta y el canal están separados por una fina capa de óxido de metal (normalmente, SiO2).

Los MOSFET se clasifican en modo de agotamiento y modo de mejora. Nuevamente, los transistores de modo de agotamiento y mejora se clasifican además en canales N y canales P respectivos.

1.1. MOSFET de canal P

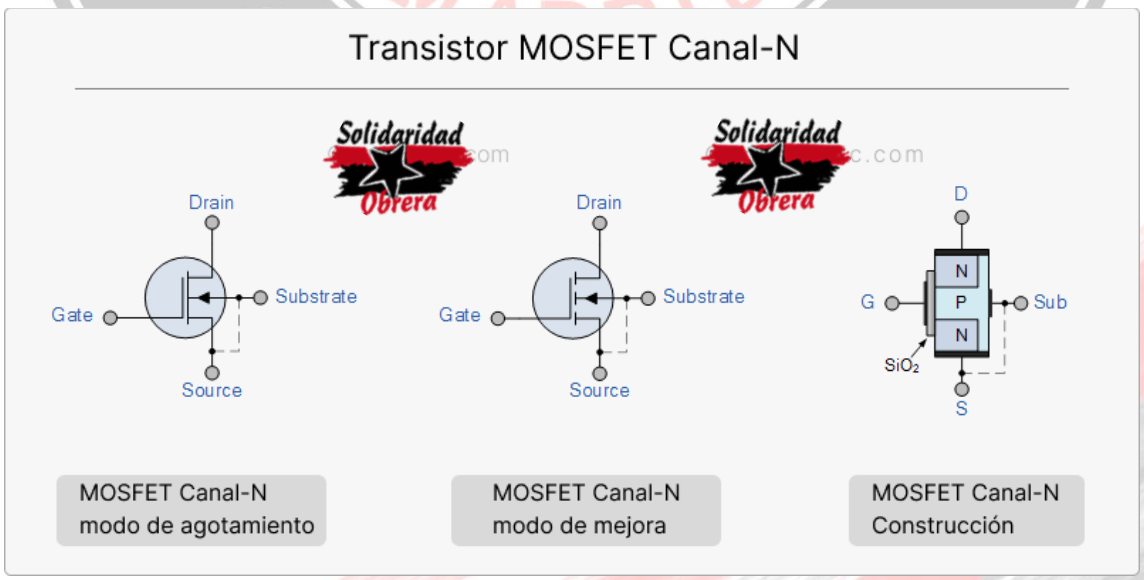
El MOSFET que tiene una región de canal P entre la fuente y el drenaje se denomina MOSFET de canal P. Aquí, los terminales de fuente y drenaje están fuertemente dopados con material tipo P y el sustrato está dopado con material tipo N. El flujo de corriente entre la fuente y el drenaje se debe a la concentración de agujeros. El voltaje aplicado en la puerta controlará el flujo de corriente a través de la región del canal.



MOSFET Canal-P

1.2. MOSFET de canal N

El MOSFET que tiene una región de canal N entre la fuente y el drenaje se denomina MOSFET de canal N. Aquí, los terminales de la fuente y la puerta están fuertemente dopados con materiales de tipo N situados en un material semiconductor (sustrato) de tipo P fuertemente dopado.



MOSFET Canal-N

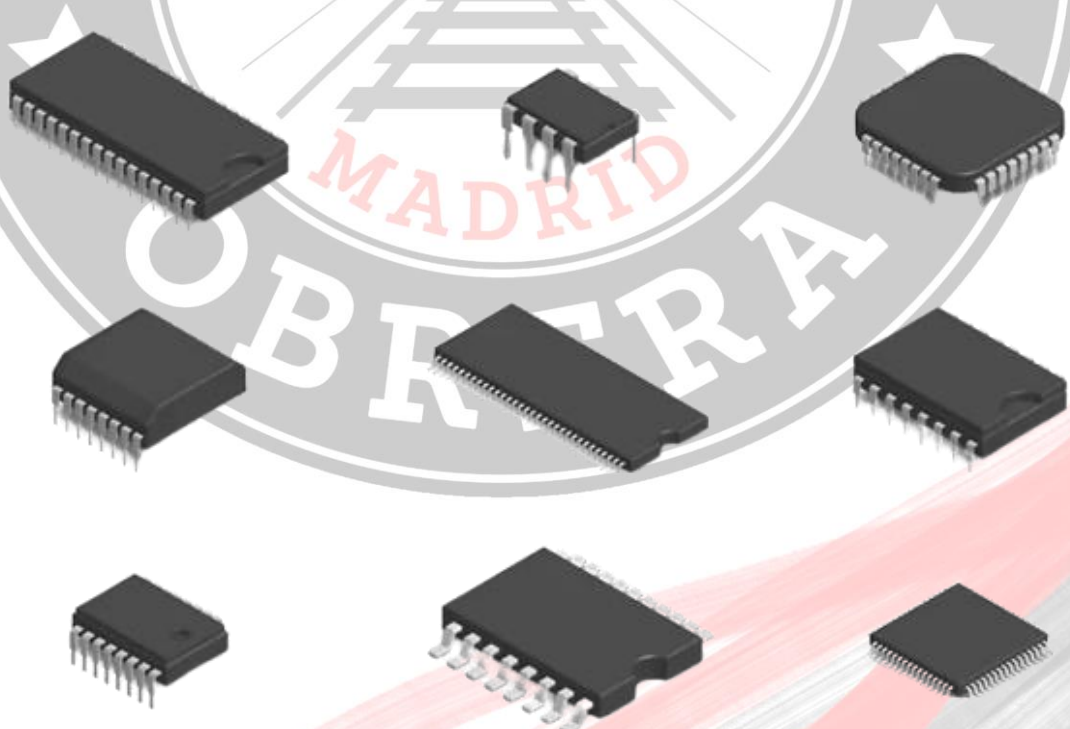
3. Según la tecnología de fabricación

- **Transistores de Silicio (Si)**
  - Los más comunes en electrónica general.
- **Transistores de Germanio (Ge)**
  - Antiguos, pero con menor caída de voltaje base-emisor.
- **Transistores de Arseniuro de Galio (GaAs)**
  - Más rápidos y eficientes en radiofrecuencia.

2.2.7. CIRCUITOS INTEGRADOS:

Los circuitos integrados, a menudo llamados IC, son chips diminutos hechos de materiales como el silicio. Están repletos de componentes electrónicos como **transistores**, **resistencias**, y **condensadores.** Estos componentes realizan tareas específicas, como amplificar señales o controlar el flujo de datos.

Los circuitos integrados son esenciales para la mayoría de los dispositivos electrónicos modernos. Solo los teléfonos inteligentes, las computadoras o los dispositivos domésticos inteligentes los tienen. Permiten colocar una gran cantidad de tecnología en espacios pequeños, lo que hace que los dispositivos sean más compactos, potentes y asequibles.



2.2.7.1. ¿QUÉ ES UN CIRCUITO INTEGRADO?

DEFINICIÓN TÉCNICA

Un circuito integrado (CI) es un pequeño chip fabricado con material semiconductor, generalmente silicio. Contiene muchos **componentes electrónicos**, como transistores, resistencias, condensadores y diodos, todos ellos agrupados. Estos componentes realizan diversas tareas, como procesar datos o amplificar señales.

COMPONENTES BÁSICOS

Un circuito integrado es como una pequeña ciudad de componentes electrónicos. Cada componente tiene una función:

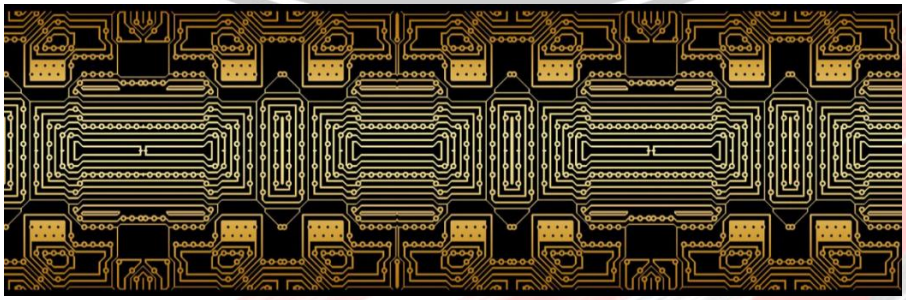
- **Transistores**: Actúan como interruptores que pueden encender o apagar señales.
- **Resistencias**: Controlar el flujo de corriente eléctrica.
- **Condensadores**: Almacenar y liberar energía eléctrica.
- **diodos**: Permitir que la corriente fluya en una sola dirección.

Estas piezas están conectadas a través de vías metálicas aceptables para formar un circuito completo. Juntas, realizan tareas específicas, como controlar el flujo de información o generar señales.

2.2.7.2. FABRICACIÓN DE CIRCUITOS INTEGRADOS

La creación de un circuito integrado es compleja y precisa. Comienza con una fina lámina de silicio conocida como *oblea*. Usando **fotolitografía**, los diseñadores crean patrones en la superficie de la oblea. Este patrón indica dónde se colocará cada pequeño componente. Se utilizan productos químicos y luz para grabar estos patrones en la oblea.

Una vez que los componentes están en su lugar, se añaden capas finas de metal para unirlos, creando las vías por las que viajan las señales eléctricas. Todo el proceso se realiza en salas blancas para evitar que las partículas de polvo interfieran. Este montaje paso a paso garantiza que cada pequeña pieza esté perfectamente alineada, lo que hace que los circuitos integrados sean fiables y eficientes.



La fotolitografía es el proceso utilizado para fabricar dispositivos semiconductores

2.2.7.3. ¿CÓMO FUNCIONAN LOS CIRCUITOS INTEGRADOS?

Un circuito integrado (CI) utiliza componentes diminutos para controlar el flujo de señales eléctricas. Cada parte del circuito tiene una función específica. Los transistores activan o desactivan las señales, las resistencias controlan el flujo y los condensadores almacenan energía eléctrica.

Todos estos componentes trabajan juntos para realizar una tarea, como procesar datos o amplificar el sonido. Las interacciones ocurren en fracciones de segundo, lo que permite realizar operaciones complejas dentro de dispositivos diminutos.

DISPOSICIÓN INTERNA

Los circuitos integrados se construyen sobre una fina lámina de material semiconductor, normalmente silicio. El silicio es único porque puede actuar como aislante y conductor. Esta propiedad le permite controlar el flujo de electricidad.

Los componentes se graban sobre el silicio en capas, lo que crea una estructura de varias capas. Cada capa forma diferentes partes del circuito. Algunas capas pueden contener transistores, mientras que otras forman vías que conectan estos transistores con otras partes.

FLUJO DE PROCESO

Así es como viajan las señales a través de un circuito integrado paso a paso:

1. **Señal de entrada**: El IC recibe una entrada, como un pequeño pulso eléctrico o datos digitales.
2. **Procesamiento de señales**: La señal se mueve a través de varias partes: los transistores conmutan, las resistencias la controlan y los capacitores la almacenan temporalmente.
3. **Conexión de caminos**: Cada componente está conectado a través de pequeñas líneas de metal, lo que permite que las señales pasen de una parte a otra.
4. **Señal de salida**: Después del procesamiento, el CI envía el resultado final. Puede ser un simple interruptor de encendido y apagado o un resultado computacional más complejo, como un comando de computadora.

La disposición precisa de estas vías es lo que hace que los circuitos integrados sean tan potentes. Con millones de piezas diminutas que trabajan juntas, pueden realizar tareas complejas de manera rápida y eficiente.

2.2.7.4. TIPOS DE CIRCUITOS INTEGRADOS

Existen muchos tipos de circuitos integrados, cada uno con su función. Veamos algunos de los tipos más comunes que se utilizan en la actualidad.

CIRCUITOS INTEGRADOS DIGITALES

Circuitos integrados digitales Funcionan con señales binarias, es decir, manejan 1 y 0. Son la columna vertebral de las computadoras, calculadoras y otros dispositivos digitales. Estos circuitos integrados realizan operaciones lógicas, como sumar números o comparar valores.

Los circuitos integrados digitales se encuentran en microprocesadores y chips de memoria. Procesan la información rápidamente y son muy fiables. Por ello, se utilizan en casi todos los dispositivos informáticos.

CIRCUITOS INTEGRADOS ANALÓGICOS

Circuitos integrados analógicos Trabajan con señales continuas, como niveles de sonido o voltaje. Se utilizan en dispositivos que necesitan procesar información del mundo real. Algunos ejemplos son los amplificadores de audio, los sensores de temperatura y los receptores de radio.

A diferencia de los circuitos integrados digitales, que trabajan con valores específicos, los circuitos integrados analógicos pueden trabajar con varios valores, lo que los hace ideales para tareas como amplificar una señal de audio débil o convertir la temperatura en una señal eléctrica.

CIRCUITOS INTEGRADOS DE SEÑAL MIXTA

Circuitos integrados de señal mixta Combinan componentes digitales y analógicos. Pueden manejar ambos tipos de señales en un solo chip, lo que los hace útiles en dispositivos que requieren ambos tipos de procesamiento.

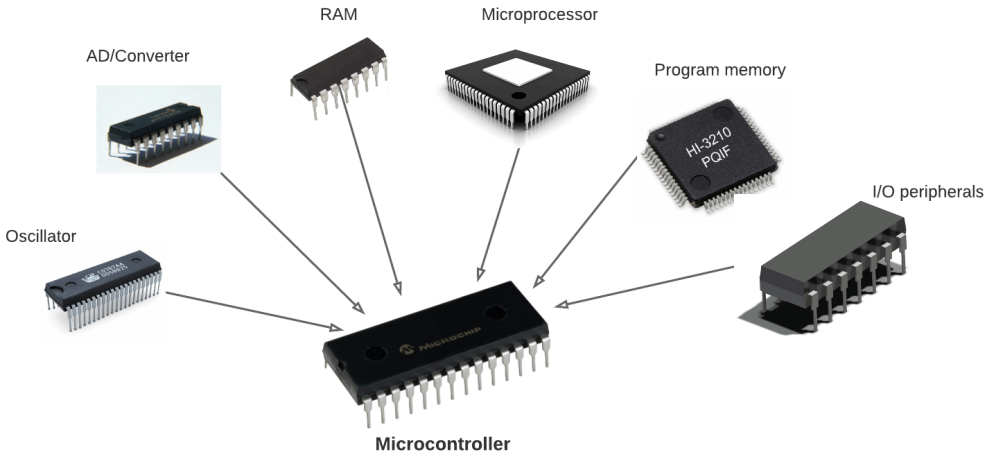
Entre los ejemplos se incluyen los teléfonos inteligentes, las cámaras y las radios digitales. Estos circuitos integrados permiten que los dispositivos alternen sin problemas entre el procesamiento de datos sin procesar (analógico) y la realización de cálculos (digital).

Por ejemplo, podrían tomar una señal de audio (analógica), convertirla a digital para procesarla y luego volverla a analógica para reproducirla.

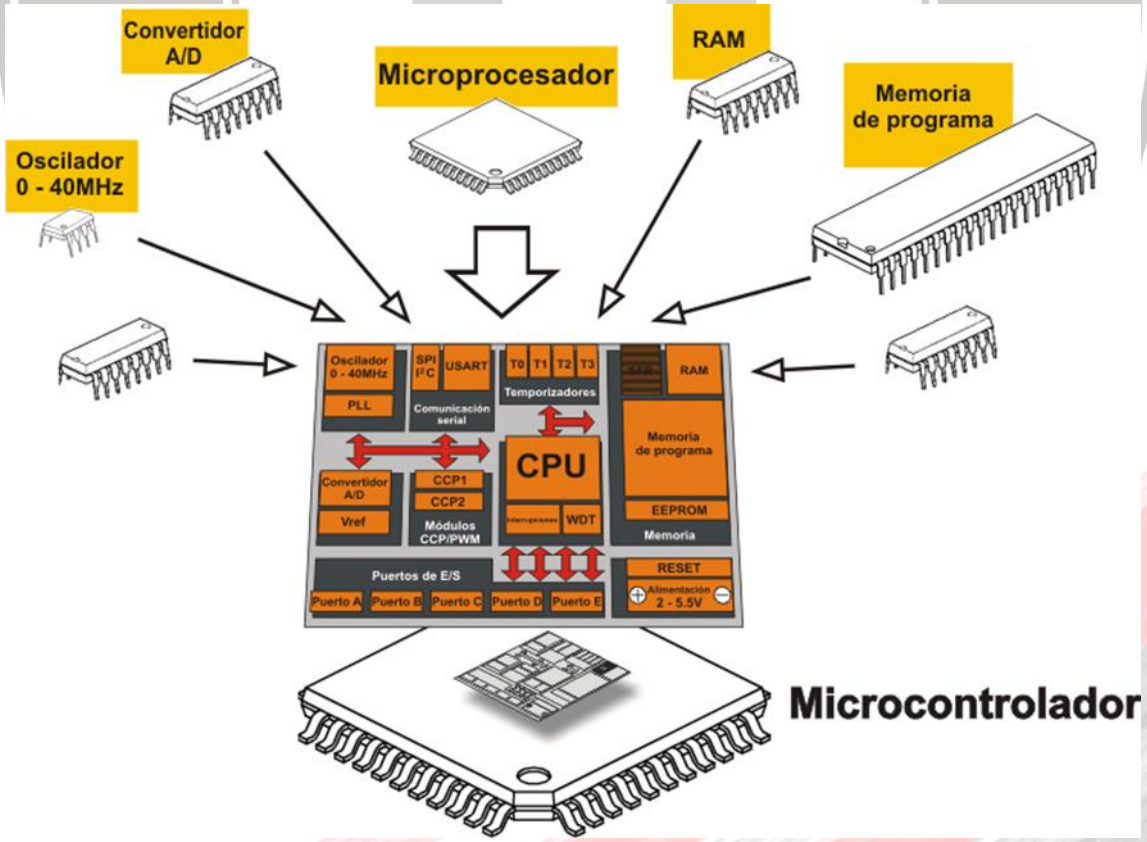
CIRCUITOS INTEGRADOS ESPECIALIZADOS

Los circuitos integrados especializados están diseñados para tareas específicas. Existen varios tipos principales:

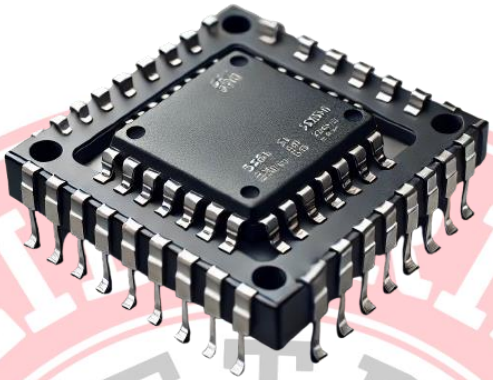
1. **Microcontroladores**: Son pequeñas computadoras en un solo chip. Tienen una CPU, memoria y puertos de entrada/salida (E/S). Se utilizan en aparatos domésticos como microondas, lavadoras y juguetes.



2. **Microprocesadores**: Son los "cerebros" de las computadoras. Procesan instrucciones complejas y manejan datos. Los encontrarás en PC, teléfonos inteligentes y consolas de juegos.



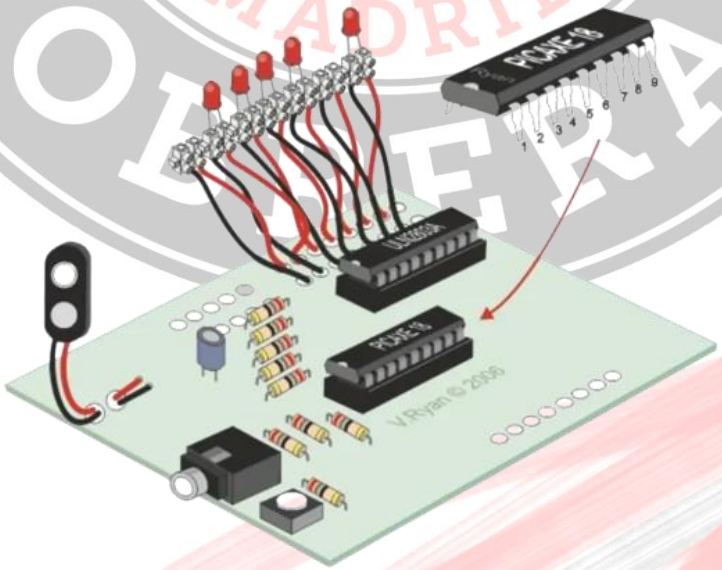
3. **Circuitos integrados de potencia**: Estos gestionan la distribución de energía en un circuito. Se utilizan en fuentes de alimentación, cargadores de baterías y controladores de LED. Los circuitos integrados de potencia garantizan que cada parte de un dispositivo reciba la cantidad correcta de energía sin sobrecalentarse.



Cada tipo tiene una función única para que los dispositivos electrónicos funcionen de manera eficiente y sin problemas. Comprender estos tipos nos ayuda a entender por qué los circuitos integrados son cruciales en nuestra vida diaria.

2.2.7.5. PROCESO DE FABRICACIÓN DE CIRCUITOS INTEGRADOS

El proceso de fabricación de circuitos integrados (CI) implica varios pasos detallados. He aquí un vistazo a las fases críticas:



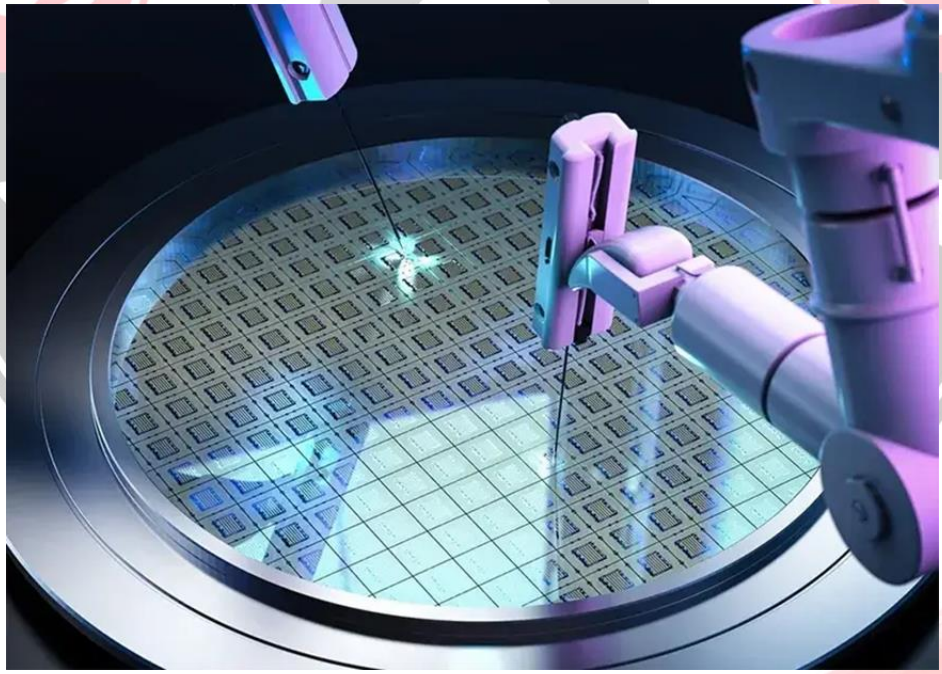
FASE DE DISEÑO

Los ingenieros crean el plano del circuito integrado durante la fase de diseño. Mediante herramientas de diseño asistido por ordenador (CAD), desarrollan un diseño detallado del chip, especificando dónde se colocará. Esta fase es crucial ya que determina la funcionalidad y el rendimiento del CI.

PASOS DE FABRICACIÓN

La fabricación es la parte más compleja de la producción de circuitos integrados. Implica varias etapas:

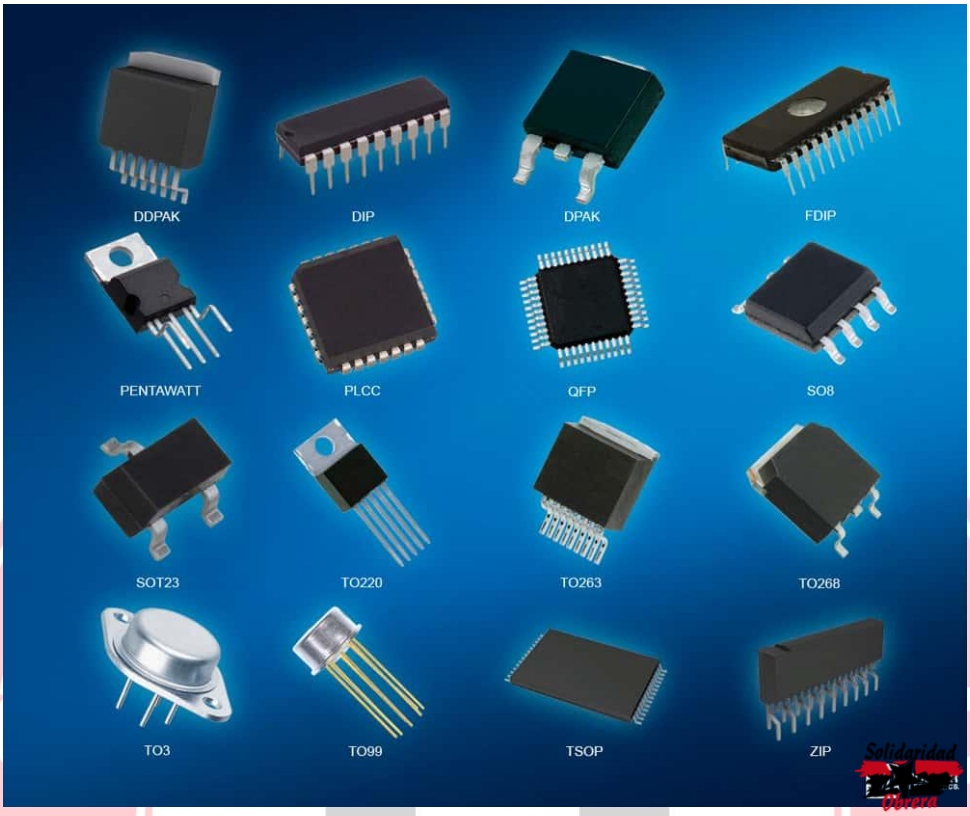
1. **Preparación de oblea:** Como material base se prepara una oblea de silicio puro.
2. **Fotolitografía:** Los patrones se transfieren a la oblea mediante exposición a la luz a través de máscaras.
3. **Grabando:** Se elimina el material no deseado para crear el patrón del circuito.
4. **Dopaje:** Se añaden impurezas para alterar las propiedades eléctricas del silicio.
5. **Capas:** Se depositan y modelan múltiples capas de materiales para construir el circuito completo.



MONTAJE Y EMBALAJE

Después de la fabricación, las obleas se cortan en chips individuales. Luego, cada chip se monta en un marco de cables y los cables conectan el chip a los cables externos.

Finalmente, el chip está encapsulado en un paquete protector para protegerlo de daños físicos y factores ambientales. Este embalaje garantiza que el CI pueda manipularse e integrarse fácilmente en varios dispositivos.



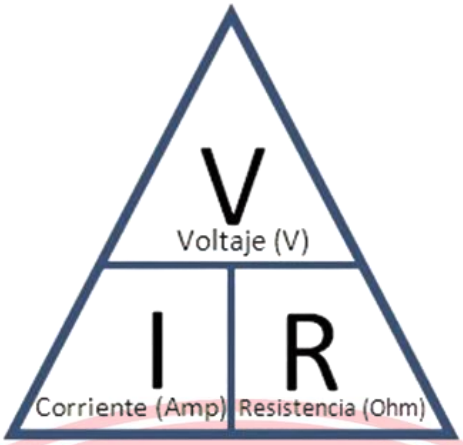
2.3. LEYES Y TEOREMAS DE CIRCUITOS

Las **Leyes de Kirchhoff** y los **Teoremas de Superposición y Thevenin** son herramientas clave para el análisis de circuitos eléctricos. Estas leyes establecen principios de conservación de carga y energía, permitiendo calcular corrientes y tensiones en diferentes puntos de un circuito. Los teoremas facilitan el estudio de circuitos con múltiples fuentes y su simplificación en modelos equivalentes, haciendo más eficiente su resolución.

2.3.1. LEY DE OHM:

La Ley de Ohm es un principio fundamental en la teoría de circuitos eléctricos y describe la relación entre la corriente eléctrica (I), la diferencia de potencial o voltaje (V), y la resistencia eléctrica (R) en un circuito eléctrico.

La expresión matemática de la Ley de Ohm es:



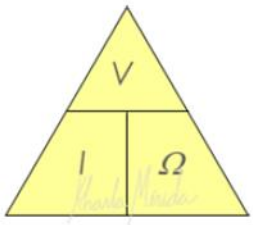
Donde:

- V es el voltaje en voltios (V).
- I es la corriente en amperios (A).
- R es la resistencia en ohmios (Ω).

Ley de Ohm. En un circuito recorrido por una corriente eléctrica, la tensión es igual al producto de la intensidad de corriente por la resistencia total del circuito. $V = I \cdot \Omega$

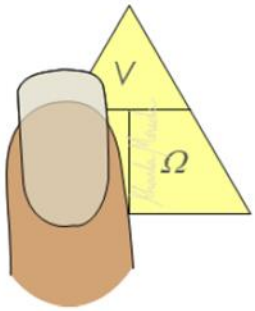
De esta ley podemos deducir dos relaciones más, despejando I o Ω, respectivamente:

$$I = \frac{V}{\Omega} \qquad \Omega = \frac{V}{I}$$

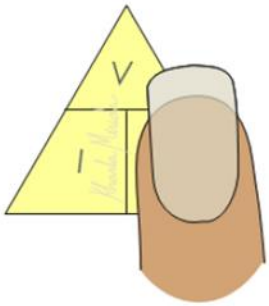


Existe una recurso mnemotécnico (recurso para recordar) presentado como la **regla de la pirámide**, para recordar la fórmula despejada de la intensidad y de la resistencia.

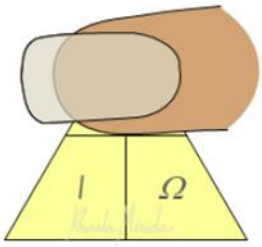
Cuando se desea saber la igualdad de una de las magnitudes se tapa la magnitud deseada y se observa la relación que queda.



$I = \frac{V}{\Omega}$



$\Omega = \frac{V}{I}$



$V = I \cdot \Omega$

Esta ecuación establece que la corriente en un circuito es directamente proporcional al voltaje aplicado e inversamente proporcional a la resistencia del circuito. En otras palabras, la corriente aumenta si el voltaje aumenta o si la resistencia disminuye.

2.3.2. LEYES DE KIRCHHOFF:

Las leyes de Kirchhoff son como las reglas de tránsito para la electricidad en los circuitos. Sirven para analizar cómo se comporta la corriente y el voltaje en diferentes partes de un circuito eléctrico. El físico alemán Gustav Kirchhoff formuló dos leyes básicas que gobiernan el comportamiento de las corrientes y voltajes en un circuito eléctrico.

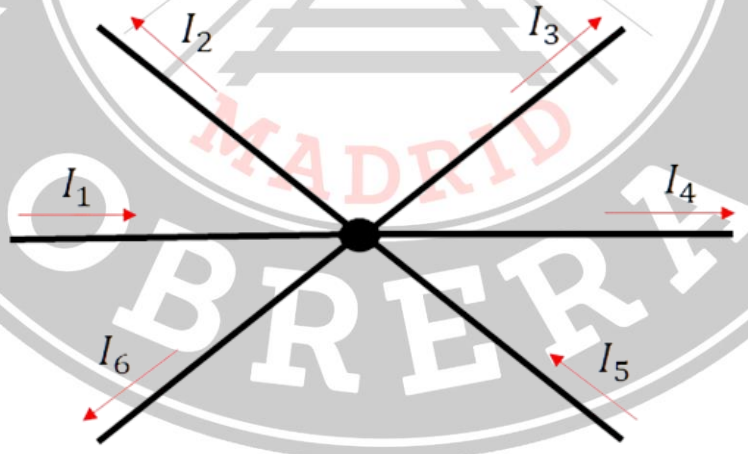
2.3.2.1. PRIMERA LEY: Ley de Kirchhoff de Corrientes (LKC)

Esta ley establece que la suma algebraica de las corrientes que entran en cualquier nodo de un circuito eléctrico es igual a la suma algebraica de las corrientes que salen de ese nodo. En otras palabras, en cualquier nodo de un circuito la suma de las corrientes entrantes y salientes en ese nodo es igual a cero. Matemáticamente, se expresa como:

$$\sum_{n=1}^{n} I_n = 0$$

$$I_1 + I_2 + I_3 + \cdots + I_n = 0$$

donde ***In*** representa las corrientes entrantes y salientes en un nodo y **n** es el número total de corrientes.



$$I_1 - I_2 - I_3 - I_4 + I_5 - I_6 = 0$$

En el ejemplo anterior se puede observar que las corrientes ***I1*** y ***I5*** entran al nodo, por lo que tendrán un signo positivo en la ecuación, mientras que las corrientes ***I2***, ***I3***, ***I4*** y ***I6*** salen del nodo, por lo que tendrán un signo negativo en la ecuación.

2.3.2.2. SEGUNDA LEY: Ley de voltajes de Kirchhoff (LKV):

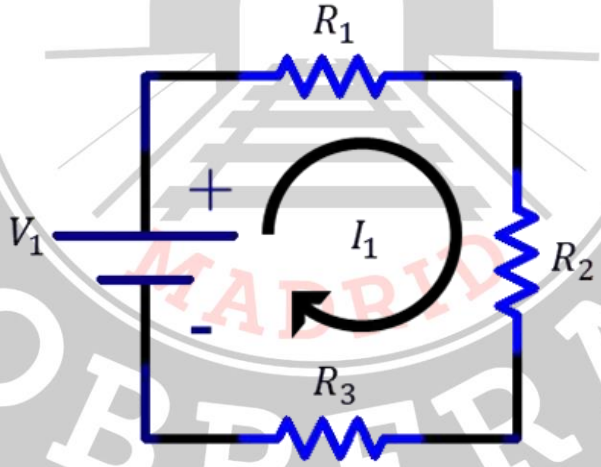
Esta ley establece que en cualquier lazo cerrado o malla de un circuito eléctrico, la suma algebraica de los voltajes alrededor de la malla es igual a cero. En otras palabras, en una malla cerrada la suma de los voltajes en una misma dirección es igual a cero. Matemáticamente, se expresa como:

$$\sum_{n=1}^{n} V_n = 0$$

$$V_1 + V_2 + V_3 + \cdots + V_n = 0$$

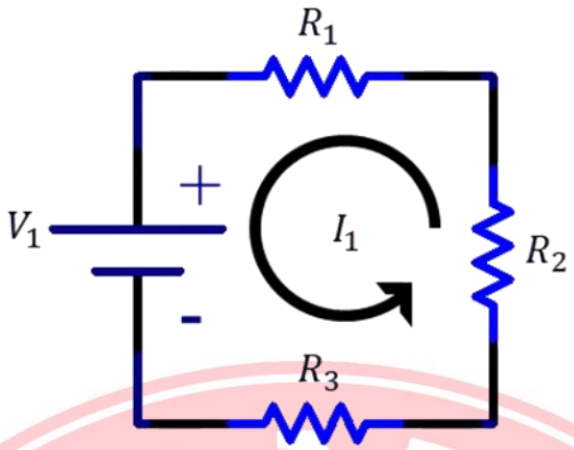
donde ***Vn*** representa los voltajes en una malla y ***n*** es el número total de elementos de voltaje en esa malla.

Ejemplos:



$$V_1 - I_1R_1 - I_1R_2 - I_1R_3 = 0$$

En el ejemplo anterior la dirección de la malla se establece en un sentido horario, **V1** suministra un voltaje por lo que tendrán un signo positivo en la ecuación de acuerdo al sentido de la malla, mientras que **R1**, **R2**, y **R3** representan caídas de voltaje, por lo que tendrán un signo negativo en la ecuación de acuerdo al sentido de la malla. Utilizando la ley de Ohm se puede calcular la caída de voltaje en las resistencias ***V=RI***.



$$-V_1 + I_1R_1 + I_1R_2 + I_1R_3 = 0$$

En el ejemplo anterior la dirección de la malla se establece en un sentido antihorario, **V1** suministra un voltaje por lo que tendrán un signo negativo en la ecuación de acuerdo al sentido de la malla, mientras que **R1**, **R2**, y **R3** representan caídas de voltaje, por lo que tendrán un signo positivo en la ecuación de acuerdo al sentido de la malla. Utilizando la ley de Ohm se puede calcular la caída de voltaje en las resistencias ***V=RI***.

Estas leyes son esenciales para analizar y resolver circuitos eléctricos complejos, ya que proporcionan las bases para la aplicación de métodos como el análisis de mallas y el análisis de nodos.

2.3.3. TEOREMA DE SUPERPOSICIÓN:

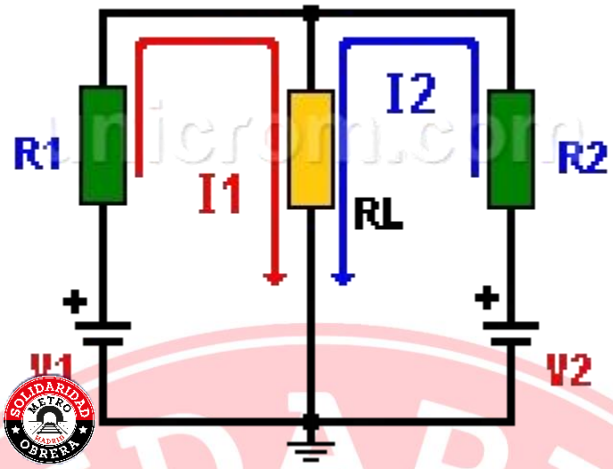
El teorema de superposición establece que, el efecto dos o más fuentes de voltaje y/o corriente tienen sobre un punto cualquiera en un circuito lineal, es igual a la suma de cada uno de los efectos de cada fuente tomados por separado, sustituyendo todas las fuentes de voltaje restantes por un corto circuito y las fuentes de corriente por circuitos abiertos.

El **teorema de superposición** ayuda a encontrar:

- Valores de tensión, en una posición de un circuito, que tiene más de una fuente de tensión y/o corriente.
- Valores de corriente, en un circuito con más de una fuente de tensión y/o voltaje.

Ejemplo de aplicación del Teorema de Superposición

Se desea saber cuál es la corriente que circula por la resistencia RL (resistencia de carga) en un circuito con dos fuentes de voltaje.

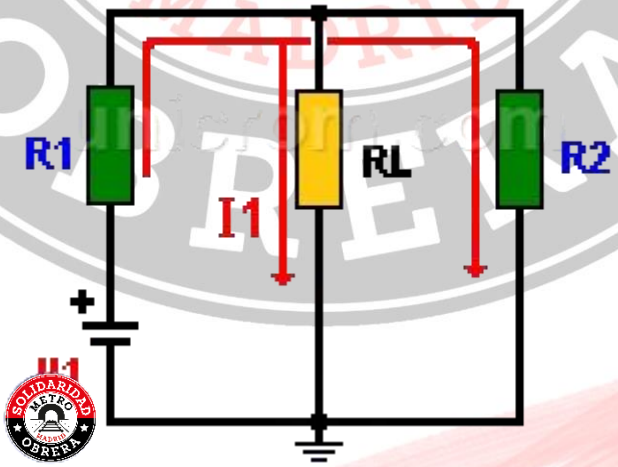


Teorema de Superposición – Circuito original

Los valores de las resistencias del circuito son las siguientes:

- **R1 = 2 kiloohmios**
- **R2 = 1 kiloohmio**
- **RL = 1 kiloohmio**
- **V1 = 10 voltios**
- **V2 = 20 voltios**

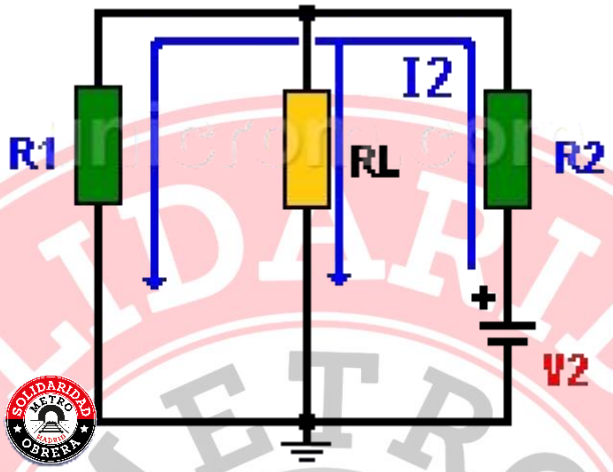
Como hay dos fuentes de voltaje, se utiliza una a la vez mientras se cortocircuita la otra. En el siguiente diagrama se toma en cuenta solo la fuente V1.



Teorema de Superposición – Primera fuente (V1)

En el diagrama inferior se toma en cuenta solo la fuente V2.

De cada caso se obtiene la corriente que circula por la resistencia RL y después estos dos resultados se suman para obtener la corriente total en la resistencia RL.



Teorema de Superposición – Segunda fuente (V2)

Procedimiento y Cálculos

Primero se analiza el caso en que solo está conectada la fuente **V1**. Se obtiene la corriente total que entrega esta fuente obteniendo la resistencia equivalente de las dos resistencias en paralelo **R1** y **RL**.

Req.= RL // R2 = 0.5 kiloohmios.

Nota: **//** significa paralelo.

A este resultado se le suma la resistencia **R1 (R1 está en serie con Req.)** y la resistencia total **RT = R1 + Req. = 0.5 + 2 = 2.5 kiloohmios.**

De esta manera se habrá obtenido la resistencia total equivalente en serie con la fuente **V1.**

Para obtener la corriente total se utiliza la **Ley de Ohm**:

I = V/R. I total = 10 Voltios / 2.5 kiloohmios = 4 mA (miliamperios).

Por el **teorema de división de corriente** se obtiene la corriente que circula por **RL**:

IRL = [I x RL // R2] / RL, donde RL // R2 significa el paralelo de RL y R2 (se obtuvo antes Req. = 0.5 kiloohmios).

Reemplazando: **IRL = [4 mA x 0.5 kiloohmios] / 1 kiloohmio = 2 mA. (miliamperios).**

El caso de la fuente **V2** se desarrolla de la misma manera, solo que se deberá cortocircuitar la fuente **V1**. En este caso la corriente se debe solo a la presencia de **V2** y es **8 mA**. (miliamperios). La corriente tiene el mismo sentido que la corriente encontrada debido a la fuente **V1** y por eso se suman.

Sumando las dos corrientes se encontrará la corriente que circula por la resistencia **RL** del circuito original. **Corriente total = IT = 2 mA. + 8 mA. = 10 mA. (miliamperios).**

Nota: Si las corrientes tuvieran sentidos opuestos se deben restar y el valor de la corriente resultante tendrá el sentido de la corriente de mayor valor.

Si se tiene la corriente total en la resistencia **RL**, también se puede obtener su voltaje en esta resistencia con solo utilizar la ley de Ohm: **VL= IT x RL.**

2.3.4. TEOREMA DE THEVENIN:

En la teoría de circuitos eléctricos, el teorema de Thévenin establece que si una parte de un circuito eléctrico lineal está comprendida entre dos terminales A y B, esta parte en cuestión puede sustituirse por un circuito equivalente que esté constituido únicamente por un generador de tensión en serie con una resistencia, de forma que al conectar un elemento entre los dos terminales A y B, la tensión que queda en él y la intensidad que circula son las mismas tanto en el circuito real como en el equivalente.

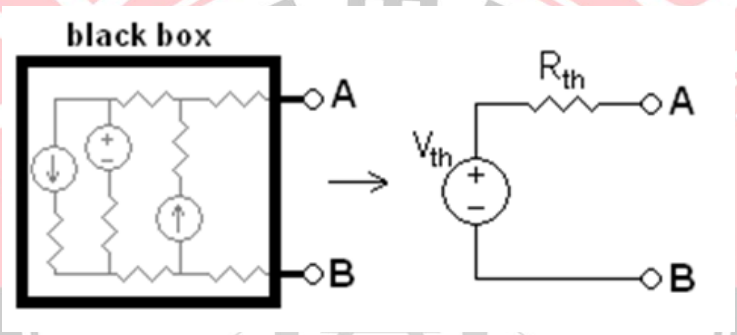
El teorema de Thévenin fue enunciado por primera vez por el científico alemán Hermann von Helmholtz en el año 1853,pero fue redescubierto en 1883 por el ingeniero de telégrafos francés Léon Charles Thévenin (1857–1926), de quien toma su nombre. El teorema de Thévenin es el dual del teorema de Norton.

Cálculo de la tensión y resistencia de Thévenin

Para calcular la tensión de Thévenin, Vth, se desconecta la carga (es decir, la resistencia de la carga) y se calcula VAB. Al desconectar la carga, la intensidad que atraviesa Rth en el circuito equivalente es nula y por tanto la tensión de Rth también nula, por lo que ahora VAB = Vth por la segunda ley de Kirchhoff.

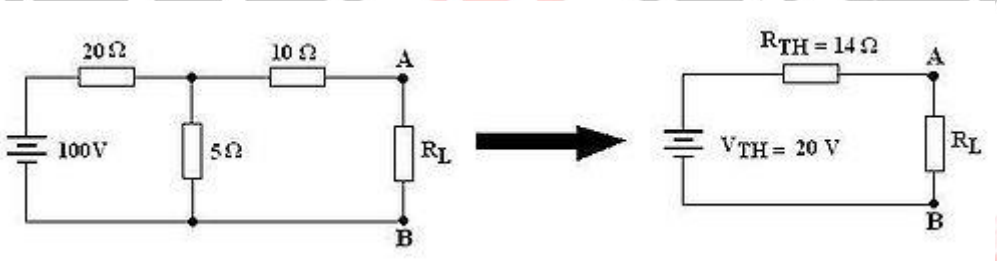
Debido a que la tensión de Thévenin se define como la tensión que aparece entre los terminales de la carga cuando se desconecta la resistencia de la carga también se puede denominar tensión en circuito abierto.

Para calcular la resistencia de Thévenin, se desconecta la resistencia de carga, se cortocircuitan las fuentes de tensión y se abren las fuentes de corriente. Se calcula la resistencia que se ve desde los terminales AB y esa resistencia RAB es la resistencia de Thévenin buscada Rth = RAB



Caja negra (izquierda) y su circuito Thévenin equivalente (derecha).

Ejemplo



En primer lugar, se calcula la **tensión de Thévenin** entre los terminales A y B de la carga; para ello, se desconecta RL del circuito (queda un circuito abierto entre A y B). Una vez hecho esto, podemos observar que la resistencia de 10 Ω está en circuito abierto y no circula corriente a través de ella, con lo que no produce ninguna caída de tensión. En estos momentos, el circuito que se necesita estudiar para calcular la tensión de Thévenin está formado únicamente por la fuente de tensión de 100 V en serie con dos resistencias, una de 20 Ω y otra de 5 Ω. Como la carga R_L está en paralelo con la resistencia de 5 Ω

(recordar que no circula intensidad a través de la resistencia de 10 Ω), la diferencia de potencial entre los terminales A y B es igual que la tensión que cae en la resistencia de 5 Ω (ver también Divisor de tensión), con lo que la tensión de Thévenin resulta:

$$V_{TH} = \frac{100V}{20\Omega + 5\Omega} \cdot 5\Omega \ = 20 \ V$$

Para calcular la **resistencia de Thévenin**, se desconecta la carga R_L del circuito y se anula la fuente de tensión sustituyéndola por un cortocircuito. Si se colocara una fuente de tensión (de cualquier valor) entre los terminales A y B, veríamos que las tres resistencias soportarían una intensidad. Por lo tanto, se halla la equivalente a las tres: las resistencias de 20 Ω y 5 Ω están conectadas en paralelo y estas están conectadas en serie con la resistencia de 10 Ω, entonces:

$$R_{TH} = \frac{20 \cdot 5}{20 + 5} + 10 \ \Omega = 14 \ \Omega$$

2.3.5. ELECTRÓNICA DIGITAL

2.3.5.1. SISTEMAS DE NUMERACIÓN

En electrónica digital, el sistema numérico esSe utiliza para representar la información. El sistema numérico tiene diferentes bases y las más comunes son el decimal, binario, octal y hexadecimal. los base o radix del sistema numérico es el número total del dígito utilizado en el sistema numérico. Supongamos que si el sistema numérico representa el dígito de 0 a 9, la base del sistema es el 10.

Tipos de sistemas de números

Algunos de los tipos importantes de sistema numérico son

- Sistema de números decimales
- Sistema de números binarios
- Sistema de números octales
- Sistema de números hexadecimales

Estos sistemas de números se explican a continuación en detalle.

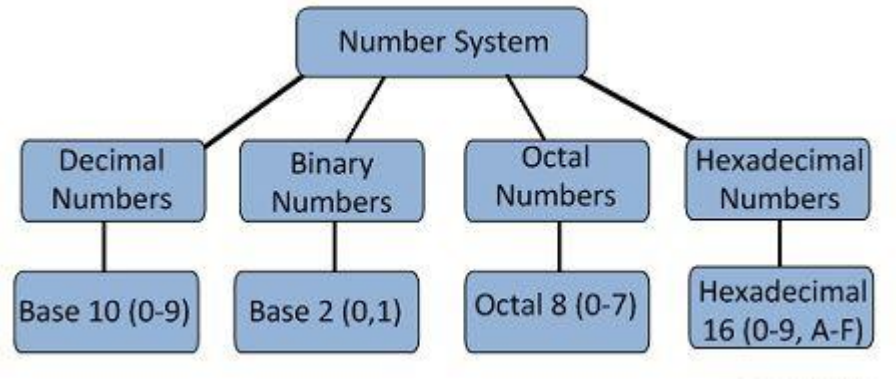


diagrama de bloques del sistema de números

1. **Sistemas de números decimales**

El sistema numérico tiene dígitos 0, 1, 2, 3, 4,5, 6, 7, 8, 9; este sistema numérico se conoce como sistema numérico decimal porque están involucrados un total de diez dígitos. La base del sistema numérico decimal es 10.

2. **Sistemas de números binarios**

DECIMAL	BINARIO	OCTAL	HEXADECIMAL
0	0	0	0
1	1	1	1
2	10	2	2
3	11	3	3
4	100	4	4
5	101	5	5
6	110	6	6
7	111	7	7
8	1000	10	8
9	1001	11	9
10	1010	12	A
11	1011	13	B
12	1100	14	C
13	1101	15	D
14	1110	16	E
15	1111	17	F
16	10000	20	10
17	10001	21	11
18	10010	22	12
19	10011	23	13

Las computadoras modernas no procesan decimales. Número; funcionan con otro sistema numérico conocido como sistema numérico binario que usa solo dos dígitos 0 y 1. La base del sistema numérico binario es 2 porque tiene solo dos dígitos 0 y 1. Los equipos electrónicos digitales funcionan en el sistema numérico binario y, por lo tanto, el sistema numérico decimal se convierte en sistema binario.

La tabla se muestra debajo de los números decimales, binarios, octales y hexadecimales de 0 a 15 y su número binario equivalente.

3. **Números octales**

La base de un sistema numérico es igual al número de dígitos utilizados, es decir, para el sistema numérico decimal, la base es diez, mientras que para el sistema binario la base es dos. El sistema octal tiene la base de ocho, ya que utiliza ocho dígitos 0, 1, 2, 3, 4, 5, 6, 7.

Todos estos dígitos del 0 al 7 tienen el mismo significado físico como por símbolos decimales, el siguiente dígito en el número octal se representa por 10, 11, 12, que son equivalentes a los dígitos decimales 8, 9, 10 respectivamente. De esta manera, el número octal 20 representará el dígito decimal y, posteriormente, 21, 22, 23 .. Los números octales representarán el dígito decimal número 17, 18, 19 ... etc. y así sucesivamente.

4. **Números hexadecimales**

Estos números se utilizan ampliamente en el trabajo con microprocesadores. El sistema de números hexadecimales tiene una base de 16, y por lo tanto consta de los siguientes dieciséis números de dígitos.

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

El tamaño del hexadecimal es mucho más corto que el número binario que hace que sean fáciles de escribir y recordar. Dejemos que 0000 a 000F representen números hexadecimales de cero a quince, luego 0010, 0011, 0012, ... etc. Representará dieciséis, diecisiete, dieciocho ... etc. hasta 001F que representan treinta abiertos y así sucesivamente.

2.4. ÁLGEBRA DE BOOLE

Aprender los conceptos básicos e importantes del álgebra booleana es de gran importancia para la solución de problemas en electrónica digital. Descubre qué es y cómo resolver de manera simple.

¿Qué es el álgebra booleana?

Es una rama especial del álgebra que se usa principalmente en electrónica digital. El álgebra booleana fue inventada en el año 1854 por el matemático inglés George Boole.

El álgebra de Boole es un método para simplificar los circuitos lógicos (o a veces llamados circuitos de conmutación lógica) en electrónica digital.

Por lo tanto, también se llama como "Cambio de álgebra". Podemos representar el funcionamiento de los circuitos lógicos utilizando números, siguiendo algunas reglas, que son bien conocidas como "Leyes del álgebra de Boole".

También podemos hacer los cálculos y las operaciones lógicas de los circuitos aún más rápido siguiendo algunos teoremas, que se conocen como "Teoremas del álgebra de Boole". Una función booleana es una función que representa la relación entre la entrada y la salida de un circuito lógico.

La lógica booleana solo permite dos estados del circuito, como True y False. Estos dos estados están representados por 1 y 0, donde 1 representa el estado "Verdadero" y 0 representa el estado "Falso".

Lo más importante para recordar en el álgebra de Boole es que es muy diferente al álgebra matemática regular y sus métodos. Antes de aprender sobre el álgebra de Boole, vamos a contar un poco sobre la historia del álgebra de Boole y su invención y desarrollo.

Historia del álgebra de Boole

Como se mencionó anteriormente, el álgebra de Boole se inventó en el año de 1854, por el matemático inglés George Boole. Primero declaró la idea del álgebra de Boole en su libro "Una investigación de las leyes del pensamiento".

Después de esto, el álgebra de Boole es bien conocida como la forma perfecta para representar los circuitos lógicos digitales.

A fines del siglo XIX, los científicos Jevons, Schroder y Huntington utilizaron este concepto para términos modernizados. Y en el año de 1936, MHStone demostró que el álgebra de Boole es 'isomorfo' para los conjuntos (un área funcional en matemáticas).

En la década de 1930, un científico llamado Claude Shannon desarrolló un nuevo método de álgebra tipo "Cambio de álgebra" utilizando los conceptos de álgebra de Boole, para estudiar los circuitos de conmutación.

La síntesis lógica de las herramientas modernas de automatización electrónica se representa de manera eficiente mediante el uso de funciones booleanas conocidas como "Diagramas de decisión binarios".

El álgebra de Boole permite solo dos estados en un circuito lógico, como Verdadero y Falso, Alto y bajo, Sí y No, Abierto and Cerrado o 0 y 1.

Leyes e identidades del álgebra booleana

Al formular expresiones matemáticas para circuitos lógicos es importante tener conocimiento del álgebra booleana, que define las reglas para expresar y simplificar enunciados lógicos binarios. Una barra sobre un símbolo indica la operación booleana NOT, que corresponde a la inversión de una señal.

Leyes fundamentales

OR	AND	NOT
$A + 0 = A$	$A \cdot 0 = 0$	$\overline{\overline{A}} = A$
$A + 1 = 1$	$A \cdot 1 = A$	
$A + A = A$	$A \cdot A = A$	
$A + \overline{A} = 1$	$A \cdot \overline{A} = 0$	

Leyes conmutativas

$A + B = B + A$

$A \cdot B = B \cdot A$

Leyes asociativas

$(A + B) + C = A + (B + C)$

$(A \cdot B) \cdot C = A \cdot (B \cdot C)$

Leyes distributivas

$A \cdot (B + C) = (A \cdot B) + (A \cdot C)$

$A + (B \cdot C) = (A + B) \cdot (A + C)$

Otras identidades útiles

$A + (A \cdot B) = A$

$A \cdot (A + B) = A$

$A + (A \cdot B) = A + B$

$(A + B) \cdot (A + B) = A$

$(A + B) \cdot (A + C) = A + (B \cdot C)$

$A + B + (A \cdot B) = A + B$

$(A \cdot B) + (B \cdot C) + (B \cdot C) = (A \cdot B) + C$

$(A \cdot B) + (A \cdot C) + (B \cdot C) = (A \cdot B) + (B \cdot C)$

Simplificación de funciones booleanas

Al usar los teoremas y leyes booleanas, podemos simplificar las expresiones booleanas, mediante las cuales podemos reducir el número requerido de compuertas lógicas a implementar. Podemos simplificar la función Boolean utilizando dos métodos:

1. El método algebraico: mediante el uso de identidades (leyes booleanas).
2. El método gráfico: utilizando el método del Mapa de Karnaugh.

***Ejemplo**: Se va a simplificar la siguiente expresión aplicando las leyes e identidades booleanas mencionadas:*

E = (X · Y · Z) + (Y · Z) + (X · Y)

Es posible aplicar la ley asociativa y la ley fundamental de que A · 1 = A:

E = X · (Y · Z) + 1 · (Y · Z) + (X · Y)

Ahora es posible factorizar el termino (Y · Z):

E = (X + 1) · (Y · Z) + (X · Y)

Dado que A + 1 = 1 según las leyes fundamentales por lo tanto X + 1 = 1:

E = 1 · (Y · Z) + (X · Y)

Al realizar la operación tendremos ya simplificada la expresión:

E = (Y · Z) + (X · Y)

Aún podemos simplificar la expresión al factorizar Y:

E = Y · (Z + X)

2.5. PUERTAS LÓGICAS

Las puertas lógicas son de los componentes electrónicos de mayor uso en el área de la electrónica digital, por esa razón es importante entender los conceptos básicos de cada compuerta lógica.

¿Qué son las puertas lógicas?

Las **puertas lógicas son el corazón de la electrónica digital**. Básicamente, todas las puertas lógicas tienen una salida y dos entradas, algunas compuertas lógicas como la

compuerta NOT o el inversor tienen solo una entrada y una salida. Las entradas de las compuertas lógicas están diseñadas para recibir solo datos binarios (bajo 0 o alto 1) al recibir la señal de voltajes.

El nivel lógico en bajo representa cero volts y el nivel lógico en alto representa 3 o 5 volts.

Es posible conectar cualquier número de puertas lógicas para diseñar un circuito digital requerido. Prácticamente, implementamos una gran cantidad de puertas lógicas en circuitos integrados, mediante las cuales podemos guardar el espacio físico ocupado por éstas. También es posible realizar operaciones complicadas a altas velocidades mediante el uso de circuitos integrados (IC).

Combinando puertas lógicas, podemos diseñar muchos circuitos específicos, como flip flops, multiplexores, registros de desplazamiento, etc.

> **Nota**: Algunos datos mencionados pueden variar, es recomendable verificar en la hoja de datos del componente.

¿Qué es activo alto y activo bajo?

El pin bajo activo debe estar conectado a un nivel lógico bajo o a tierra. De la misma manera, el pin alto activo debe estar conectado a un nivel lógico alto como pudiera ser 5 voltios o 3.3 voltios.

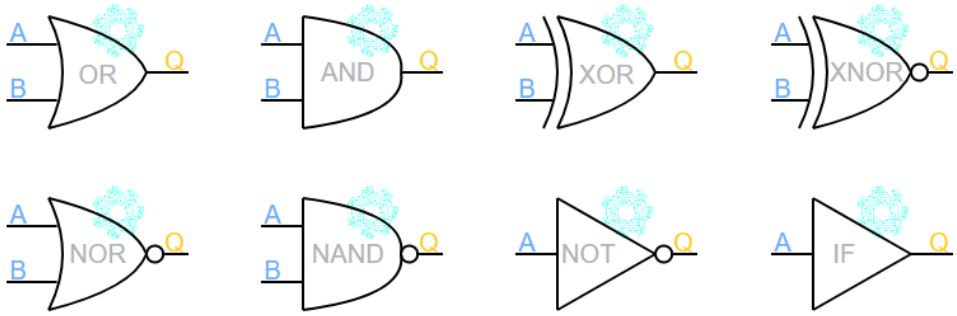
Comprendamos esto de una manera simple. Cuando vemos el pin de habilitación CE en un IC de registro de desplazamiento, sin ninguna línea (barra), lo conectamos a una entrada activa baja, es decir, a 0 voltios de tierra. De lo contrario, si vemos el pin de habilitación con una línea como $(\overline{CE})$, lo conectamos a la entrada alta activa, es decir, a 3.3 o 5 voltios de suministro, para habilitar el pin.

Puertas lógicas y tablas de verdad

Los dispositivos lógicos combinacionales son dispositivos digitales que convierten entradas binarias en salidas binarias con base en las reglas de la lógica matemática. Estos dispositivos son comúnmente conocidos como puertas, ya que controlan el flujo de señales de las entradas a una sola salida.

Es recomendable conocer las operaciones básicas del álgebra booleana.

Cada puerta lógica se puede representar mediante un símbolo gráfico correspondiente a la siguiente representación:



Como podemos observar, vamos a tratar con 8 puertas importantes INV o NOT, AND, NAND, OR, NOR, XOR, XNOR y BUFFER o IF en las cuales se dará a conocer la operación que realiza, la expresión con la que se puede denotar, símbolo y tabla de verdad.

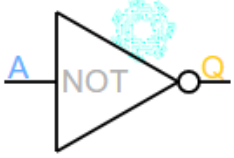
Consideración:

- Se considera un estado activo "1" (alto lógico) e inactivo "0" (bajo lógico).
- Las entradas de las compuertas se consideran como "A" y "B", la salida se representa con "Q".

2.5.1.1. Puerta NOT o INV

Su expresión es representada con una letra testada, para esta puerta únicamente se cuenta con una entrada y una salida por lo tanto actúa como un inversor. Si la entrada se encuentra en estado activo "1" se tendrá a la salida un estado inactivo "0" y para el caso contrario, si la entrada se encuentra en estado inactivo "0" a la salida estará en estado activo "1".

Símbolo



Expresión

$Q = \bar{A}$

Tabla de verdad

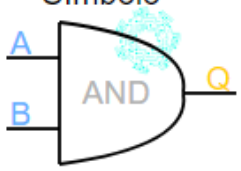
A	Q
0	1
1	0

2.5.1.2. Puerta AND

En el Álgebra de Boole se representa por una multiplicación, por lo tanto, para tener la salida en estado activo es necesario que sus entradas tengan un estado binario 1, al tener una entrada inactiva "0" su salida será 0. Es posible representarlo mediante un circuito

que tenga sus interruptores en serie, al tener todos los interruptores activos permite cerrar el circuito y por lo tanto el flujo de la corriente.

Símbolo



Expresión

$Q = A \cdot B$

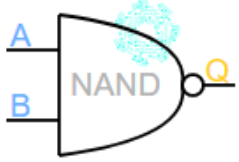
Tabla de verdad

A	B	Q
0	0	0
0	1	0
1	0	0
1	1	1

2.5.1.3. Puerta NAND

También conocida como AND negada o inversa, es una combinación de las puertas AND y NOT que se representa con la compuerta AND con un círculo a la salida, al tener sus entradas activas "1" la salida se encuentra inactiva "0", otra variación con respeto a las entradas mantendrá su salida en estado activo "1". Se puede representar mediante un circuito con dos interruptores en serie y debemos recordar que el flujo de corriente circula por donde se tenga menor resistencia.

Símbolo



Expresión

$Q = \overline{A \cdot B}$

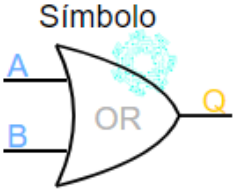
Tabla de verdad

A	B	Q
0	0	1
0	1	1
1	0	1
1	1	0

2.5.1.4. Puerta OR

Su expresión en el Álgebra de Boole es representada por una suma. Esta puerta se encuentra en estado activo siempre y cuando una de sus entradas tenga un estado binario activo "1". Para lograr un estado inactivo "0" a la salida, es necesario que todas sus entradas se encuentren en estado inactivo "0". Se puede representar mediante un circuito que tenga dos interruptores en paralelo, al accionar un interruptor permite cerrar el circuito y por lo tanto el flujo de la corriente.

Símbolo



Expresión

$Q = A + B$

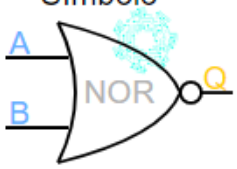
Tabla de verdad

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	1

2.5.1.5. Puerta NOR

Es una combinación de las puertas OR y NOT, en otras palabras, la puerta NOR es la versión inversa de la puerta OR. Al tener sus entradas en estado inactivo “0” su salida estará en un estado activo “1”, pero si alguna de las entradas pasa a un estado binario “1” su salida tendrá un estado inactivo “0”. Se puede representar mediante un circuito con los interruptores y salida en paralelo, para tener la salida en estado activo “1” es necesario que ambos interruptores se encuentren abiertos, mientras alguno de los interruptores se encuentre cerrado la salida “y” tendrá un estado binario “0”.

Símbolo



Expresión

$$Q = \overline{A + B}$$

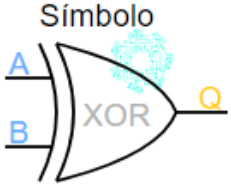
Tabla de verdad

A	B	Q
0	0	1
0	1	0
1	0	0
1	1	0

2.5.1.6. Puerta XOR

También conocida como “OR exclusiva”, su expresión Booleana es una suma binaria de un dígito cada uno y el resultado obtenido será la salida. La salida tiene un estado activo “1” al tener las entradas en estados diferentes (Una activa y otra inactiva). Su representación es mediante cuatro interruptores que se encuentran acoplados mecánicamente a su valor negado, de este modo cuando A se cierra entonces A´ se abre y viceversa, lo mismo ocurre con el interruptor B con respecto al B´.

Símbolo



Expresión

$$Q = A \oplus B$$

$$Q = A \cdot \overline{B} + \overline{A} \cdot B$$

Tabla de verdad

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

2.5.1.7. Puerta XNOR

Es la negación de la puerta XOR, cuando las entradas sean iguales se representará una salida en estado “1” y si son diferentes la salida será un estado “0”.

Símbolo

Expresión

$$Q = \overline{A \oplus B}$$

$$Q = \overline{A \cdot \overline{B} + \overline{A} \cdot B}$$

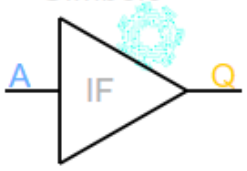
Tabla de verdad

A	B	Q
0	0	1
0	1	0
1	0	0
1	1	1

2.5.1.8. Puerta IF o Buffer

Es una de las puertas menos utilizadas o reconocidas, pero a veces es necesaria, sus estados lógicos permanecen del mismo modo, se podría considerar como un cable conectado ya que lo que tenemos a la entrada se obtendrá a la salida. La función principal del buffer es aumentar la corriente suministrada a la salida mientras se retiene el estado lógico, en la práctica es utilizado para amplificar la corriente o como seguidor de tensión para adaptar impedancias.

Símbolo



Expresión

$$Q = A$$

Tabla de verdad

A	Q
0	0
1	1

Niveles lógicos digitales

Un nivel lógico se define como un estado o voltaje específico de una señal, sabemos que 0 y 1 son los dos estados de puertas lógicas. Los niveles lógicos 0 y 1 se conocen como BAJO y ALTO, respectivamente. En electrónica digital, estos niveles lógicos binarios desempeñan un papel crucial en el almacenamiento y la transferencia de datos.

En general, estos niveles lógicos se pueden entender como estados de encendido y apagado. Como se mencionó anteriormente, los niveles lógicos se introducen en la puerta lógica mediante el voltaje de suministro.

De manera similar, si el voltaje de suministro a la puerta lógica es de 5 voltios o 3.3 voltios (para circuitos integrados modernos), se refiere al nivel lógico alto o estado de encendido. Los fabricantes seguirán el TTL (Transistor - Transistor Logic) como nivel de voltaje estándar, mientras diseñan los circuitos integrados.

Niveles lógicos TTL

Los transistores son interruptores controlados eléctricamente. Los niveles de voltaje de las familias lógicas son:

- **VOH**: Mínimo nivel de voltaje de salida para señal ALTA.
- **VOL**: Máximo nivel de voltaje de salida para señal BAJA.
- **VIH**: Mínimo nivel de voltaje de entrada de un dispositivo para ser considerado en señal ALTA.
- **VIL**: Máximo nivel de voltaje de entrada de un dispositivo para ser considerado en señal BAJA.

Si observamos los niveles lógicos TTL, podemos identificar que el nivel mínimo de alto voltaje para la salida es de 2.7 voltios. Esto significa que, cuando el dispositivo está funcionando en ALTO, el voltaje debe ser de al menos 2.7 voltios.

De manera similar, el nivel del estado alto tendrá un voltaje mínimo para la entrada, el cual es de 2 voltios. Por lo tanto, los voltajes superiores a 2 voltios se considerarán como lógicos 1, en un dispositivo TTL. Los voltajes entre 0,8 voltios y 2 voltios se conocen como margen de ruido.

De manera similar, el nivel máximo de estado bajo tendrá un voltaje para la entrada, el cual es de 0,8 voltios.

Por ello, los voltajes menores a 0 voltios se considerarán como lógicos 0, en un dispositivo TTL. Entonces, cuando el dispositivo lógico recibe voltajes entre 0.8 V y 2 V, el nivel lógico del dispositivo cambiará entre Alto y Bajo. Este cambio se llama 'Flotante'.

Niveles lógicos CMOS

Los dispositivos lógicos CMOS también se conocen como dispositivos de 3.3 voltios debido a que tendrán el nivel máximo de voltaje de 3.3 V. Esta es una tecnología avanzada que ejecutará los dispositivos con bajo suministro de energía (3.3 V en lugar de 5 V).

Sobre todo, utilizamos dispositivos de 5 V (compatibles con TTL) para diseñar compuertas lógicas, por lo que estos dispositivos CMOS se utilizan para interactuar con dispositivos TTL. Un dispositivo CMOS puede interactuar con cualquier dispositivo TTL y no requieren ningún componente adicional.

Por ejemplo, el valor mínimo para un nivel lógico alto (1) de un dispositivo CMOS es de 2,4 V. Por lo tanto, este dispositivo se puede interpretar con un dispositivo TTL que tiene una tensión de entrada mínima lógica en estado 1 como 2 V.

Pero, antes de conectar los dispositivos TTL a CMOS (3.3 V y 5 V), debemos verificar que los dispositivos de 3.3 V sean o no tolerantes a 5 V. Debido a que muchos de ellos causarán daños en el chip permanentemente cuando suministremos voltajes superiores a 3.6 V. Podemos utilizar un circuito divisor de voltaje o palancas de nivel lógico para controlar las señales de voltaje de 5 V.

Margen de ruido

El margen de ruido de un nivel lógico se define como la brecha de voltaje entre la baja tensión máxima de entrada alta (VIL máx.) y la tensión máxima de la entrada baja (VIL mín.) de una compuerta lógica. El margen de ruido también se define como la cantidad por la cual la señal de voltaje excede el nivel de umbral para el mínimo o alto exacto.

Vamos a entender esto claramente con un ejemplo. Cuando un circuito lógico está alterando entre 0 voltios y 1.2 voltios, con cualquier voltaje por debajo de 0.2 voltios se considera BAJO, es decir, 0. Y cualquier voltaje superior a 1 voltio se considera ALTO, es decir, 1.

Los dispositivos lógicos CMOS tienen mayor nivel de ruido o margen de ruido que los dispositivos lógicos TTL porque su tensión de salida mínima para alta lógica (VOH min) está más cerca de la tensión de alimentación y la tensión máxima de salida para baja lógica (VOL máx.) es aproximadamente 0. Por lo tanto, este nivel es la cantidad máxima de ruido que un circuito lógico puede soportar.

Si aplicamos un voltaje de cierto nivel de ruido, no sabemos con certeza si el circuito responderá o no. El nivel de ruido es el nivel de voltaje no deseado, causado por interferencia externa tal como fluctuaciones de voltaje de suministro y otros conductores en el circuito.

El nivel de ruido que puede tolerar un circuito se denomina "Inmunidad al ruido" o "Margen de ruido". Para dispositivos TTL, el rango de tolerancia de los voltajes de salida es mayor que el de los voltajes de entrada.

Algunos IC más utilizados para el diseño de puertas lógicas

Puertas de 2 entradas

- 74LS00 - puerta NAND de 2 entradas.
- 74LS01 - puerta NAND de 2 entradas, salidas de colector abierto.
- 74LS02 - puerta NOR de 2 entradas.
- 74LS03 - puerta NAND de 2 entradas con salidas de colector abierto.
- 74LS08 - puerta AND de 2 entradas.
- 74LS09 - puerta cuádruple de 2 entradas y con salidas de colector abierto.
- 74LS32 - puerta OR de 2 entradas.
- 74LS132 - puerta con entrada NAND de 2 entradas con entradas de activación Schmitt
- 74LS37, 74LS32, 74LS28 - puerta NOR de 2 entradas.
- 74LS26 - puerta NAND de 2 entradas, OC (15V).

- 74LS28 - puerta NAND de 2 entradas con OC (15V).
- 74LS33 - puerta NOR de 2 entradas, salidas de colector abierto.
- 74LS38 - puerta NOR de 2 entradas, salidas de colector abierto.

Puertas de 3 entradas

- 74LS10 - puerta NAND de 3 entradas.
- 74LS11 - puerta AND de 3 entradas.
- 74LS12 - puerta NAND de 3 entradas con salidas de colector abierto.
- 74LS27 - puerta NOR de 3 entradas.
- 74LS15 - puerta AND de 3 entradas y salida de colector abierto.

Puertas de 4 entradas

- 74LS30 - puerta NAND de 8 entradas.

Puertas de 8 entradas

- 74LS30 - puerta NAND de 8 entradas.

Puertas inversores

- 74LS04 - puerta NOT.
- 74LS05 - puerta NOT con salidas de colector abierto.
- 74LS14 - puerta NOT con entradas de Schmitt Trigger.
- 74LS19 - puerta NAND con entradas Schmitt Trigger.
- 74lS23
- 74LS30 - puerta NAND de 8 entradas.
- 74LS39 - puerta NAND, colector abierto.

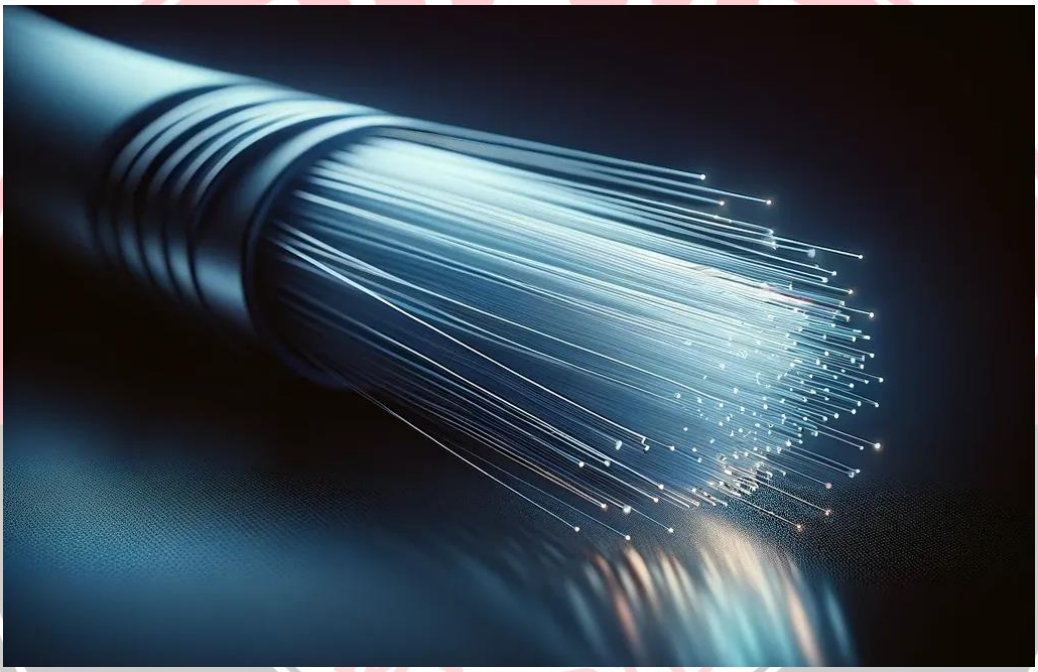
2.5.2. OPTOELECTRÓNICA:

La optoelectrónica es un campo en rápido crecimiento que combina la electrónica y la óptica para utilizar la luz en el tratamiento de la información.

Se basa en los fenómenos de interacción de la luz y otras formas de radiación electromagnética con materiales semiconductores. Esto permite convertir las señales eléctricas en ópticas y viceversa. Los dispositivos optoelectrónicos utilizan efectos como la fotoelectricidad, la fotovoltaica, la fotoemisión o la electroluminiscencia para detectar, emitir y modular la luz.

La optoelectrónica combina los logros de la química, la física del estado sólido y la electrónica para crear un campo interdisciplinar con un amplio espectro de aplicaciones. Incluye las tecnologías de adquisición, transmisión, tratamiento y presentación de la información por medio de la luz. Permite diseñar dispositivos rápidos y eficaces, como láseres, detectores de radiación, moduladores ópticos o pantallas.

La optoelectrónica desempeña un papel fundamental en las telecomunicaciones y los sistemas informáticos actuales. Permite la transmisión ultrarrápida de enormes cantidades de datos mediante fibras ópticas. También se utiliza en medicina, industria, transporte y muchos otros campos. Su importancia crecerá a medida que el mundo se digitalice y aumente la necesidad de sistemas de procesamiento de la información cada vez más rápidos. Podría decirse que la optoelectrónica está impulsando la revolución digital y es una tecnología clave del futuro.



Historia de los descubrimientos y sus aplicaciones en optoelectrónica

Uno de los primeros descubrimientos físicos que condujeron al desarrollo de la optoelectrónica moderna es lo que se conoce como «optoelectrónica». el efecto fotoeléctrico. El efecto fotoeléctrico consiste en la emisión de electrones por un material cuando se expone a determinados tipos de luz. Cuando el material absorbe suficiente energía en forma de luz, los electrones pueden desprenderse de la superficie del material, provocando el paso de una corriente eléctrica y dejando huecos de electrones. Un fenómeno similar es el efecto fotovoltaico, en el que la luz absorbida provoca un cambio en los estados energéticos de los electrones del material, lo que da lugar a una tensión que puede producir una corriente eléctrica.

1. **Células Las células solares utilizan la optoelectrónica para convertir la luz en energía**
   La generación de electricidad en células solares que absorben la luz del sol es una aplicación habitual que utiliza estos efectos. La electricidad así generada puede utilizarse directamente o almacenarse en baterías para su uso posterior. Las aplicaciones prácticas de las células solares incluyen la generación de energía tanto en la Tierra, por ejemplo, en hogares aislados en zonas remotas, como en el espacio, por ejemplo, en satélites.

2. **Los dispositivos optoelectrónicos desempeñan un papel clave en aplicaciones y productos, desde ordenadores a comunicaciones.**
   La electroluminiscencia es otro fenómeno importante utilizado en optoelectrónica. Cuando una corriente eléctrica fluye a través de ciertos materiales, hace que los electrones de niveles de energía altos se combinen con huecos de electrones y se desplacen a niveles de energía más bajos y estables, liberando energía en forma de luz. Los LED son un ejemplo común del uso de la electroluminiscencia. Los LED de distintos colores se utilizan como indicadores de potencia, en pantallas digitales como las de calculadoras y electrodomésticos, para iluminar señales y farolas, como faros y luces de coches, y mucho más. Los salpicaderos de los vehículos también suelen utilizar la electroluminiscencia para iluminarse.

3. **El uso de la optoelectrónica permitió desarrollar fotocopiadoras**
   La fotoconductividad es el fenómeno de aumento de la conductividad de un material cuando se expone a la luz. Este efecto depende de que una mayor intensidad luminosa genera más electrones y huecos electrónicos en algunos materiales, lo que aumenta su conductividad eléctrica. Este fenómeno particular de la optoelectrónica hizo posible la construcción de fotocopiadoras. Cuando una superficie fotoconductora de una fotocopiadora se expone a una imagen, se crea una diferencia de conductividad entre las zonas iluminadas que no contienen imagen y las zonas no iluminadas que sí la contienen. Como resultado, el polvo en la máquina se distribuye en forma de imagen, después de lo cual se fija en una hoja de papel, completando el proceso de copia.

4. **La optoelectrónica puede utilizarse para automatizar el trabajo administrativo de varias maneras**
   Estos y otros efectos optoelectrónicos se están integrando en un enorme número de dispositivos y aplicaciones en numerosas combinaciones, y aún hay más en fase de desarrollo. El uso de la optoelectrónica ha revolucionado muchas industrias. Los dispositivos optoelectrónicos desempeñan un papel fundamental en aplicaciones y productos: desde ordenadores a comunicaciones, pasando por tecnología médica o equipos militares, fotografía y otras técnicas de imagen, entre otros.

Elementos optoelectrónicos: ¿qué tipos existen y cómo funcionan?

Existen diversos componentes optoelectrónicos que convierten las señales luminosas en eléctricas y viceversa. Las más importantes son:

- **Fotodiodos**: sensores de luz semiconductores construidos a partir de una unión P-N activa que genera una corriente o tensión cuando la luz incide sobre la unión. Tienen distintos modos de funcionamiento y se utilizan, entre otros. en equipos médicos e industriales.
- **Células fotovoltaicas**: convierten la energía solar directamente en electricidad. Ampliamente utilizado en sistemas de telecomunicaciones, navegación marítima o electrificación rural.
- **Fotoresistencias**: resistencias controladas por la luz cuya resistencia disminuye con la iluminación. Se utiliza en sensores de luz e interruptores.
- **LED**: diodos semiconductores que emiten luz por electroluminiscencia. Se utilizan mucho como indicadores y fuentes de luz en electrónica.
- **Circuitos integrados de sensores codificadores**: convierten el movimiento rotativo o lineal en señales eléctricas en sistemas de control de movimiento.
- **Diodos láser**: diodos semiconductores que convierten la energía eléctrica en luz láser. Se aplica, entre otras cosas, a en reproductores de CD, dispositivos médicos y telecomunicaciones.
- **Fibra óptica**: transmite información en forma de luz modulada. Utilizado en telecomunicaciones, sensores.

Aplicaciones de la optoelectrónica

Los dispositivos y componentes optoelectrónicos se utilizan ampliamente en muchos campos:

Comunicación

La optoelectrónica desempeña un papel fundamental en los sistemas de comunicación modernos. La fibra óptica, que utiliza el fenómeno de la reflexión total interna, permite transmitir señales a grandes distancias. Los láseres y otros componentes, como

moduladores o fotodetectores, se utilizan para convertir señales eléctricas en ópticas y viceversa. Esto permite una comunicación rápida, segura y fiable.

Medicina y diagnóstico

En medicina se utiliza, entre otras cosas, la optoelectrónica. en diagnóstico por imagen, medición de biomarcadores, endoscopia o imagen in vivo. También se utiliza en aplicaciones terapéuticas, como la terapia con láser para tratar trastornos cutáneos o la corrección de la visión con láser. Con la optoelectrónica es posible un diagnóstico rápido y seguro del paciente.

Industria

En la automatización y el control industriales, la optoelectrónica desempeña un papel importante como sensores, transductores de medición y actuadores en sistemas de control. Los sensores optoelectrónicos controlan los parámetros de producción, el estado de la máquina y la posición de los componentes. Permiten racionalizar y automatizar los procesos industriales.

Entretenimiento

En la industria del entretenimiento se utiliza, entre otras cosas, la optoelectrónica. en sistemas de iluminación escénica, proyectores multimedia o entretenimiento virtual. Permite una iluminación y unos efectos visuales espectaculares, aumentando el atractivo de los eventos.

Avances tecnológicos en optoelectrónica

Los nuevos materiales y tecnologías, como la electrónica flexible, están creando nuevas oportunidades para la optoelectrónica. Su aplicación en inteligencia artificial permite construir sistemas sensoriales y de visión avanzados. La optoelectrónica está impulsando el progreso en muchos ámbitos.

En resumen, la optoelectrónica es un campo extremadamente versátil y en rápido desarrollo que encuentra cada vez nuevas aplicaciones gracias a los avances tecnológicos. Su papel crecerá con la demanda de comunicaciones rápidas y fiables, sistemas sensoriales avanzados o iluminación energéticamente eficiente.

2.6. AMPLIFICADORES Y FUENTES DE ALIMENTACIÓN

2.6.1. AMPLIFICADORES:

Dispositivos que aumentan la amplitud de una señal. Se clasifican en clases A, B, AB y C según su eficiencia y fidelidad.

Clasificación de los amplificadores

La primera clasificación que podemos hacer con los amplificadores viene determinada por las frecuencias con las que van a trabajar.

Si las frecuencias están comprendidas dentro de la banda audible, los amplificadores reciben el nombre de amplificadores de audio frecuencia o amplificadores de Baja frecuencia. (amplificadores A.F. o amplificadores B.F., respectivamente).

En el tema anterior veíamos que en las transmisiones vamos a utilizar otros amplificadores que trabajan con la gama alta de frecuencias, las radiofrecuencias (amplificadores de R.F.). Dentro de las dos gamas de amplificadores vistas, también, podemos hacer una clasificación atendiendo a su forma de trabajo:

A. **Amplificadores de tensión:** son los que su principal misión es suministrar una tensión mayor en su salida que en su entrada
B. **Amplificadores de potencia:** aquellos que, aparte de suministrar una mayor tensión, suministran también un mayor corriente (amplificación de tensión y amplificación de corriente y, por ende, amplificación de potencia).

Podemos, según esto, tener: amplificadores de tensión (tanto para B.F. como para R.F.) y amplificadores de potencia (también, para ambas gamas de frecuencias).

En este tema únicamente vamos a entrar en los amplificadores de potencia, que son los que nos interesan para iniciar el campo de las R.F., el resto los damos por estudiados y aprendidos (porque son los montajes de amplificadores que se estudian en los principios básicos).

Clases de amplificadores de potencia

Tal y como decíamos en el punto anterior, este tipo de amplificadores (amplificadores de potencia, ya sean para B.F. o para R.F.), tienen la particularidad de que en su salida tenemos ganancia de tensión y de corriente con respecto a la señal de entrada.

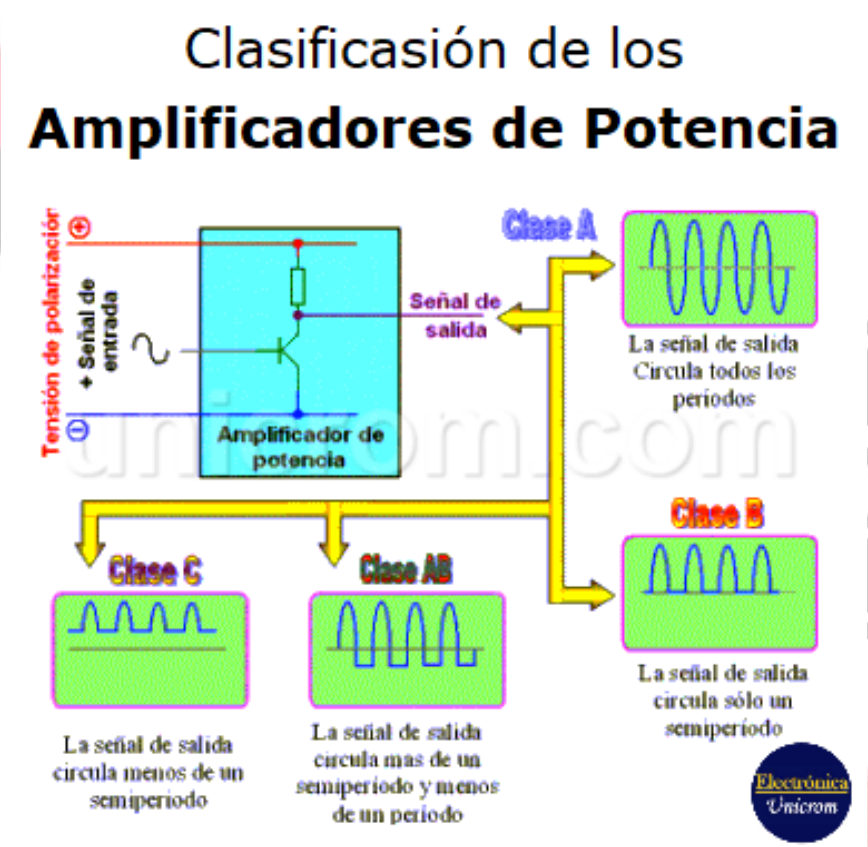
Este tipo de amplificadores pueden entregarnos en su salida toda la señal de entrada o una parte de la misma; atendiendo a esta característica, los amplificadores de potencia, podemos clasificarlos de la siguiente forma:

- **Amplificadores de potencia clase A:** un amplificador de potencia funciona en clase A cuando la tensión de polarización y la amplitud máxima de la señal de entrada poseen valores tales que hacen que la corriente de salida circule durante todo el período de la señal de entrada.
- **Amplificadores de potencia clase B:** un amplificador de potencia funciona en clase B cuando la tensión de polarización y la amplitud máxima de la señal de entrada poseen valores tales que hacen que la corriente de salida circule durante un semiperíodo de la señal de entrada.

- **Amplificadores de potencia clase AB:** son, por así decirlo, una mezcla de los dos anteriores, un amplificador de potencia funciona en clase AB cuando la tensión de polarización y la amplitud máxima de la señal de entrada poseen valores tales que hacen que la corriente de salida circule durante menos de un período y más de un semiperíodo de la señal de entrada.
- **Amplificadores de potencia clase C:** un amplificador de potencia funciona en clase C cuando la tensión de polarización y la amplitud máxima de la señal de entrada poseen valores tales que hacen que la corriente de salida circule durante menos de un semiperíodo de la señal de entrada.

En los **amplificadores de clase A** no hay nunca corriente de reja (base) por lo que es indiferente decir que el amplificador es de clase A1 o de clase A. Lo contrario ocurre en los amplificadores de clase C donde siempre va a existir corriente de reja (base), en este caso es indiferente decir que el amplificador es de clase C2 o de clase C (a secas).

En los **amplificadores de clase B y AB**, puede que exista o no la corriente de base (o reja) por lo que sí es importante que nos especifiquen el tipo de amplificador del que se trata (AB1 diría que no tiene corriente de base y B2 indicaría que sí hay corriente de base). Este tipo de notación también podemos encontrarla en los amplificadores transistorizados



2.6.2. FUENTES DE ALIMENTACIÓN:

Proporcionan la energía eléctrica necesaria para el funcionamiento de los circuitos. Pueden ser lineales o conmutadas.

¿Qué tipos de fuente de alimentación eléctrica existen?

Existen cuatro tipos diferentes de fuentes de alimentación, cada una de ellas responde a las necesidades de diferentes redes y dispositivos.

- **Fuente de alimentación AC/DC**: es la fuente de alimentación utilizada en la mayoría de los dispositivos que utilizamos diaramente, como los cargadores de los teléfonos móviles. La fuente de alimentación convierte la corriente alterna de la red en corriente continua y ajusta la tensión a las necesidades del dispositivo.

- **Fuente de alimentación DC/DC:** es la fuente de alimentación utilizada en electrónica. Cambia la tensión de la corriente y puede, si es necesario, cambiar la forma de onda.

- **Fuente de alimentación AC/AC:**se utiliza en aplicaciones muy específicas, como en algunos amplificadores de audio. Permite reducir la tensión de red.

- **Fuente de alimentación de laboratorio**: permite alterar los diferentes parámetros de corriente eléctrica para testar los equipos eléctricos.

¿Fuente de alimentación lineal o conmutada?

Las fuentes de alimentación pueden dividirse en dos tipos, de acuerdo con la tecnología utilizada:

- Fuente de alimentación lineal
- Fuente de alimentación conmutada

Fuente de alimentación lineal

Este tipo de fuente de alimentación proporciona una o varias tensiones continuas estabilizadas y constantes, independientemente de las variaciones de tensión de la red.

Una fuente de alimentación lineal consta de un transformador, un rectificador, un filtro y un regulador.

El transformador reduce el nivel de tensión de la red, el rectificador convierte la tensión alterna en tensión continua, el filtro almacena energía para dejar la tensión de salida del rectificador lo más continua posible y, por último, el regulador estabiliza y regula la tensión de salida

Una fuente de alimentación lineal puede suministrar desde unos pocos vatios hasta varios cientos de vatios.

- Aplicaciones: este tipo de fuente de alimentación es adecuada para equipos de audio y para fuentes de alimentación de laboratorio.
- Ventajas: es fácil de instalar, ofrece una buena estabilidad y presenta buena resistencia térmica.
- Inconvenientes: presenta un nivel bajo de eficiencia y genera pérdidas de energía. Además, la fuente de alimentación lineal es voluminosa y pesada.

Fuente de alimentación conmutada

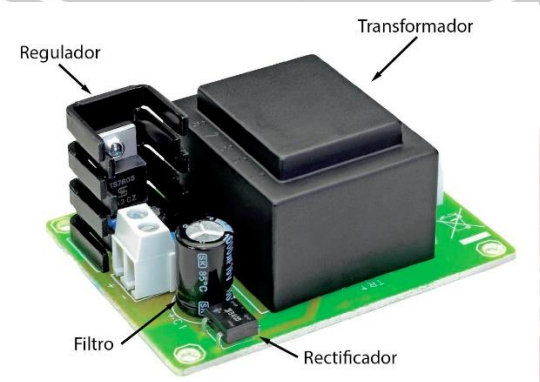
En este tipo de fuentes de alimentación, la regulación eléctrica es efectuada por los componentes electrónicos de potencia, como los transistores, utilizados en la conmutación. A diferencia de las fuentes lineales, las fuentes conmutadas transmiten la potencia de manera instantánea.

Las fuentes de alimentación conmutadas se han desarrollado considerablemente desde la década de 1980 como alternativa a las fuentes de alimentación lineales, que presentan dos desventajas principales, el peso elevado y la baja eficiencia

- **Aplicaciones**: este tipo de fuente de alimentación es adecuada para dispositivos electrónicos comunes, como ordenadores, televisores, cargadores de teléfonos móviles, etc.
- **Ventajas**: presenta una eficiencia muy elevada. Como funciona con un transformador bastante pequeño, es más ligero y menos voluminoso que una fuente lineal.
- **Inconvenientes**: este tipo de alimentación genera ruido armónico y ondas residuales.

¿Cuáles son los diferentes componentes de una fuente de alimentación?

La función de una fuente de alimentación es suministrar una tensión estable independientemente del valor de la corriente de entrada. Esa función es realizada por diferentes componentes de la fuente:



Transformador: Es el encargado de adaptar los niveles de tensión entre el primario y el secundario, además de proporcionar aislamiento galvánico entre estas dos zonas.

Rectificador: Está compuesto por 4 diodos (pueden ir separados o encapsulados en un mismo elemento), la función de este rectificador es la de convertir la corriente alterna que sale del transformador en una corriente pulsante.

Filtro: El filtro está constituido por uno o varios condensadores (normalmente condensadores polarizados), cuya función es la de suavizar el rizado de la señal que sale del rectificador, quedando una señal prácticamente continua.

Regulador de tensión: En la etapa final se colocará un elemento que asegure que la tensión a la salida va a ser siempre constante, y que no va a superar el valor de tensión para el que ha sido diseñado, esto puede conseguirse de varias maneras, podría colocarse un diodo zener polarizado en inversa que limite dicha tensión a la salida, pero lo más común es colocar un circuito integrado comercial en cuyo interior tenemos integrados tanto elementos de protección como de regulación de la tensión (según sea el modelo). Este regulador no es más que un sistema de control en lazo cerrado o realimentado, que ajustará una especie de resistencia interna variable para dar siempre una salida constante. Debido a la forma de trabajar de este integrado, parte de la potencia que suministra la disipará en forma de calor, esto hace que este tipo de fuentes sea menos eficiente que las fuentes de alimentación conmutadas, además de tener que colocar a dicho integrado un disipador para que no alcance temperaturas excesivas que dañarían al propio integrado.

2.7. APLICACIONES ELECTRÓNICAS EN TELECOMUNICACIONES Y REDES

La electrónica desempeña un papel fundamental en el desarrollo y funcionamiento de los sistemas de telecomunicaciones y redes, permitiendo la transmisión, procesamiento y seguridad de la información. A continuación, se detallan algunas de sus principales aplicaciones:

2.7.1. SISTEMAS DE TRANSMISIÓN Y RECEPCIÓN DE SEÑALES

Los sistemas de telecomunicaciones dependen de circuitos electrónicos para la transmisión y recepción de señales de audio, video y datos. Estos sistemas incluyen:

- **Transmisores**: Convierte información en señales eléctricas o electromagnéticas que pueden viajar a través de diferentes medios (cables, fibra óptica, radiofrecuencia).
- **Receptores**: Captan y procesan las señales transmitidas, recuperando la información original.

- **Amplificadores**: Aumentan la intensidad de la señal para evitar pérdidas de calidad.
- **Filtros**: Eliminan interferencias y ruidos no deseados en la señal.

Ejemplos de aplicaciones incluyen la radiodifusión, televisión digital, comunicaciones satelitales y redes de telefonía móvil.

2.7.2. ELECTRÓNICA EN REDES DE DATOS Y COMUNICACIÓN INALÁMBRICA

La infraestructura de redes de comunicación se basa en dispositivos electrónicos que facilitan la conectividad entre computadoras y otros dispositivos. Estos incluyen:

- **Routers y switches**: Administran el tráfico de datos en redes locales e internet.
- **Módems y adaptadores de red**: Permiten la conexión a redes de telecomunicaciones, ya sea mediante cables o de forma inalámbrica.
- **Wi-Fi y Bluetooth**: Tecnologías inalámbricas basadas en electrónica de radiofrecuencia que permiten la comunicación entre dispositivos sin necesidad de cables.
- **Sistemas de fibra óptica**: Utilizan pulsos de luz controlados por circuitos electrónicos para transmitir datos a altas velocidades con baja latencia.

Estas tecnologías permiten la existencia de redes de internet, redes móviles (4G, 5G) y sistemas de comunicación IoT (Internet de las Cosas).

2.7.3. SISTEMAS DE MODULACIÓN Y DEMODULACIÓN DE SEÑALES

Para transmitir señales de manera eficiente, es necesario convertir la información en formas que puedan viajar a través de los medios de comunicación. Los sistemas electrónicos de modulación y demodulación permiten esta conversión:

- **Modulación**: Es el proceso de alterar una señal portadora para transportar información. Existen diferentes tipos, como:
    - **AM (Amplitud Modulada)** y **FM (Frecuencia Modulada)** en radiocomunicaciones.
    - **Modulación digital** como ASK, FSK y PSK para transmisión de datos en redes.
- **Demodulación**: Es el proceso inverso, en el que se recupera la información original a partir de la señal modulada.

Estos sistemas son esenciales en radio, televisión, telefonía móvil y redes de datos, ya que permiten la transmisión eficiente y robusta de información sobre distintos medios.

2.7.4. SEGURIDAD Y PROTECCIÓN EN REDES ELECTRÓNICAS

La seguridad en redes de telecomunicaciones es un aspecto crucial para evitar accesos no autorizados, ataques cibernéticos y pérdida de información. La electrónica juega un papel clave en la protección de datos a través de:

- **Cifrado de señales y datos**: Técnicas electrónicas como la encriptación aseguran la privacidad de la información transmitida.
- **Firewalls y sistemas de detección de intrusos (IDS/IPS)**: Dispositivos electrónicos especializados en filtrar tráfico no deseado y detectar amenazas en redes.
- **Autenticación y control de acceso**: Uso de tecnologías como tarjetas RFID, biometría y protocolos de autenticación para verificar identidades.
- **Protección contra interferencias electromagnéticas (EMI)**: Uso de filtros y blindajes electrónicos para evitar que señales externas afecten la transmisión de datos.

Estos sistemas garantizan comunicaciones seguras en redes empresariales, telecomunicaciones móviles y transacciones financieras, entre otras aplicaciones críticas.

Conclusión

Las aplicaciones electrónicas en telecomunicaciones y redes han revolucionado la forma en que nos comunicamos y compartimos información. Desde la transmisión de señales hasta la seguridad de los datos, la electrónica es la base de los sistemas modernos de comunicación, permitiendo conexiones más rápidas, confiables y seguras en un mundo cada vez más digitalizado.

3. CIRCUITOS ELECTRÓNICOS ANALÓGICOS

3.1. ANÁLISIS DE CIRCUITOS CON RESISTENCIAS, CONDENSADORES E INDUCTANCIAS

3.1.1. CONCEPTOS BÁSICOS DE RESISTENCIA, CAPACITANCIA E INDUCTANCIA

Los componentes pasivos fundamentales en los circuitos electrónicos analógicos son las resistencias, condensadores e inductores. Cada uno cumple una función específica:

- **Resistencias**: Limitan la cantidad de corriente que fluye en un circuito, disipando energía en forma de calor.
- **Condensadores**: Almacenan y liberan energía en forma de campo eléctrico, permitiendo el filtrado de señales y la estabilización del voltaje.
- **Inductores**: Generan un campo magnético cuando circula corriente a través de ellos y se usan en filtros, conversión de energía y osciladores.

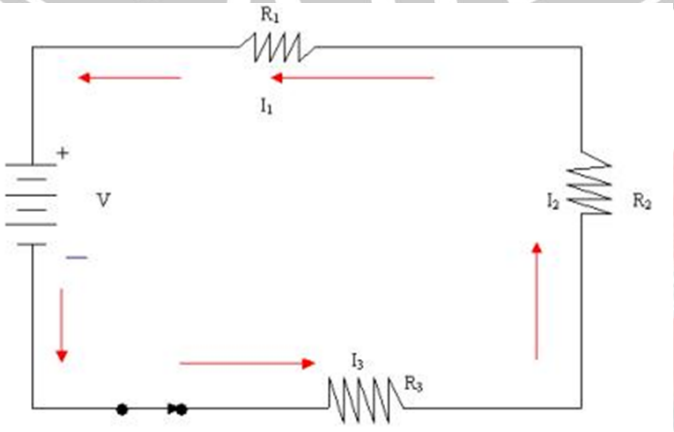
3.1.2. ASOCIACIÓN DE RESISTENCIAS EN SERIE Y PARALELO

Las resistencias pueden asociarse de dos maneras principales:

3.1.2.1. CIRCUITOS EN SERIE

En este tipo de circuito, los componentes están conectados secuencialmente, uno tras otro, formando una única trayectoria para la corriente eléctrica. La corriente que fluye es la misma a través de todos los componentes, pero el voltaje se divide entre ellos. Una desventaja es que, si un componente falla o se desconecta, la corriente se interrumpe y todos los demás componentes dejan de funcionar.

En el caso concreto de solo arreglos de resistencias la corriente eléctrica es la misma en todos los puntos del circuito. Ver la siguiente imagen.



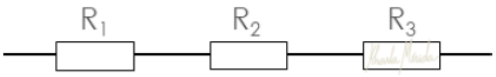
$$I_1 = I_2 = I_3 = \cdots = I$$
$$V = V_1 + V_2 + V_3 + \cdots + V_n$$
$$R = R_1 + R_2 + R_3 + \cdots + R_n$$

donde I la corriente de la fuente
V el voltaje de la fuente
R es la resistenci a total
R_i la resistenci a i
V_i de la resistenci a R_i

Circuitos en serie

La resistencia total es la suma de las resistencias.

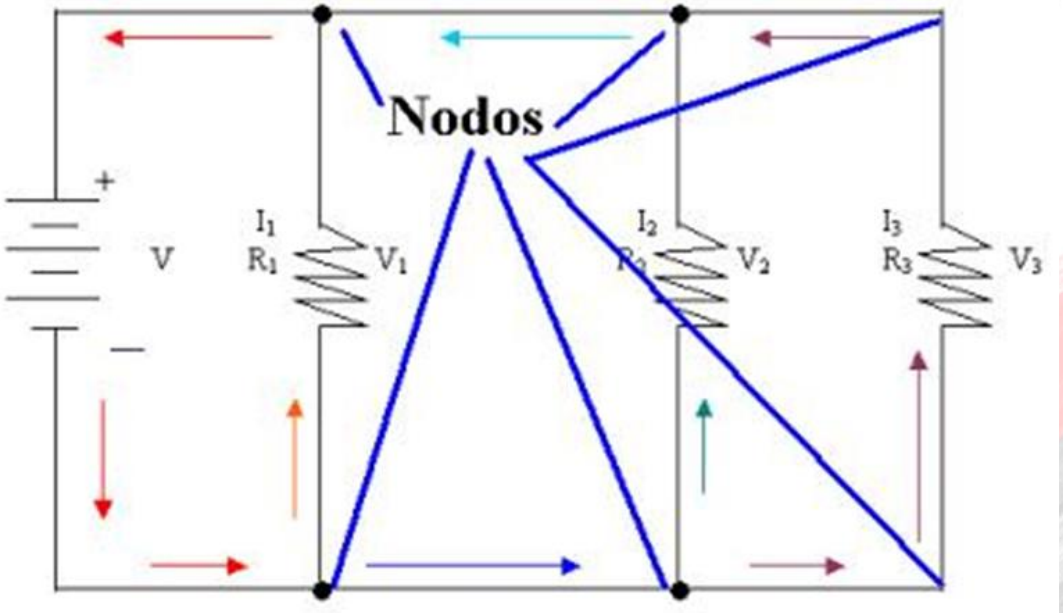
$$R_T = R_1 + R_2 + R_3$$



3.1.2.2. CIRCUITOS EN PARALELO.

En este circuito, los componentes están conectados de manera que cada uno tiene su propia ruta independiente hacia la fuente de energía. El voltaje a través de cada componente es el mismo, pero la corriente se divide entre las diferentes ramas. Una ventaja es que, si un componente falla, los demás pueden seguir funcionando sin interrupción.

Su característica más importante es el hecho de que el potencial en cada elemento del circuito tiene la misma diferencia de potencia



Donde, en general :

$$V_1 = V_2 = V_3 = \cdots = V$$

$$I = I_1 + I_2 + I_3 + \cdots + I_n$$

$$R = \frac{1}{\frac{1}{R_1} + \frac{1}{R_2} + \frac{1}{R_3} \ldots + \frac{1}{R_n}}$$

donde I la corriente de la fuente

V el voltaje de la fuente

R es la resistenci a total

R_i la resistenci a i

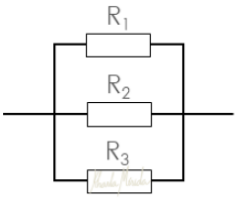
V_i de la resistenci a R_i

I_i la corriente i de la resistenci a R_i

Circuitos en paralelo

El inverso de la resistencia total es la suma de los inversos de las resistencias.

$$\frac{1}{R_T} = \frac{1}{R_1} + \frac{1}{R_2} + \frac{1}{R_3}$$



3.1.3. ASOCIACIÓN DE CONDENSADORES Y SU EFECTO EN CIRCUITOS ELÉCTRICOS

Hay dos tipos de conexión típicos entre condensadores y son: **Condensadores en serie** y **Condensadores en paralelo.** También se pueden hacer conexiones que involucren conexiones serie y paralelo simultáneamente, lo que llamaríamos conexiones mixtas de condensadores.

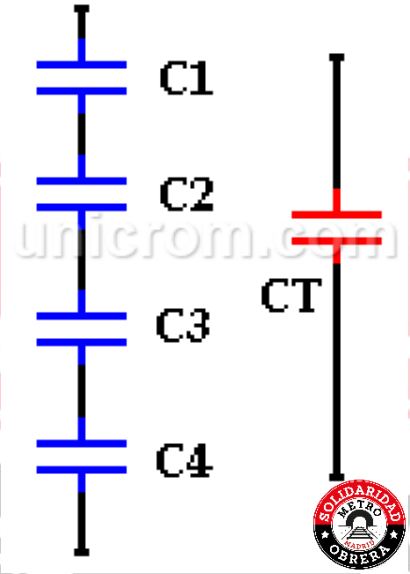
3.1.3.1. Condensadores en serie

Los capacitores o condensadores conectados uno después del otro, están conectados en serie. Estos condensadores se pueden reemplazar por un único condensador equivalente que tendrá un valor que será el equivalente de los que están conectados en serie.

Para obtener el valor de este único condensador equivalente se utiliza la fórmula (para 4 condensadores):

1/Ceq = 1/C1 + 1/C2 + 1/C3 + 1/C4

Ceq = (C1 x C2 x C3 x C4) / (C1 + C2 + C3 + C4)



Pero fácilmente se puede hacer un cálculo para cualquier número de condensadores que se conecten en serie con ayuda de la siguiente fórmula:

1/Ceq = 1/C1 + 1/C2 + ….+ 1/CN o

Ceq = (C1 x C2 x … x CN) / (C1 + C2 + … + CN)

Donde N es el número de condensadores que están conectados en serie. En el gráfico hay 4 condensadores en serie. Esta operación se hace de manera similar al proceso de sacar el resistor equivalente de un grupo de resistencias en paralelo.

Ejemplo:

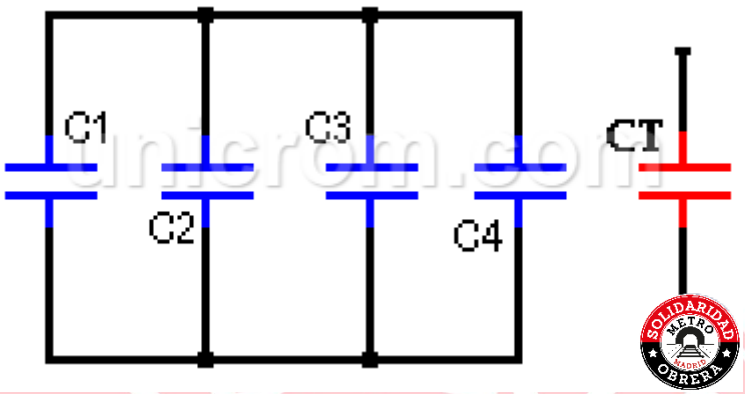
Si tengo 2 condensadores colocados en paralelo, C1 = 470 uF, C2 = 100 uF. ¿Cuál el condensador equivalente?

Usando la fórmula: **Ceq = (C1 x C2) / (C1 + C2)**

Ceq = (470 uF x 100 uF) / (470 uF + 100 uF) = 47000 / 570 = 82.456 uF

3.1.3.2. Condensadores en paralelo

Del gráfico se puede ver 4 condensadores si conectados en paralelo (los terminales de cada lado de los elementos están conectadas a un mismo punto).



Para encontrar el valor del condensador equivalente se utiliza la fórmula:

CT = C1 + C2 + C3 + C4

Fácilmente, se puede hacer un cálculo para cualquier número de condensadores con ayuda de la siguiente fórmula:

Ceq = C1 + C2 + …+ CN

Donde **N** es el número de condensadores conectados en paralelo. Como se ve, para obtener el condensador equivalente de condensadores en paralelo, solo basta con sumarlos. Esta operación se hace de manera similar al proceso de sacar el resistor equivalente de un grupo de resistencias en serie.

Ejemplo:

Sí tengo 3 condensadores colocados en paralelo,

C1 = 470 uF, C2 = 1000 uF y C3 = 100 uF.

¿Cuál el condensador equivalente?

Usando la fórmula: **Ceq = C1 + C2 + C3**.

Ceq = 470 uF + 1000 uF + 100 uF = 1570 uF

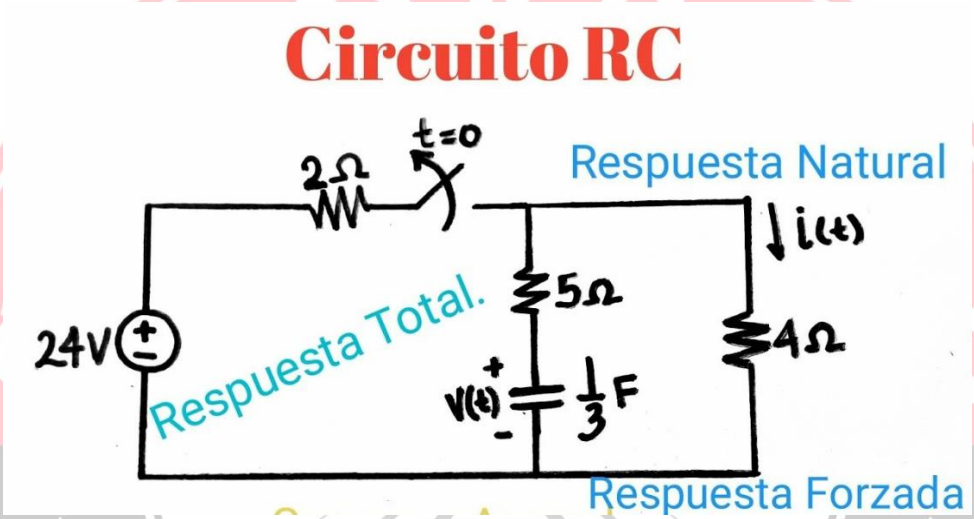
Nota: capacitor = condensador.

3.1.4. CIRCUITOS RC, RL, LC Y RLC: ANÁLISIS DE COMPORTAMIENTO EN CORRIENTE CONTINUA Y ALTERNA

Los circuitos que contienen resistencias, inductores y condensadores tienen comportamientos diferentes en corriente continua y alterna:

3.1.4.1. CIRCUITOS RC:

Un circuito RC es un circuito eléctrico compuesto de resistencias y condensadores. La forma más simple de circuito RC es el circuito RC de primer orden, compuesto por una resistencia y un condensador. Los circuitos RC pueden usarse para filtrar una señal alterna, al bloquear ciertas frecuencias y dejar pasar otras.



CIRCUITO RC EN SERIE

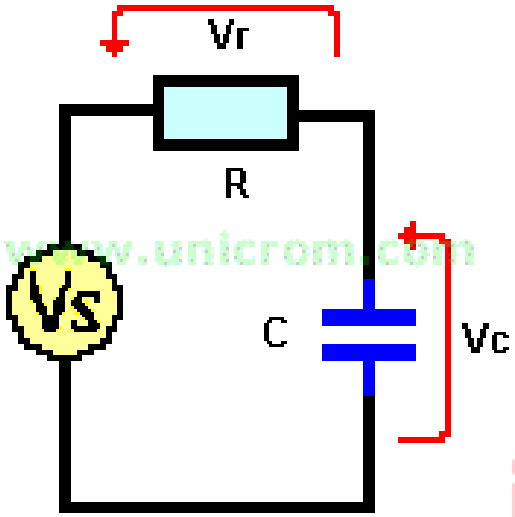
Un circuito RC es un circuito eléctrico compuesto de resistencias y condensadores. La forma más simple de circuito RC es el circuito RC de primer orden, compuesto por una resistencia y un condensador. Los circuitos RC pueden usarse para filtrar una señal alterna, al bloquear ciertas frecuencias y dejar pasar otras.

El voltaje entregado **VS** es igual a la suma fasorial de la caída de voltaje en el resistor **(Vr)** y de la caída de voltaje en el capacitor (**Vc**).

Ver la siguiente fórmula:

Vs = Vr + Vc (suma fasorial)

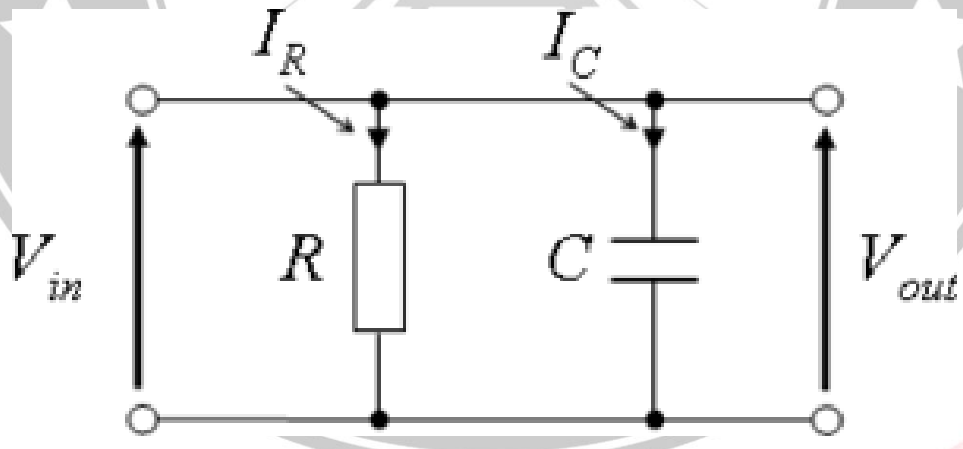
Esto significa que cuando la corriente está en su punto más alto (corriente pico), será así tanto en el resistor como en el capacitor. Pero algo diferente pasa con los voltajes. En el resistor, el voltaje y la corriente están en fase (sus valores máximos y mínimos coinciden en el tiempo). Pero el voltaje en el capacitor no es así



CIRCUITO RC EN PARALELO

En un **circuito RC paralelo en AC,** el valor del voltaje es el mismo en el condensador y en la resistencia. La corriente (corriente alterna) que la fuente entrega al circuito se divide entre la resistencia y el condensador. **(It = Ir + Ic).**

La corriente que pasa por la resistencia y la tensión que hay en ella están en fase debido a que la resistencia no causa desfase. La corriente en el capacitor / condensador está adelantada con respecto a la tensión (voltaje), que es igual que decir que el voltaje está retrasado con respecto a la corriente.



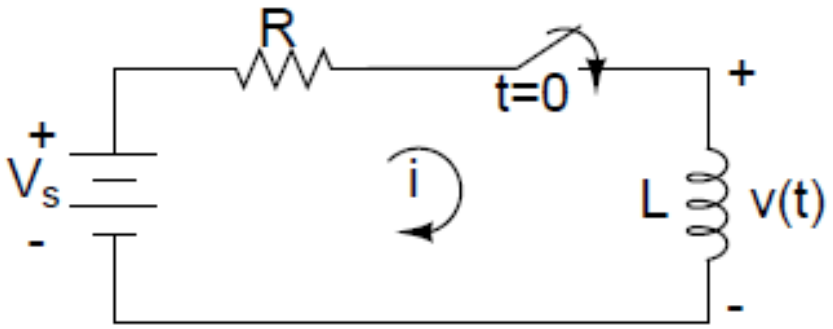
3.1.4.2. CIRCUITO RL

¿Que es un circuito RL?

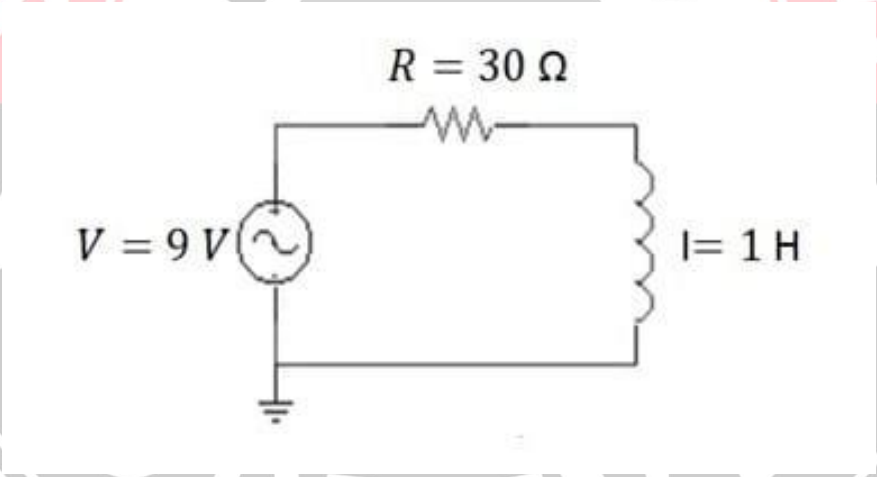
Son aquellos circuitos que poseen una resistencia (R), un inductor o bobina como solenoide (L) y un ferm (fuerza motriz) o fuente de voltaje. ahora a medida que la corriente avanza por el circuito, el inductor se comienza a cargar y comienza a generar

una corriente eléctrica en el sentido opuesto. En partículas en este tipo de circuitos, no existen cambios bruscos de corriente.

Un circuito RL, se tiene una resistencia y una bobina en serie, La corriente en ambos elementos es la misma, la tensión en la bobina esta en fase con la corriente que pasa por ella, pero el voltaje en la bobina esta adelantado a la corriente que pasas por ella en 90° (ejemplo de circuito en serie).



CIRCUITO RL EN PARALELO



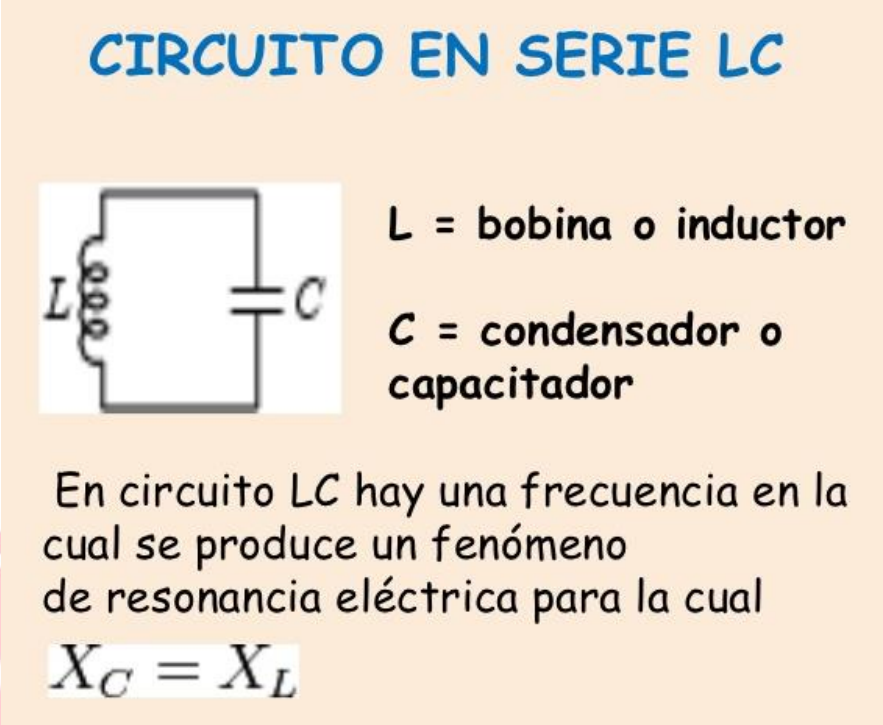
En un circuito RL Paralelo el valor del voltaje es el mismo para la resistencia y para la bobina. (ver imagen)

La corriente que pasa por la resistencia esta en fase con el voltaje aplicado, en cambio en la bobina la corriente se atrasa 90° con respecto al voltaje.

Su fórmula es:

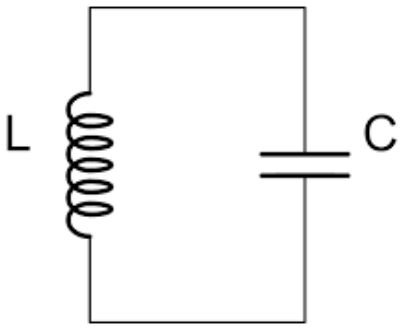
V= VR= VL

3.1.4.3. CIRCUITO LC



Es un circuito eléctrico formado por una bobina representada por la letra L y un condensador eléctrico representado por la letra C, los cuales se encuentran conectadas entre si. el circuito actúa como un resonador eléctrico, como una analogía eléctrica un diapasón, basados en el almacenamiento de energía oscilante a la frecuencia de resonancia del circuito

CIRCUITO LC EN PARALELO



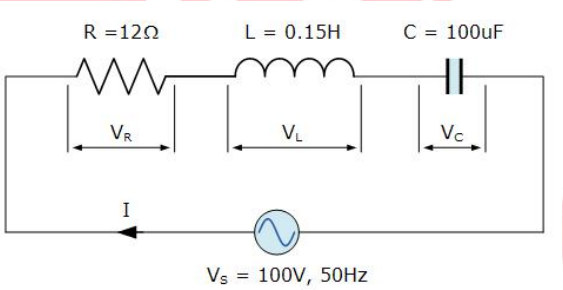
Al estar el condensador y la bobina en paralelo, la energía almacenada por el campo eléctrico del condensador (en forma de cargas electrostáticas), es absorbida por la bobina, que la almacena en su campo magnético, pero a continuación es absorbida y almacenada por el condensador; nuevamente en forma de campo eléctrico; para ser nuevamente absorbida por la bobina, y así sucesivamente. Esto crea un vaivén de la corriente (cargas eléctricas) entre el condensador y la bobina. Este vaivén constituye una oscilación electromagnética, en la cual el campo eléctrico y el magnético son perpendiculares entre sí, que cuando el campo magnético de la bobina está en su punto máximo, el campo eléctrico almacenado en el condensador es cero, y que cuando el campo eléctrico en el condensador es máximo, no existe campo magnético en la bobina.

3.1.4.4. CIRCUITO RLC

En electrodinámica, un **circuito RLC** es un circuito lineal que contiene una resistencia eléctrica, una bobina y un capacitor.

Existen dos tipos de circuitos RLC, en *serie* o en *paralelo*, según la interconexión de los tres tipos de componentes. El comportamiento de un circuito RLC se describe generalmente por una ecuación diferencial de segundo orden (en donde los circuitos RC o RL se comportan como circuitos de primer orden).

CIRCUITO RLC EN SERIE

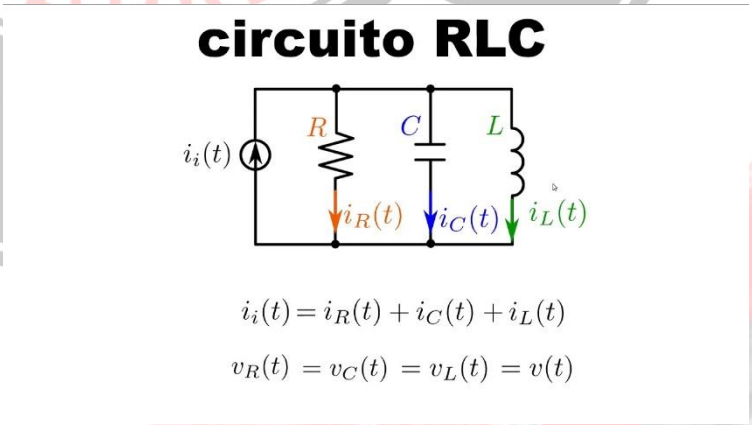


Se tiene un circuito compuesto por un capacitor C, una inductancia y una resistencia conectadas en serie a un generador de funciones.

Un circuito en serie RLC que contiene una resistencia de 12Ω , una inductancia de 0,15H y un condensador de 100uF están conectados en serie a través de una 100V, 50Hz. Calcular la impedancia total del circuito, la corriente de los circuitos, factor de potencia y dibujar el diagrama de fasores de tensión.

CIRCUITO RLC EN PARALELO

En un circuito que presenta los tres elementos conectados en paralelo, la tensión total aplicada el circuito es la misma que la que tenemos en bornes que cada elemento, mientras que la intensidad que circula para cada uno de ellos es distinta y depende de los efectos de la R, de la L y de la C.

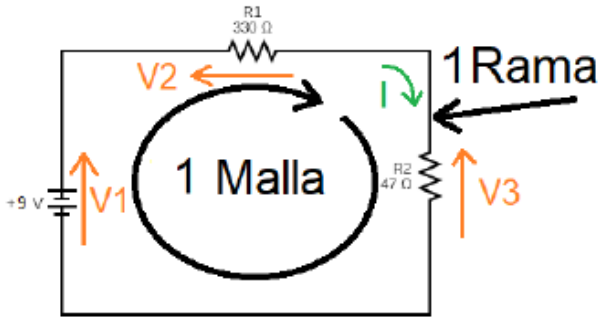


3.1.5. MÉTODOS DE ANÁLISIS DE CIRCUITOS: MALLAS Y NODOS.

Ramas, Mallas y Nodos

Rama
Es la parte del circuito que se encuentra entre dos nodos. Por todos los componentes de una rama circula la misma corriente.

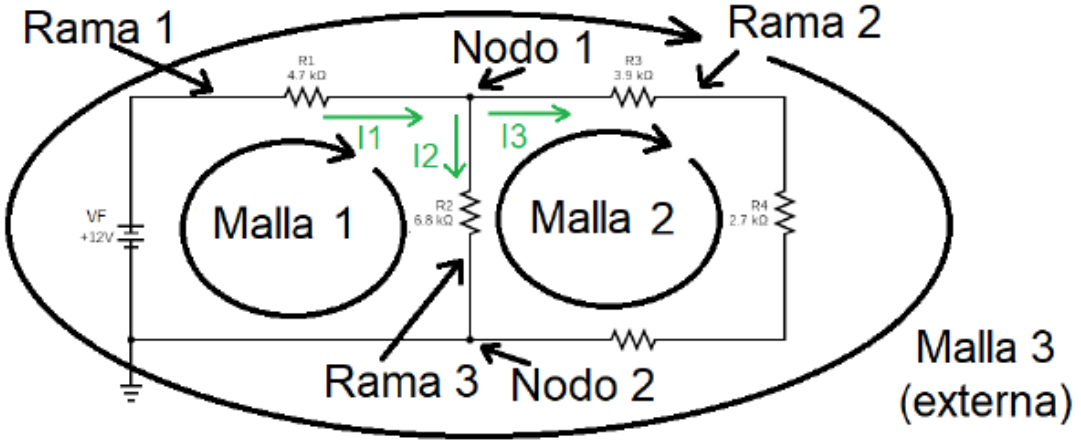
Malla
Es el camino cerrado que forman dos o más ramas de un circuito. En una malla la suma de todas las tensiones, cada una con su signo correspondiente, es igual a 0 (Ley de Kirchoff de las mallas). Esto ocurre porque la suma de todas las subidas de tensión debe ser igual a la suma de todas las caídas de tensión.



Dando la vuelta a la malla en el sentido indicado:

V1 – V2 – V3 = 0

Nodo
Es el punto de unión entre 3 o más ramas. La suma de las corrientes entrantes a un nodo debe ser igual a la suma de todas las corrientes salientes (Ley de Kirchoff de los nodos).



En el nodo 1 se cumple que

$$I1 = I2 + I3$$

Lo mismo se puede plantear en el nodo 2, sin embargo, con escribirlo una vez alcanza. En general, hay que escribir una ecuación de nodo menos que el número de nodos.

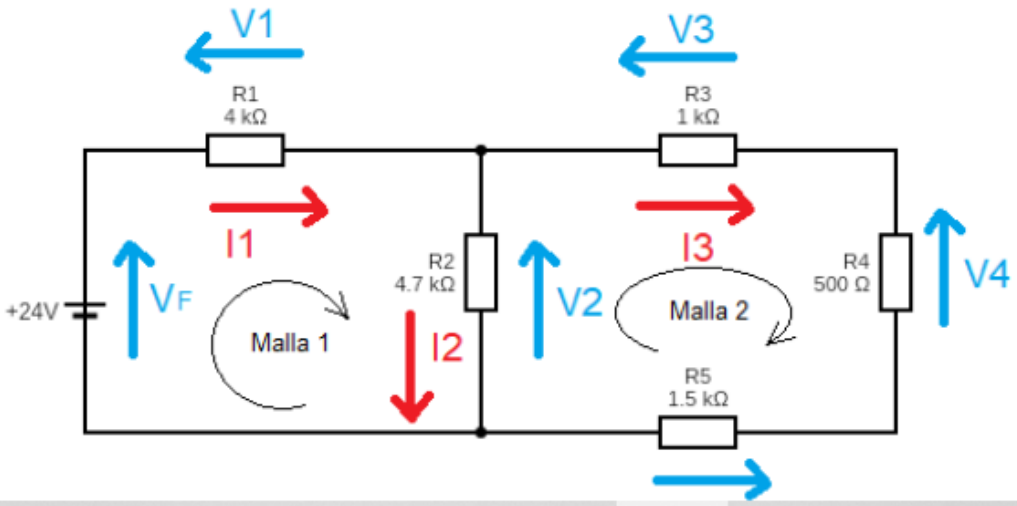
El objetivo de plantear las ecuaciones de mallas y nodos es el de tener un sistema de ecuaciones que permita encontrar todas las corrientes y tensiones.

Procedimiento para el cálculo de corrientes y tensiones

1) Dibujar el circuito
2) Ponerle las flechitas de tensiones y corrientes con sus respectivos nombres. El sentido de las corrientes y tensiones es arbitrario. Es importante mantener ese sentido hasta el final, sin cambiarlo en el medio del procedimiento. Si al terminar todos los cálculos alguna tensión o corriente dio negativa, significa que el sentido es el opuesto al dibujado.
3) Plantear, en cada nodo, las ecuaciones de los nodos.
4) Elegir un sentido de circulación de la malla y plantear, en cada malla, las ecuaciones de mallas. Es conveniente dibujar el sentido de circulación.
5) Resolver el sistema de ecuaciones.

Ejemplo:

Hallar la tensión y la corriente en cada resistencia del siguiente circuito.



En la malla 1:

$$V_F = V1 + V2$$
$$V1 = I1 \,.\, R1$$
$$V2 = I2 \,.\, R2$$
$$V_F = I1 \,.\, R1 + I \,.\, R2 \qquad \textbf{Ecuación 1}$$

En la malla 2:

$$0 = V2 - V3 - V4 - V5$$
$$V2 = I2 \,.\, R2$$
$$V3 = I3.R3$$
$$V4 = I3 \,.\, R4$$
$$V5 = I3 \,.\, R5$$
$$0 = I2 \,.\, R2 - I3 \,.\, R3 - I3 \,.\, R4 - I3 \,.\, R5$$
$$0 = I2 \,.\, R2 - I3 \,.\, (R3 + R4 + R5) \qquad \textbf{Ecuación 2}$$

Luego de aplicar la primera ley de Kirchoff o, suma de tensiones en una malla, tenemos dos ecuaciones y tres incógnitas. Las incógnitas son I1, I2 e I3.

La tercera ecuación es la de suma de corrientes en un nodo o segunda ley de Kirchoff:

$$I1 - I2 - I3 = 0 \qquad \textbf{Ecuación 3}$$

Ahora que tenemos todas las ecuaciones. El sistema de 3 ecuaciones con 3 incógnitas es el formado por las ecuaciones 1, 2 y 3. Para resolverlo, lo vamos a transformar en un sistema de dos ecuaciones con dos incógnitas al eliminar la corriente I2. Entonces, luego de despejar la Ecuación 3, reemplazamos I2 en las ecuaciones 1 y 2:

De la ecuación 3:

$$I2 = I1 - I3$$

Reemplazando en la Ecuación 1:

$$V_F = I1 \,.\, R1 + (I1 - I3) \,.\, R2$$
$$V_F = I1 \,.\, (R1 + R2) - I3 \,.\, R2 \qquad \textbf{Ecuación 4}$$

Reemplazando en la Ecuación 2:

$$0 = (I1 - I3).R2 - I3 \,.\, (R3 + R4 + R5)$$
$$0 = I1 \,.\, R2 - I3 \,.\, (R2 + R3 + R4 + R5) \qquad \textbf{Ecuación 5}$$

Las ecuaciones 4 y 5 son un sistema de dos ecuaciones con dos incógnitas. Reemplazamos por los valores de los datos y lo resolvemos.

$$24\,V = I1\,.\,(4\,K\Omega + 4{,}7\,K\Omega) - I3\,.\,(4{,}7\,K\Omega)$$
$$24 = 8{,}7\,.\,I1 - 4{,}7\,.\,I3$$
$$0\,V = I1\,.\,4{,}7\,K\Omega - I3\,.\,(4{,}7\,K\Omega + 1\,K\Omega + 0{,}5\,K\Omega + 1{,}5\,K\Omega)$$
$$0 = 4{,}7\,.\,I1 - 7{,}7\,I3$$

Queda por resolver el siguiente sistema de dos ecuaciones con dos incógnitas:

$$24 = 8{,}7\,.\,I1 - 4{,}7\,.\,I3$$
$$0 = 4{,}7\,.\,I1 - 7{,}7\,I3$$

Podemos resolverlo por varios métodos: sustitución, igualación, sumas y restas, Cramer, Gauss, etc.

El resultado es:

$$I1 = 4{,}1\ mA$$
$$I3 = 2{,}5mA$$

Recordemos que I2 = I1 – I3

$$I2 = 1{,}6\ mA$$

Ahora que conocemos las corrientes, las tensiones en cada resistencia, las obtenemos aplicando la Ley de Ohm (V = I . R) y recordemos que mA . KΩ = V

Resistencia	R1	R2	R3	R4	R5
Corriente mA	4,1 mA	1,6 mA	2,5 mA	2,5 mA	2,5 mA
Tensión V	16,4 V	7,52 V	2,5 V	1,25 V	3,75 V

De este ejemplo podemos obtener una conclusión importante, que nos va a facilitar el planteo de ecuaciones, las que obtendremos por simple inspección del circuito.

Observemos las ecuaciones 4 y 5 y el circuito.

$$V_F = I1\,.\,(R1 + R2) - I3\,.\,R2 \qquad \textbf{Ecuación 4}$$
$$0 = I1\,.\,R2 - I3\,.\,(R2 + R3 + R4 + R5) \qquad \textbf{Ecuación 5}$$

En la ecuación 4 o ecuación de la malla 1:

Sólo hay una fuente de tensión (V_F). Va a la izquierda del signo =.

La corriente I1 pasa por las resistencias R1 y R2. Planteamos la ley de Ohm en el primer término: I1. (R1 + R2). Con signo positivo porque son caídas de tensión, de acuerdo a como circulamos por la malla.

La corriente I3 pasa por R2 en sentido contrario a I1. Planteamos la ley de Ohm en el segundo término: - I3 . R2. Con signo negativo por ser subidas de tensión, de acuerdo a como circulamos por la malla.

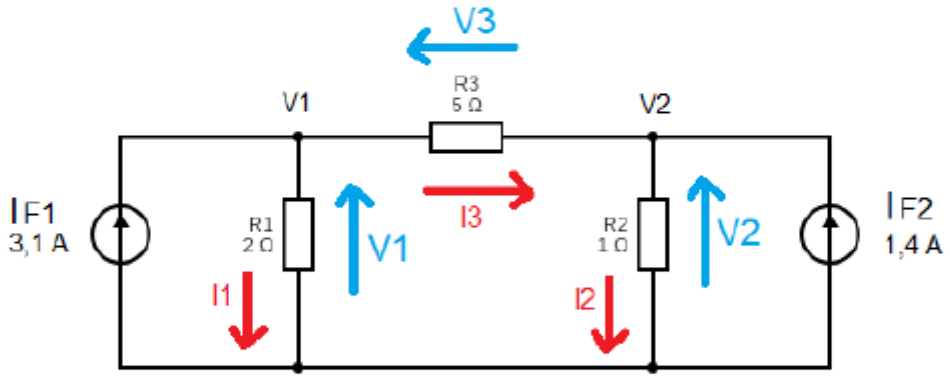
En la ecuación 5 o ecuación de la malla 2:

No hay fuentes de tensión. Ponemos 0 a la izquierda del signo =.

La corriente I3 pasa por las resistencias R2, R3, R4 y R5. Planteamos la ley de Ohm en el término de la derecha: I3 . (R2 + R3 + R4 + R5). Dado que de acuerdo a como circulamos por la malla, son caídas de tensión, lo escribimos con signo positivo.

La corriente I1 pasa por R2 y lo hace en sentido opuesto a I3. Planteamos la ley de Ohm en el primer término con signo opuesto al anterior por ser una subida de tensión: - I1 .R2

Ejemplo 2



En el nodo V1:

$$I_{F1} - I1 - I3 = 0$$

$$I1 = \frac{V1}{R1}$$

$$I3 = \frac{V3}{R3} = \frac{V1 - V2}{R3}$$

Reemplazando:

$$I_{F1} = V1 . \frac{1}{R1} + (V1 - V2) . \frac{1}{R3} = V1 . \left(\frac{1}{R1} + \frac{1}{R3}\right) - V2 . \frac{1}{R3}$$

En el nodo V2:

$$I_{F2} + I3 - I2 = 0$$

$$I3 = \frac{V1 - V2}{R3}$$

$$I2 = \frac{V2}{R2}$$

$$I_{F2} = V2 . \frac{1}{R2} - (V1 - V2) . \frac{1}{R3} = -V1 . \frac{1}{R3} + V2 . \left(\frac{1}{R2} + \frac{1}{R3}\right)$$

Reemplazando por los datos:

$$3{,}1\ A = V1 . \left(\frac{1}{2\Omega} + \frac{1}{5\Omega}\right) - V2 . \frac{1}{5\Omega}$$

$$1{,}4\ A = -V1 . \frac{1}{5\Omega} + V2 . \left(\frac{1}{1\Omega} + \frac{1}{5\Omega}\right)$$

Nos queda el siguiente sistema de dos ecuaciones con dos incógnitas:

$$3{,}1 = 0{,}7\ V1 - 0{,}2\ V2$$

$$1{,}4 = -0{,}2\ V1 + 1{,}2\ V2$$

La solución es:

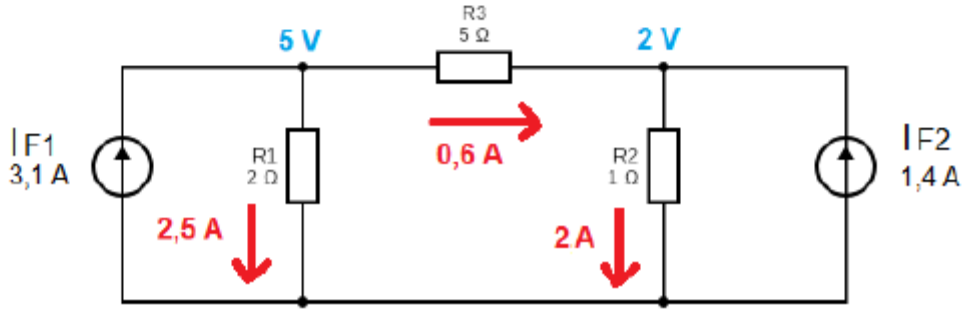
$$V1 = 5\ V$$

$$V2 = 2\ V$$

$$V3 = V1 - V2 = 3\ V$$

Las corrientes en cada resistencia las obtenemos por ley de Ohm.

Resistencia	R1	R2	R3
Corriente mA	2,5 A	2 A	0,6 A
Tensión V	5 V	2 V	3 V



4. MONTAJE Y MANTENIMIENTO DE EQUIPOS ELECTRÓNCOS

4.1. HERRAMIENTAS Y EQUIPOS PARA EL MONTAJE

4.1.1. HERRAMIENTAS MANUALES

- **Destornilladores de precisión**: Se utilizan para ensamblar o desmontar equipos electrónicos con tornillos pequeños.
- **Alicates de corte y de punta**: Facilitan la manipulación de componentes y el corte de cables o terminales.
- **Llaves y pinzas**: Para sujetar pequeños componentes sin dañarlos.
- **Cuchillas y bisturíes electrónicos**: Útiles para retirar recubrimientos o aislamientos.

4.1.2. HERRAMIENTAS ELÉCTRICAS

- **Estación de soldadura**: Esencial para la unión de componentes en circuitos impresos.

- **Desoldador**: Permite retirar soldadura y corregir errores en las conexiones.

- **Multímetro**: Mide voltaje, corriente y resistencia para comprobar el funcionamiento de circuitos.

- **Osciloscopio**: Analiza señales eléctricas en circuitos electrónicos.

- **Fuente de alimentación regulable**: Proporciona energía para realizar pruebas en los dispositivos ensamblados.

Un correcto uso de estas herramientas garantiza una instalación adecuada de los componentes electrónicos y evita daños por manipulación incorrecta.

4.2. SOLDADURA Y ENSAMBLAJE DE COMPONENTES

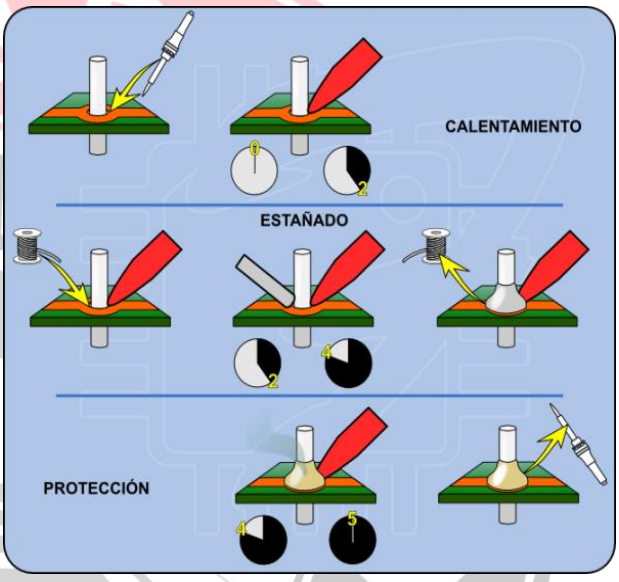
La soldadura es un proceso fundamental en el ensamblaje de equipos electrónicos, ya que permite la conexión eléctrica y mecánica entre componentes y placas de circuito impreso (PCB).

4.2.1. TIPOS DE SOLDADURA EN ELECTRÓNICA

1. **Soldadura blanda**: Utiliza estaño y plomo o aleaciones sin plomo.
2. **Soldadura en frío**: Se emplean conectores sin aplicación de calor.
3. **Soldadura por reflujo**: Técnica utilizada en ensamblajes automatizados con componentes de montaje superficial (SMD).
4. **Soldadura por ola**: Método industrial para soldar múltiples puntos en PCBs a la vez.

4.2.2. PROCESO DE SOLDADURA

1. **Preparación de la superficie**: Limpieza de los componentes y la PCB para garantizar una conexión óptima.
2. **Aplicación de fundente**: Ayuda a mejorar la adhesión de la soldadura.
3. **Uso del cautín**: Aplicación de calor adecuado para derretir la aleación de soldadura.
4. **Fijación del componente**: Soldadura del terminal al PCB sin aplicar calor excesivo.
5. **Verificación de la unión**: Inspección visual y uso de microscopios en caso de circuitos con alta densidad de componentes.



4.3. PROCEDIMIENTOS DE PRUEBA Y VERIFICACIÓN

Tras el montaje, los equipos electrónicos deben pasar por pruebas para asegurar que funcionan correctamente y cumplen con los requisitos de diseño.

4.3.1. MÉTODOS DE PRUEBA EN ELECTRÓNICA

1. **Pruebas de continuidad**: Uso de multímetros para verificar la conexión entre terminales.
2. **Pruebas de voltaje y corriente**: Comprobación de la alimentación y consumo de los circuitos.
3. **Pruebas funcionales**: Validación del rendimiento del equipo bajo condiciones normales de operación.

4. **Pruebas de estrés**: Evaluación del comportamiento del equipo en condiciones extremas de temperatura o carga.
5. **Análisis de señal**: Uso de osciloscopios y analizadores lógicos para examinar el comportamiento de las señales electrónicas.

El cumplimiento de estos procedimientos reduce fallos en la fabricación y montaje de equipos electrónicos.

4.4. DIAGNÓSTICO Y REPARACIÓN DE EQUIPOS ELECTRÓNICOS

Cuando un equipo electrónico presenta fallos, es necesario identificar la causa del problema y realizar las correcciones pertinentes.

4.4.1. TIPOS DE FALLOS EN EQUIPOS ELECTRÓNICOS

- **Fallos eléctricos**: Cortocircuitos, sobrecargas y fallos en la alimentación.
- **Fallos mecánicos**: Problemas en conectores, soldaduras frías o componentes dañados físicamente.
- **Fallos térmicos**: Sobrecalentamiento que afecta el funcionamiento de los componentes.
- **Fallos por obsolescencia**: Deterioro de componentes con el tiempo.

4.4.2. MÉTODOS DE DIAGNÓSTICO

- **Inspección visual**: Detección de soldaduras defectuosas, componentes quemados o conectores sueltos.
- **Medición con multímetro**: Verificación de continuidad, voltajes y resistencias.
- **Pruebas con osciloscopio**: Análisis del comportamiento de las señales electrónicas.
- **Sustitución de componentes**: Cambio de piezas defectuosas para comprobar si se soluciona el problema.

5. MONTAJE Y MANTENIMIENTO DE EQUIPOS MICROINFORMÁTICOS.

5.1. INTRODUCCIÓN A LOS SISTEMAS MICROINFORMÁTICOS

Los sistemas microinformáticos se han convertido en una parte esencial de la vida cotidiana y el mundo empresarial. Se refieren a conjuntos de equipos informáticos interconectados que pueden operar de manera independiente o en red para procesar datos, ejecutar programas y facilitar la comunicación entre usuarios.

Estos sistemas pueden incluir computadoras personales, servidores, dispositivos de almacenamiento y periféricos conectados a través de redes cableadas o inalámbricas. Su correcto montaje, mantenimiento y optimización garantizan un rendimiento eficiente y una vida útil prolongada de los dispositivos.

Los sistemas microinformáticos están compuestos por hardware (componentes físicos) y software (programas que permiten su funcionamiento). La integración y configuración adecuada de ambos elementos es fundamental para asegurar su correcto desempeño y evitar problemas técnicos a largo plazo.

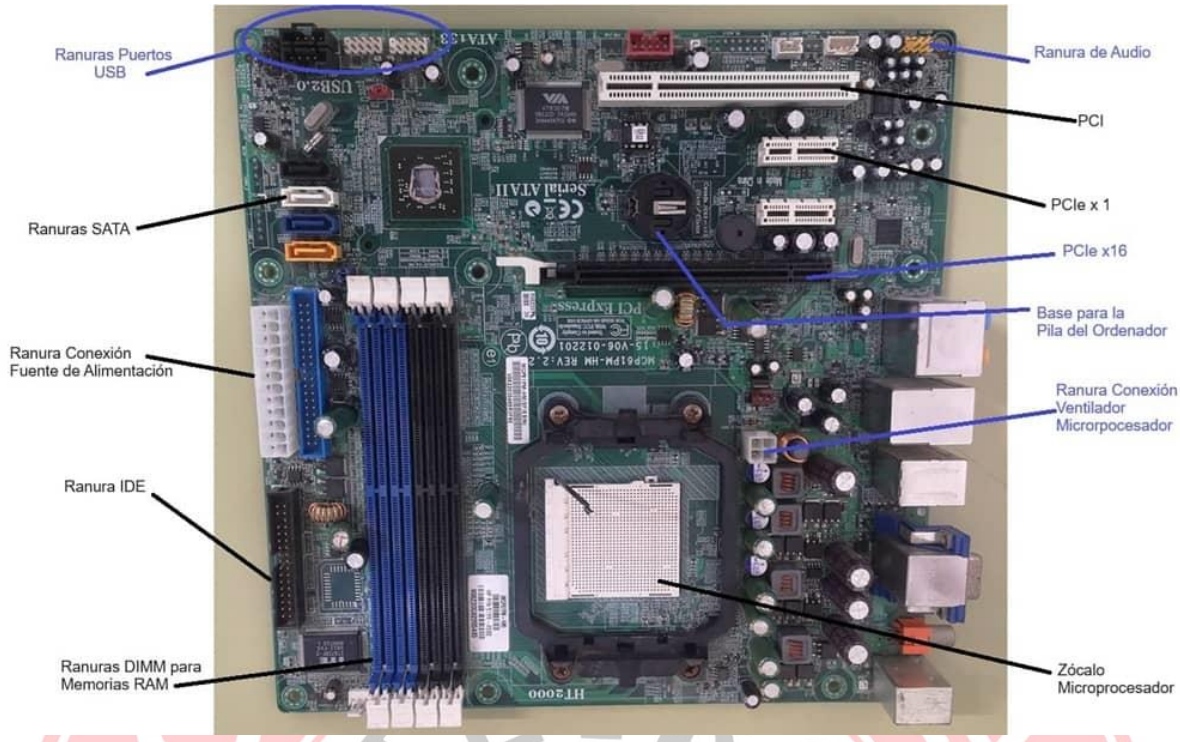
5.2. ENSAMBLAJE Y CONFIGURACIÓN DE HARDWARE

El ensamblaje de hardware consiste en la instalación y conexión de los componentes físicos de un equipo microinformático. Cada componente cumple un papel específico y debe instalarse correctamente para garantizar un rendimiento óptimo del sistema.

5.2.1. COMPONENTES PRINCIPALES DE UN SISTEMA MICROINFORMÁTICO:

5.2.1.1. PLACA BASE (MOTHERBOARD)

La placa base es considerada como uno de los componentes principales de un ordenador. Conocida también como placa madre, tarjeta madre o en sus concepciones originales en inglés (motherboard, mainboard), es uno de los elementos imprescindibles que tu sistema informático debe incluir.



Funciones de la placa base

A nivel general, una placa base es responsable de que todos los sistemas funcionen correctamente.

Se responsabiliza de la interconexión entre todos los componentes de un aparato electrónico. Por este motivo no es difícil también ver placas base en un teléfono móvil como en cualquier ordenador, de sobremesa o portátil.

En función del tipo de placa base y de sus características, la capacidad del equipo informático será mayor o menor. Esto se debe a que también depende de estos factores la calidad de los componentes que podamos tener instalados o modificar y sustituir en el futuro.

Características de la placa base

En función de las características de una placa base, esta permite la inclusión de ciertos componentes, así como ofrece una capacidad y potencia distintas.

Las características más importantes que condicionan estos elementos son las siguientes:

- **Memoria RAM**: La cantidad, la tipología y la velocidad de la memoria RAM van a depender de los slots disponibles en la placa base, así como de las limitaciones que la tarjeta permite.

- **Tamaño de la placa**: La capacidad del hardware instalado está directamente relacionada con el tamaño de la placa base, así como obviamente también el espacio disponible. Es también identificado como factor de forma y de él depende la tipología de la placa que podamos instalar (Extended ATX, ATX, Micro ATX o Mini ITX).
- **Puertos USB**: La placa base delimita entre otros aspectos la cantidad de puertos USB que puede tener el equipo, así como también la tipología a la que corresponden.
- **Socket de la CPU**: Este elemento es clave. En él se conectan componentes tan importantes como la CPU y arquitecturas compatibles.
- **Unidades de almacenamiento**: La placa base delimita la cantidad de unidades de almacenamiento, así como la velocidad a la que pueden trabajar.
- **Conectividad de otros componentes:** De la placa base depende la conectividad de red, la misma BIOS o incluso el sonido, entre otros componentes.

Partes de una placa base

Si alguna vez tienes la oportunidad de analizar con detenimiento una placa base, vas a descubrir que tiene múltiples partes y todas ellas son de gran importancia, para el buen funcionamiento de todo el sistema informático que controla.

Las partes más importantes de una placa base podemos identificarlas de esta manera:

Chipset

La placa base cuenta con un chipset, que es el centro de comunicaciones de todo el equipo. No es responsable absolutamente de todas las comunicaciones de datos, pero sí de muchas interacciones entre la tarjeta y el resto de componentes del ordenador.

De hecho, en base al chipset instalado, tendremos o no compatibilidad con algunas tarjetas gráficas, con la memoria RAM, etc. De él dependen incluso los puertos USB que podemos aprovechar.

En la actualidad los chipset Intel y AMD son los más comercializados en el mercado.

Socket de CPU

Es conocido tanto como socket como zócalo. Se trata del espacio en el que se conecta el procesador del sistema informático. Su forma, determina la compatibilidad con los procesadores.

Slots RAM

Una placa base limita la capacidad RAM por los slots disponibles. La cantidad de slots, su tipología y compatibilidad, nos permitirán tener más o menos RAM en nuestro ordenador, con la que hacer funcionar todos los programas.

Puertos de disco

El disco duro que utilicemos estará conectado a la placa base a través de estos puertos. Aquí también es importante la tipología, porque no es lo mismo la compatibilidad que requiere un disco duro mecánico que uno de estado sólido o SSD.

Ranuras PCIe

Un ordenador puede contar con múltiples componentes, con los que podemos disfrutar de sonido, gráficos o almacenamiento, entre otros elementos. Para que estos componentes estén correctamente conectados a la placa madre, es necesario que cuenten con estas ranuras PCIe, donde vincularemos la tarjeta gráfica, la tarjeta de sonido, periféricos, etc.

Conectores de alimentación

La placa base funciona en base a una fuente de alimentación, que se vincula a través de estos conectores. Es imprescindible para que la tarjeta pueda funcionar correctamente.

Conexiones exteriores

La placa base también está conectada directamente a los periféricos que utilicemos, para lo que presenta conexiones exteriores, en las que podremos colocar directamente cada cable.

Batería CMOS

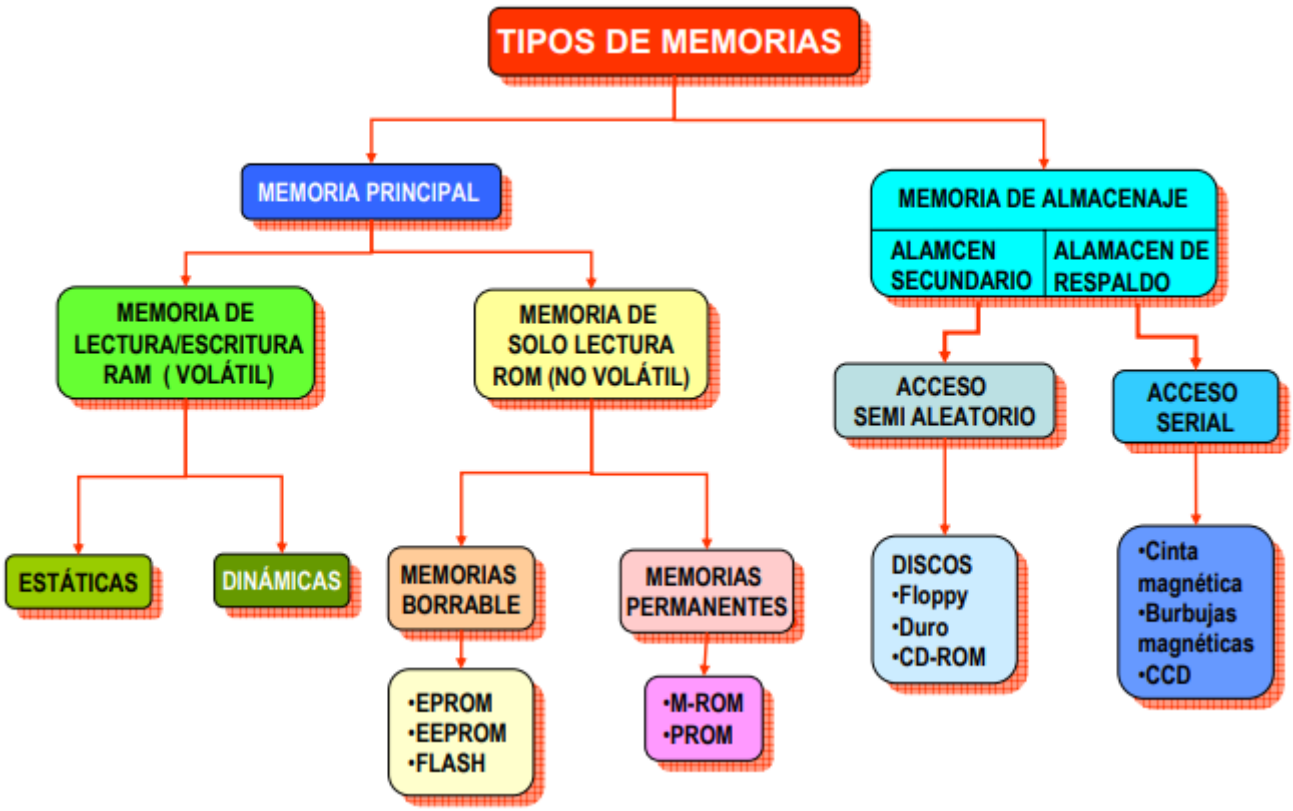
Una placa base cuenta con una batería CMOS, cuya función principal es la de almacenamiento de configuraciones de la BIOS. Básicamente nos sirve para evitar que perdamos datos cuando apagamos el ordenador.

Disipador de calor

Con el fin de que la placa base no se sobrecaliente, cuenta con un disipador que se encarga de expulsar el calor generado hacia el exterior del equipo.

- **Unidad central de procesamiento (CPU)**: Es el cerebro del equipo y ejecuta las instrucciones de los programas.
- **Memoria RAM**: Almacena temporalmente datos que se usan en tiempo real para agilizar procesos.

5.2.1.2. MEMORIAS



Cuando hablamos de los tipos de memoria de un PC u ordenador, todo son siglas y tecnicismos. En este post intentamos aclarar ideas sobre estos componentes que muchas veces están escondidos en las 'tripas' del ordenador. Destacamos las más importantes y qué función tiene cada una.

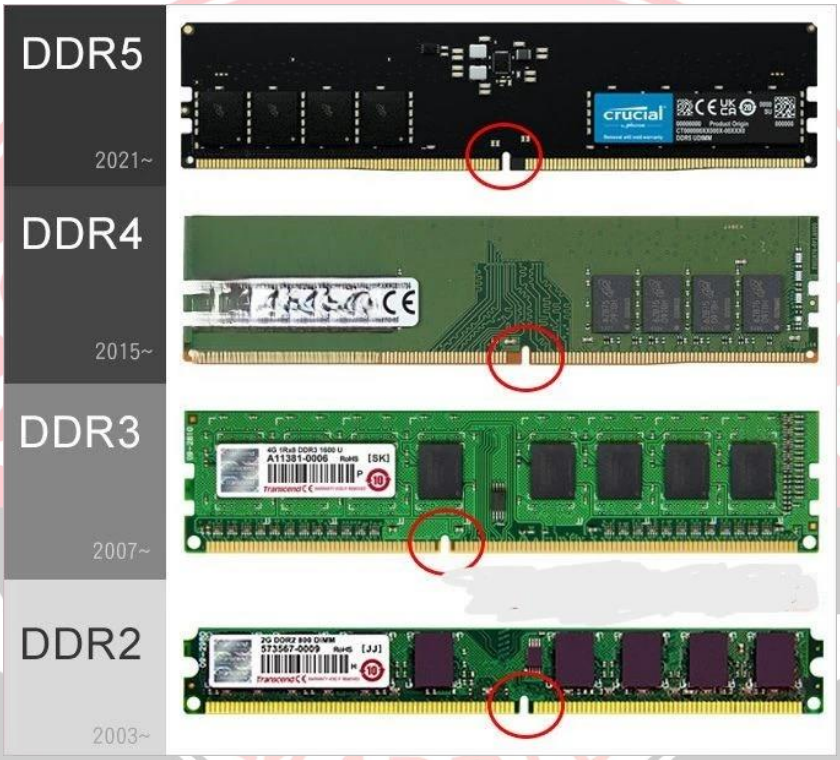
Memoria RAM

La llamada memoria RAM o Random Access Memory almacena datos e instrucciones de los programas que se requieren en un momento determinado. Esta información es usada en tiempo real por la CPU o unidad de procesamiento del equipo. Se puede decir que en la RAM están los datos de los que el ordenador va a echar mano para facilitar que el usuario, en un momento muy concreto, navegue, escriba un texto o vea un vídeo en YouTube, por ejemplo.

La RAM es fundamental porque es la que permite que los programas se inicien, se carguen y se ejecuten. De su capacidad dependerá en gran parte la velocidad en que se van a desplegar esos programas y van a responder a las demandas del usuario. Por ejemplo, si usamos un navegador, la RAM va a guardar los datos de las webs que visitamos para evitar cargarlas cada vez que accedemos a ellas. Y lo mismo pasará con las aplicaciones abiertas.

Es, por tanto, una unidad que no almacena permanentemente los datos, sino que tiene un carácter volátil. Es decir, la información que se guarda en un momento dado se pierde cuando el ordenador se apaga. O cuando se produce un fallo de energía. Por eso, es una memoria con una capacidad de almacenamiento mucho menor a otras, como la de los discos duros y las unidades SSD, que son el verdadero 'trastero' al que van a parar todos los archivos que generamos, desde documentos ofimáticos a fotos o vídeos.

La RAM ha tenido muchas variantes. Desde la histórica DRAM, que se utilizó hasta los años noventa, hasta las modernas DDR5 SDRAM, y la GDDR SDRAM, que se utiliza para el renderizado de vídeo, una tarea muy exigente y que consume muchos recursos del ordenador.



Memoria caché

Es una memoria que se sitúa entre la RAM y el procesador del ordenador, y que acelera el intercambio de datos. Este tipo de memoria, que suele pasar desapercibida para el usuario corriente, hace que los procesos en el ordenador se ejecuten más rápido. De esta forma evita, por ejemplo, que el procesador tenga que esperar. El tamaño de la memoria caché, que está organizada por niveles, es mucho menor que el de la RAM.

Memoria ROM

Las siglas responden a Read Only Memory. Es decir, que es una memoria solo de lectura. Donde los datos se leen y usan, pero no se modifican. En el módulo de memoria ROM de un ordenador la información permanece, incluso cuando se apaga el equipo o se queda momentáneamente sin energía eléctrica.

Así, en la ROM residen datos clave para el equipo. Se trata de todas las instrucciones que el ordenador necesita para empezar a funcionar. Lo que se conoce como la BIOS o instrucciones de inicio. Y también está ahí el firmware del equipo, es decir, todas las instrucciones que controlan los circuitos electrónicos incluidos en la máquina. La introducción de datos en la memoria ROM la hace la marca del ordenador en fábrica. Y por eso es muy difícil cambiar la información almacenada en ella.

5.2.1.3. ALMACENAMIENTO (HDD/SSD):

Diferencias HDD vs SSD

Para que no te agobies y a modo de resumen, hemos reunido las principales diferencias de los discos HDD vs SSD en una tabla. Y es que aunque sirven para guardar grandes cantidades de información, ambos tipos de discos duros son muy diferentes entre sí.

	Discos Duros HDD	Discos SSD
Capacidad	Desde 256GB a 4TB	Desde 256GB a 1TB
Relación almacenamiento/precio	Más barato	Más caro
Vida útil	Mayor	Menor
Ruido	Mayor	Ninguno
Vibración	Si	No
Fragilidad	Mayor	Menor
Afectado por el magnetismo	Si	No
Arranque del Sistema Operativo	16 segundos	7 segundos

Velocidad de lectura	Hasta 200 MB/s	Hasta 5.200 MB/s
Velocidad de escritura	Hasta 150 MB/s	Hasta 3.800 MB/s
Consumo de energía	Mayor	Menor
Tamaño	Mayor	Menor

Como habrás podido ver, los HDD y los SSD son radicalmente opuestos. Mientras que el HDD es un camión con mucha capacidad de almacenamiento y el SSD es un deportivo. Más caro y con menos almacenamiento, si, pero muchísimo más rápido.

Pero claro, destacar las diferencias de un disco duro HDD y SSD solo con conceptos como “mayor”, ”ninguno” o “más caro” es complicado. Así que, a continuación, vamos a entrar en detalle de todas y cada una de las ventajas, desventajas y características de ambos tipos de discos duros.

Discos duros HDD

Aunque seguro que ya lo sabes, un disco duro HDD es un dispositivo de almacenamiento de datos que utiliza la grabación magnética para almacenar y recuperar información digital.

La principal diferencia del HDD vs SSD es que este segundo utiliza memorias flash interconectadas sin movimiento, una unidad de disco duro o HDD está compuesta esencialmente por un plato de metal con revestimiento magnético.

Esta diferencia en la construcción hace que el funcionamiento y las características tambíen sean diferentes entre un SSD y un HDD. En un disco duro tradicional existe un revestimiento almacena los datos que cuenta con un cabezal magnético emparejado que lee y escribe datos mientras el disco gira.

Y es que a pesar de que los discos duros HDD son más antiguos, siguen siendo un dispositivo de almacenamiento muy popular entre los fabricantes y los consumidores porque son más accesibles y asequibles que las unidades de estado sólido.

Discos duros SSD

Los SSD son la evolución de los discos duros tradicionales, los HDD. Y es que la principal diferencia entre un SSD y un HDD es que este primero no tiene piezas móviles. Los SSD se basan en chips flash (como una memoria USB) lo que hace que sean extremadamente rápidos y menos volátiles que las HDD.

5.2.1.4. TARJETA GRÁFICA (GPU):

Una tarjeta gráfica es un componente de un ordenador que puede estar integrado dentro de la placa base, el procesador o ser externo y cuya función es la renderizar las imágenes en la pantalla y ofrecer una visualización de alta calidad, procesando y ejecutando datos gráficos mediante técnicas, características y funciones gráficas avanzadas.

¿Y quienes necesitan estas tarjetas gráficas? En primer lugar, los usuarios que utilizan el ordenador para jugar videojuegos. Luego, los que usan aplicaciones de edición de vídeo como Adobe Premiere o DaVinci Resolve, como así para editar fotografías, como puede ser Adobe Photoshop. Por último, los usuarios que trabajan con complejos programas

informáticos de inteligencia artificial. Para realizar cualquiera de estas tres actividades, una buena tarjeta gráfica es imprescindible.

Diferencia entre una tarjeta gráfica y una GPU

Después de esta definición tan académica, hay que aclarar un malentendido general. Y es que hay que diferenciar la GPU (unidad de procesamiento gráfico) de lo que es una tarjeta gráfica, porque lo primero es un chip, mientras que lo segundo es un producto terminado.

Las siglas GPU se refieren a Graphics Processing Unit o unidad de procesamiento gráficos y se trata de un chip encargado para acelerar la representación de gráficos 3D. Sin embargo, este concepto ha evolucionado mucho debido al avance tecnológico en desarrollo y en arquitecturas. La GPU realiza multitud de operaciones relacionadas con los datos 2D y 3D, como es decodificar y renderizar objetos animados y vídeos. El grado de sofisticación con el que cuenta una GPU hoy en día es brutal, agregando más y más tareas.

diferencias entre tarjeta gráfica y GPU

Antes, la GPU no era más que un chip que se encargaba de acelerar gráficos 3D; en pleno siglo XXI, la GPU renderiza, codifica, calcula el rebote de los rayos del Ray Tracing, optimiza el rendimiento con tecnologías de reescalado y algunas hacen uso de Machine Learning e Inteligencia Artificial.

Ahora que tenemos claramente identificado qué es una GPU, vamos a explicaros qué es una tarjeta tarjeta gráfica como producto completo compuesto por:

- PCB, que es donde van soldados todos los componentes.
- Módulos de memoria (GRAM).
- Condensadores y demás componentes.
- Tuberías de calor.
- Ventiladores (o blower) y carcasa.

Ahora que sabes diferenciar una GPU de una tarjeta gráfica, vamos a seguir explicandote diferentes conceptos esenciales para que te vuelvas todo un experto.

Cómo funciona una tarjeta gráfica

Cada vez más vas sabiendo que es una tarjeta gráfica y ahora que conoces los componentes que la conforman y en especial la GPU, es el momento ideal para explicarte cómo funciona una tarjeta gráfica.

Como ya te hemos explicado, la GPU es un micro-componente muy complejo con diferentes núcleos encargados de procesar la información. Y son precisamente la cantidad y la capacidad de estos lo que determinará la potencia de la tarjeta gráfica. Al

contrario que con la CPU (procesador) la GPU tiene muchos núcleos con frecuencias bajas encargado cada uno de procesar un número muy grande de píxeles.

Otro de los componentes que te habíamos mencionado antes es la GRAM (memoria gráfica de acceso aleatorio) y su función dentro de una tarjeta gráfica es la de almacenar y transportar información. Esta información pasa el RAMDAC, que viene a ser conversor de señal digital a señal analógica necesario para que el monitor de nuestro ordenador pueda interpretar la información que se le está enviando.

Seguramente no hayas entendido ni la mitad de lo que te hemos explicado sobre cómo funciona una tarjeta gráfica, no te culpamos. Podríamos simplificar mucho y decir que para funcionar la tarjeta gráfica hace dos cosas: procesa los vértices, su ordenamiento espacial, su rotación, y qué segmentos de estos serán visibles gráficamente para transmitir luego esta información al monitor en un formato que pueda representar.

Qué tipos de tarjetas gráficas existen

Ahora que ya sabes qué es una tarjeta gráfica, es el momento de que aprendas a diferenciarlas antes de comprarlas. Y es que, lo primero que tienes que saber es que todas las tarjetas gráficas son desarrolladas por dos marcas rivales: Nvidia vs AMD.

Esto hace que tanto comprar las tarjetas gráficas Nvidia como las tarjetas gráficas AMD sea más sencillo porque, aunque hay muchas empresas que venden tarjetas gráficas, ya que todas utilizan la misma arquitectura subyacente. En otras palabras, independientemente de si la compras a Asus, MSI, Gigabyte o Nvidia, un modelo concreto tarjeta gráfica de Nvidia se comportará más o menos igual da igual quien la fabrique.

tipos de tarjetas gráficas

Además, por regla general, las mejores tarjetas AMD ofrecen un rendimiento similar al de las mejores tarjetas Nvidia. Por lo que será más cuestión de precios, de stock y de gustos personales.

Pero eso no es todo y es que, en función del fabricante de la tarjeta gráfica, podemos encontrar diferentes modelos en función a dos características principales:

- Por refrigeración:
    - Activa: hacen uso de ventiladores.
    - Pasiva: hacen uso de aletas de aluminio para expulsar el calor por el método de convección.
    - Líquida: utilizan un bloque de agua que lleva conectado 2 tubos dirigidos a un radiador con uno o varios ventiladores para expulsar el calor fuera de la caja.

- Por tamaño:

    - 1 ventilador o Mini-ITX, ideales para PCs con dicho factor de forma.
    - 2 ventiladores, es el tamaño estándar aunque algún modelo puede encajar en un mini-ITX.
    - 3 ventiladores, un tamaño bastante grande y que no cabe en todas las cajas ATX.

Qué componentes tiene una tarjeta gráfica

¿Sigues por aquí? Entonces realmente te interesa saber que es una tarjeta gráfica a fondo. La verdad es que nos encanta, así que vamos a explicar con mayor profundidad cuáles son los componentes principales de una tarjeta gráfica.

GPU

La principal pieza de una placa de vídeo es la GPU, la unidad de procesamiento gráfico. Se refiere a un procesador dedicado, justamente, al procesamiento de los gráficos. Lo que hace es aligerar la carga de trabajo del procesador central, acción que la convierte en la parte más importante de toda tarjeta gráfica y es la que determina el rendimiento de la misma.

GRAM

Luego, encontramos la GRAM, la memoria gráfica de acceso aleatorio, que son chips de memoria que almacenar y transportan información. En este sentido, identificados dos tipos de memorias gráficas. Por una parte, la dedicada, memoria más eficiente cuando la tarjeta o la GPU disponen exclusivamente para sí este tipo de memorias. Por otro lado, está la compartida, utilizada cuando se emplea memoria en detrimento de la memoria de acceso aleatorio.

A su vez, la potencia de la memoria gráfica es el resultado de tres aspectos: capacidad, interfaz de memoria y frecuencia de memoria.

La capacidad determina el número máximo de datos y texturas que puede procesar. Es un detalle muy relevante a tener en cuenta para resoluciones superiores a 1440p y monitores múltiples, donde cada imagen toma mucho más espacio.

La interfaz de memoria, o bus de datos, resulta de la multiplicación del ancho de bits de cada chip por su número de unidades. Es un detalle clave para determinar el ancho de banda, es decir, la cantidad de datos que puede transferir en cierto tiempo.

Por último, la frecuencia de memoria es, valga la redundancia, la frecuencia a la que la memoria puede transportar los datos ya procesados. Es así que se complementa con la interfaz y, entre ambas características, se determina el ancho de banda de la memoria.

5.2.1.5. FUENTE DE ALIMENTACIÓN:

Las fuentes de alimentación son esenciales en cualquier equipo: sin ellas no funciona ningún componente. Encargadas de suministrar energía a los diversos componentes que coexisten en un PC o portátil, se pueden diferenciar por su tamaño, su cableado, por su potencia y por su eficiencia energética.

Tipos de fuente de alimentación

En primer lugar, hay que clasificar todas las fuentes de alimentación que existen en el mercado siguiendo 4 criterios generales: factor de forma o tamaño, cableado, refrigeración, potencia y eficiencia energética.

Según su factor de forma

Ya sea por factor de forma o por tamaño, podemos encontrar las fuentes de alimentación ATX, SFX, SFX-L o TFX, siendo dichas dimensiones las más estandarizadas.

- **ATX**. La mayoría de fuentes vienen con este formato, sus medidas son 150 mm de ancho y 86 mm de altura, además de que ofrecen más potencia que los demás formatos de fuentes. Hay una diferencia en cuanto a su profundidad:
    - ATX PS/2 para fuentes de 140 mm.
    - ATX PS/3 para fuentes de 100 mm.
- **SFX (Small Form Factor).** Ideado para cajas con factor de forma Mini-ITX, tienen unas dimensiones de 125 mm de ancho y 63.5 mm de altura, siendo su diámetro de 100 mm. Cuenta con límites físicos obvios, por lo que cuesta ver potencias altas (más de 500 W) y las capacidades de refrigeración son más limitadas.
- **SFX-L**. La "L" supone largey se refiere a que es algo más grande, en medidas: 125 x 63.5 x 130 mm. Aquí cambia la profundidad y el diámetro del ventilador, siendo la métrica más importante la profundidad de cara a instalarla en una caja pequeña. Suele ofrecer más potencia final, aunque no son baratas.
- **TFX.** Parecidas a unas cajas de zapatos, vienen a ser una fuente de alimentación de tamaño alargado estando su ventilador dispuesto en un extremo de la fuente, y no en medio de la misma. Sus medidas son de 85 mm de ancho, 65 mm de altura y 175 mm de profundidad. Eso sí, su potencia es la menor de todas.

Cableado: fuentes modulares/semimodulares

La distinción aquí es clara porque solo tendremos 3 opciones en cuanto a la administración del cableado:

- Nuestras opciones se resumen a las que ofrece la fuente de alimentación, disponiendo de las conexiones básicas y de algún adaptador, dependiendo mucho del modelo.

- Semi-modular. Son fuentes de alimentación que vienen con ciertos cables fijos, pero que ofrece posibilidad de usar conexiones modulares opcionales, especialmente en SATA y PCIe.
- Modular. Todas las conexiones son modulares, pudiendo usar únicamente las que necesitemos, y para ello tendremos varios cables en la caja de la fuente.

Según su refrigeración

En este sentido, solo encontramos 2 opciones de refrigeración, con la excepción de algunos modos semi-pasivos que tienen algunas fuentes activas.

- **Activa**. Vienen a ser las opciones más comunes, equipando un ventilador para expulsar el calor generado por los componentes de la fuente de alimentación. Algunas fuentes más refinadas vienen con modos semi-pasivos con los que podemos disfrutar de 0 dB, es decir, pleno silencio, siempre que el PC tenga poca carga.
- **Pasiva**. Su refrigeración es mediante la convección, no equipando ningún ventilador y siendo muy silenciosas. Solo recomendamos su compra a aquellos que sepan refrigerar óptimamente su PC porque el calor del interior de la caja se disparará cuando exijamos el máximo rendimiento a nuestro equipo.

Según su potencia

La potencia de las fuentes de alimentación tiene un rango de vatios muy amplio, partiendo desde los 180 W y yendo hasta los 2.000 W. La mayoría de las personas optan entre una fuente de 450 W y 850 W debido a que no disfrutaremos nunca del 100% de toda su potencia, sino que para ello hay que tener en cuenta la eficiencia energética.

5.2.1.6. PERIFÉRICOS:

Los periféricos son dispositivos externos que complementan el funcionamiento de un sistema informático, facilitando la comunicación entre el usuario y la computadora. Se pueden clasificar en tres tipos: **periféricos de entrada**, **periféricos de salida** y **periféricos mixtos**.

1. **Monitores (Periféricos de salida)**
   - Son dispositivos de visualización que muestran la información generada por la computadora.
   - Pueden ser de distintos tipos, como LCD, LED o táctiles.
   - Su calidad se mide en factores como la resolución, el tamaño y la tasa de refresco.
2. **Teclados (Periféricos de entrada)**
   - Permiten la introducción de datos y comandos mediante teclas.
   - Existen diferentes tipos, como mecánicos, de membrana o inalámbricos.
   - Pueden incluir teclas especiales para funciones avanzadas.
3. **Ratones (Periféricos de entrada)**

- Facilitan la navegación e interacción con la interfaz gráfica del sistema.
- Pueden ser ópticos o láser y tener conexión USB o inalámbrica.
- Algunos modelos incluyen botones adicionales para funciones específicas.

4. **Impresoras (Periféricos de salida o mixtos)**
   - Transforman documentos digitales en copias físicas.
   - Existen varios tipos, como impresoras de inyección de tinta, láser o térmicas.
   - Algunas impresoras incluyen funciones de escáner, convirtiéndose en periféricos mixtos.

Estos periféricos son esenciales para optimizar la experiencia del usuario y mejorar la eficiencia en el uso de los sistemas informáticos.

5.2.2. PROCESO DE ENSAMBLAJE:

1. **Preparación del área de trabajo**: Se debe contar con una superficie limpia y libre de electricidad estática.
2. **Instalación de la fuente de alimentación**: Se coloca en el gabinete y se conectan los cables correspondientes.
3. **Montaje de la placa base**: Se fija con tornillos en el gabinete y se conectan los cables de alimentación y datos.
4. **Colocación del procesador y disipador térmico**: Se instalan en el zócalo correspondiente y se aplica pasta térmica para la disipación del calor.
5. **Instalación de la memoria RAM**: Se inserta en las ranuras específicas de la placa base.
6. **Conexión de dispositivos de almacenamiento**: Se instalan discos duros o SSD mediante interfaces SATA o NVMe.
7. **Conexión de cables y dispositivos periféricos**: Se conectan los cables de datos y de alimentación a cada componente.
8. **Pruebas iniciales**: Se verifica el encendido correcto y se accede a la BIOS para comprobar la detección de hardware.

5.3. INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE

Tras el ensamblaje del hardware, es necesario instalar y configurar el software adecuado para garantizar el correcto funcionamiento del equipo.

5.3.1. INSTALACIÓN DEL SISTEMA OPERATIVO

El **sistema operativo (SO)** es el software fundamental que gestiona los recursos del hardware y permite la interacción con el usuario. Es imprescindible para ejecutar programas y aplicaciones en una computadora.

Los sistemas operativos más utilizados son:

- **Windows:** Popular en entornos domésticos y empresariales debido a su facilidad de uso y compatibilidad con una amplia gama de software y hardware.

- **Linux:** Preferido en servidores y por usuarios avanzados gracias a su estabilidad, seguridad y opciones de personalización.

- **macOS:** Exclusivo para dispositivos Apple, destaca por su diseño intuitivo, optimización del hardware y alta seguridad.

Proceso de Instalación del Sistema Operativo

La instalación de un sistema operativo sigue una serie de pasos esenciales para garantizar un funcionamiento estable y eficiente del equipo.

1. Configuración de la BIOS/UEFI

- Se accede a la BIOS o UEFI al iniciar el equipo (generalmente presionando teclas como **F2, F12, DEL o ESC**).

- Se ajustan configuraciones básicas, como la compatibilidad con discos en modo **Legacy (BIOS) o UEFI**.
- Se establece el **orden de arranque**, priorizando el medio de instalación (USB o DVD).

2. Inicio desde un medio de instalación

- Se utiliza un **USB o DVD** que contiene la imagen del sistema operativo.
- En algunos casos, se requiere crear un medio de arranque con herramientas como **Rufus (Windows y Linux)** o **Disk Utility (macOS)**.
- Al reiniciar el equipo, el sistema se carga desde este medio y se inicia el asistente de instalación.

3. Selección de particiones

- Se define la estructura del disco duro o SSD para la instalación del sistema operativo y almacenamiento de datos.
- Existen varias opciones:
  - **Instalación limpia:** Se borra todo el contenido y se crea una nueva partición.
  - **Partición manual:** Se asigna espacio específico para el sistema, datos y, en algunos casos, archivos de intercambio (*swap* en Linux).
  - **Arranque dual:** Se instala junto a otro sistema operativo sin eliminar el existente.

4. Configuración inicial

- Se crean usuarios y contraseñas para acceder al sistema.
- Se establecen opciones de red, como la conexión Wi-Fi o LAN.
- Se instalan controladores y actualizaciones necesarias para garantizar un rendimiento óptimo.
- En algunos casos, se instalan programas esenciales como navegadores, software de oficina y herramientas de seguridad.

Métodos de Instalación Adicionales

- **Actualización del sistema:** Se pasa de una versión anterior a una más reciente sin perder datos.
- **Virtualización:** Se instala el sistema operativo en un entorno virtual usando programas como **VirtualBox** o **VMware**.
- **Modo Live (Linux):** Permite ejecutar el sistema desde un USB sin necesidad de instalarlo en el disco.

5.3.2. INSTALACIÓN DE CONTROLADORES Y SOFTWARE BÁSICO

Después del sistema operativo, se instalan los controladores de los dispositivos para garantizar su compatibilidad y funcionamiento.

- **Drivers de chipset y almacenamiento**: Mejoran la comunicación entre la placa base y los dispositivos de almacenamiento.
- **Drivers de tarjeta gráfica**: Permiten un rendimiento óptimo en gráficos y multimedia.
- **Drivers de red**: Habilitan la conectividad a redes cableadas e inalámbricas.
- **Software de seguridad**: Antivirus y cortafuegos para protección del sistema.
- **Programas esenciales**: Navegadores, suites ofimáticas y herramientas de productividad.

5.4. DIAGNÓSTICO Y REPARACIÓN DE AVERÍAS

El diagnóstico y reparación de averías es una parte crucial del mantenimiento de los sistemas microinformáticos. Las fallas pueden originarse en el hardware, el software o la configuración del sistema.

5.4.1. TIPOS DE AVERÍAS COMUNES:

- **Problemas de hardware:**
  - Fallo en la alimentación eléctrica.
  - Sobrecalentamiento del procesador o GPU.
  - Errores en la memoria RAM o almacenamiento.
- **Problemas de software:**
  - Corrupción del sistema operativo.
  - Incompatibilidades de controladores.
  - Presencia de malware o virus.
- **Problemas de configuración:**
  - Errores en la configuración de la BIOS.
  - Configuración incorrecta de redes o permisos de usuario.

5.4.2. MÉTODOS DE DIAGNÓSTICO:

- **Uso de herramientas integradas**: Diagnósticos de hardware en la BIOS, comprobación de errores en discos duros (CHKDSK en Windows, fsck en Linux).
- **Pruebas de componentes**: Sustitución de piezas sospechosas para descartar fallos.

- **Monitoreo del sistema**: Uso de software como HWMonitor o CPU-Z para evaluar temperaturas y consumo energético.

5.5. HERRAMIENTAS Y EQUIPOS PARA EL MONTAJE

El montaje de equipos electrónicos requiere del uso de herramientas especializadas que permitan ensamblar, conectar y comprobar el correcto funcionamiento de los circuitos y componentes. Estas herramientas se pueden clasificar en manuales y eléctricas.

5.5.1. HERRAMIENTAS MANUALES

- **Destornilladores de precisión**: Se utilizan para ensamblar o desmontar equipos electrónicos con tornillos pequeños.
- **Alicates de corte y de punta**: Facilitan la manipulación de componentes y el corte de cables o terminales.
- **Llaves y pinzas**: Para sujetar pequeños componentes sin dañarlos.
- **Cuchillas y bisturíes electrónicos**: Útiles para retirar recubrimientos o aislamientos.

5.5.2. HERRAMIENTAS ELÉCTRICAS

- **Estación de soldadura**: Esencial para la unión de componentes en circuitos impresos.
- **Desoldador**: Permite retirar soldadura y corregir errores en las conexiones.
- **Multímetro**: Mide voltaje, corriente y resistencia para comprobar el funcionamiento de circuitos.
- **Osciloscopio**: Analiza señales eléctricas en circuitos electrónicos.
- **Fuente de alimentación regulable**: Proporciona energía para realizar pruebas en los dispositivos ensamblados.

Un correcto uso de estas herramientas garantiza una instalación adecuada de los componentes electrónicos y evita daños por manipulación incorrecta.

5.6. PROCEDIMIENTOS DE PRUEBA Y VERIFICACIÓN

Tras el montaje, los equipos electrónicos deben pasar por pruebas para asegurar que funcionan correctamente y cumplen con los requisitos de diseño.

5.6.1. MÉTODOS DE PRUEBA EN ELECTRÓNICA

1. **Pruebas de continuidad**: Uso de multímetros para verificar la conexión entre terminales.
2. **Pruebas de voltaje y corriente**: Comprobación de la alimentación y consumo de los circuitos.
3. **Pruebas funcionales**: Validación del rendimiento del equipo bajo condiciones normales de operación.
4. **Pruebas de estrés**: Evaluación del comportamiento del equipo en condiciones extremas de temperatura o carga.
5. **Análisis de señal**: Uso de osciloscopios y analizadores lógicos para examinar el comportamiento de las señales electrónicas.

El cumplimiento de estos procedimientos reduce fallos en la fabricación y montaje de equipos electrónicos.

5.7. DIAGNÓSTICO Y REPARACIÓN DE EQUIPOS ELECTRÓNICOS

Cuando un equipo electrónico presenta fallos, es necesario identificar la causa del problema y realizar las correcciones pertinentes.

5.7.1. TIPOS DE FALLOS EN EQUIPOS ELECTRÓNICOS

- **Fallos eléctricos**: Cortocircuitos, sobrecargas y fallos en la alimentación.
- **Fallos mecánicos**: Problemas en conectores, soldaduras frías o componentes dañados físicamente.
- **Fallos térmicos**: Sobrecalentamiento que afecta el funcionamiento de los componentes.
- **Fallos por obsolescencia**: Deterioro de componentes con el tiempo.

5.7.2. MÉTODOS DE DIAGNÓSTICO

1. **Inspección visual**: Detección de soldaduras defectuosas, componentes quemados o conectores sueltos.
2. **Medición con multímetro**: Verificación de continuidad, voltajes y resistencias.
3. **Pruebas con osciloscopio**: Análisis del comportamiento de las señales electrónicas.
4. **Sustitución de componentes**: Cambio de piezas defectuosas para comprobar si se soluciona el problema.

6. ELEMENTOS DE TELECOMUNICACIONES

6.1. DISPOSITIVOS DE TRANSMISIÓN Y RECEPCIÓN

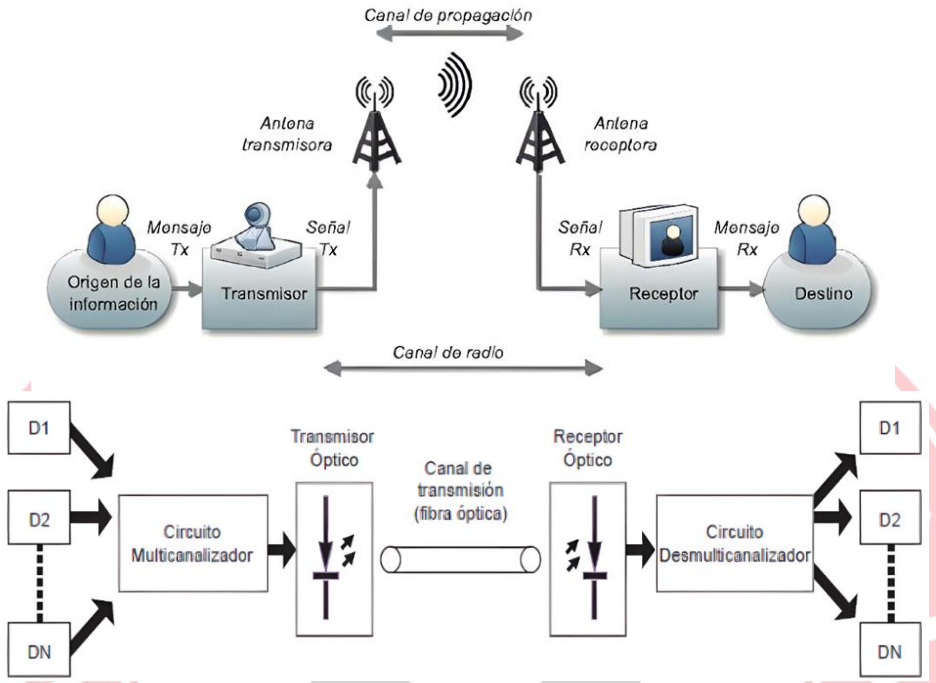
Los sistemas de telecomunicaciones están compuestos por dispositivos encargados de transmitir y recibir señales, permitiendo la comunicación a larga distancia. Estos dispositivos pueden ser analógicos o digitales y varían según la tecnología utilizada en la red. La evolución de estos dispositivos ha permitido la mejora en la velocidad, eficiencia y calidad de la comunicación global. Actualmente, se desarrollan tecnologías que optimizan la transmisión y recepción de datos, permitiendo el crecimiento de redes 5G y el Internet de las cosas (IoT). Además, con el avance de la inteligencia artificial y el machine learning, los dispositivos de telecomunicaciones están adquiriendo capacidades de autogestión y optimización dinámica de la red, mejorando su rendimiento en tiempo real.

6.1.1. DISPOSITIVOS DE TRANSMISIÓN

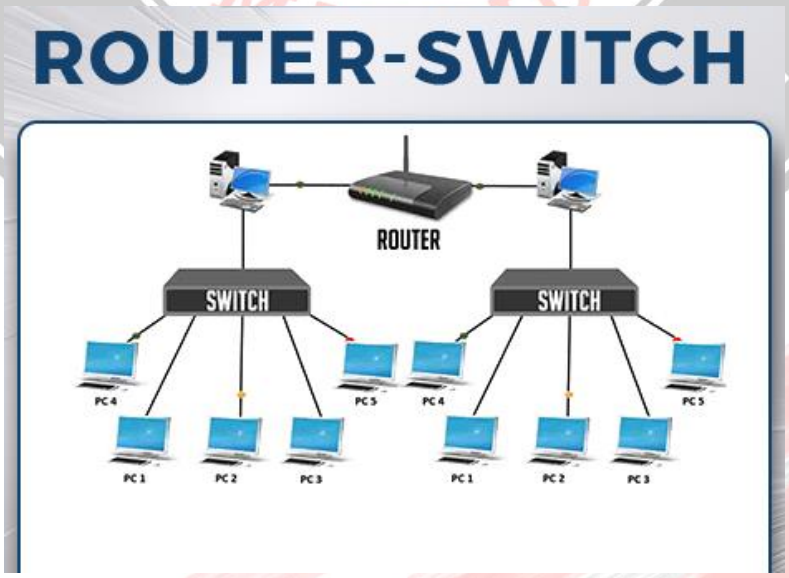
Los dispositivos de transmisión envían señales a través de distintos medios físicos o inalámbricos. Son fundamentales en la comunicación moderna y garantizan que la información viaje de manera eficiente desde un punto de origen hasta un destino. Existen diferentes tipos de dispositivos de transmisión, cada uno con funciones específicas según el medio y la tecnología utilizada. Algunos ejemplos incluyen:

- **Transmisores de radio y televisión:** Son dispositivos que convierten señales eléctricas en ondas electromagnéticas para su emisión. En la actualidad, estos

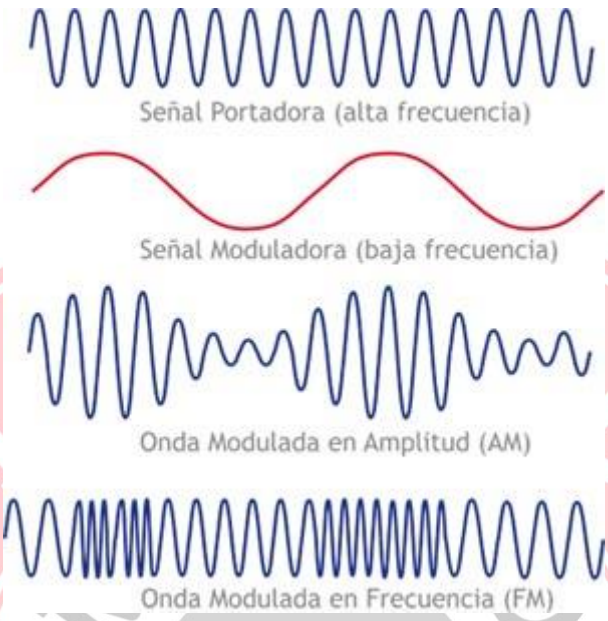
transmisores pueden trabajar con tecnologías digitales, lo que permite una mayor calidad de transmisión y menor interferencia. Con la llegada de la televisión digital terrestre (TDT) y la radio digital, la compresión de datos ha mejorado la eficiencia en la distribución del espectro electromagnético.



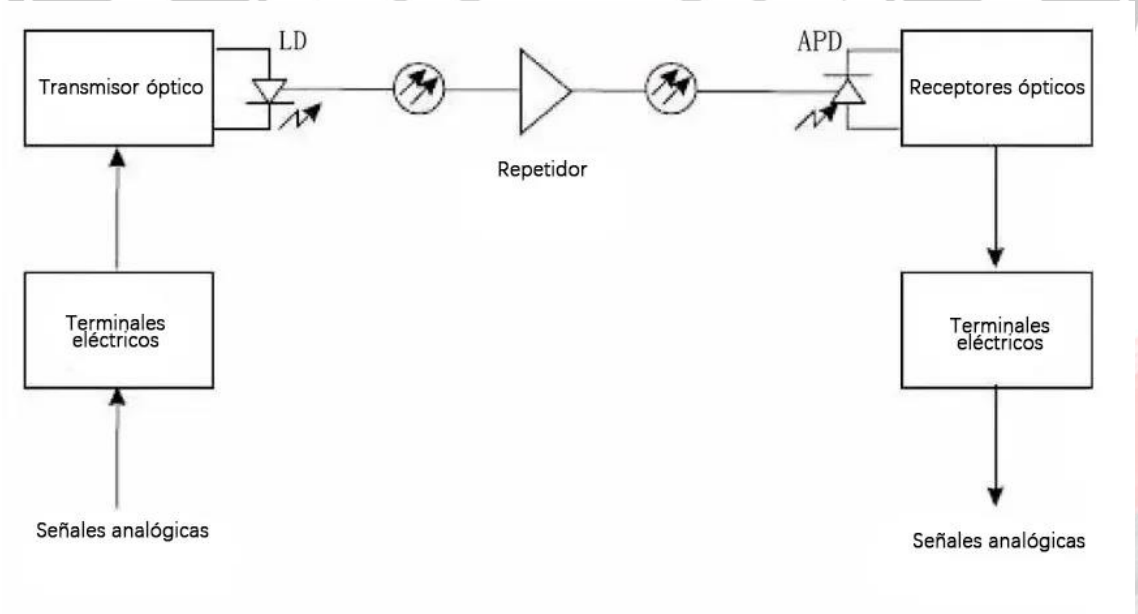
- **Routers y switches:** Son fundamentales en redes informáticas, ya que permiten la transmisión de datos entre dispositivos. Los routers administran el tráfico de datos entre redes diferentes, mientras que los switches facilitan la comunicación dentro de una misma red local (LAN). Los routers modernos pueden incluir funciones de seguridad avanzadas, como firewalls integrados y gestión de calidad de servicio (QoS).



- **Moduladores de señal:** Alteran las características de una señal portadora para su transmisión en diferentes medios. La modulación permite que las señales sean enviadas a través de distintos canales de comunicación sin interferencias. Existen moduladores analógicos y digitales, dependiendo de la aplicación y el tipo de red utilizada.



- **Emisores ópticos:** Utilizan tecnología láser o LED para la transmisión de datos en fibra óptica. Estos dispositivos permiten una velocidad de transmisión significativamente superior a la de los cables de cobre y son resistentes a interferencias electromagnéticas. Son esenciales en infraestructuras de telecomunicaciones de alta velocidad y larga distancia.



- **Antenas transmisoras:** Son esenciales en las telecomunicaciones inalámbricas. Emiten señales electromagnéticas que pueden ser captadas por dispositivos

receptores. Dependiendo de la frecuencia y direccionalidad, las antenas pueden ser omnidireccionales o direccionales. Las antenas de 5G, por ejemplo, utilizan tecnología de beamforming para mejorar la eficiencia de la señal y reducir la interferencia.

6.1.2. DISPOSITIVOS DE RECEPCIÓN

Los dispositivos de recepción interpretan las señales transmitidas y las convierten en información útil para su procesamiento y uso. Estos dispositivos han evolucionado significativamente con el tiempo, permitiendo una mejor calidad y menor latencia en la recepción de datos. Algunos ejemplos incluyen:

- **Receptores de radio y televisión:** Capturan y decodifican señales electromagnéticas para reproducir contenido audiovisual. Hoy en día, los receptores digitales permiten una mayor calidad de imagen y sonido. La tecnología de transmisión de datos por streaming ha complementado la recepción tradicional, permitiendo la visualización de contenido bajo demanda.
- **Módems:** Transforman señales analógicas en digitales y viceversa para la transmisión de datos en redes. Existen diferentes tipos de módems, como los de conexión telefónica, los de cable y los de fibra óptica. Los módems modernos incluyen capacidades de conexión LTE, 5G y Wi-Fi 6 para mejorar la conectividad en diversas condiciones.

- **Receptores ópticos:** Detectan señales luminosas en redes de fibra óptica y las convierten en señales eléctricas procesables. Estos dispositivos son cruciales en la transmisión de datos a gran velocidad y larga distancia. Son utilizados en centros de datos y redes troncales de telecomunicaciones.
- **Antenas receptoras:** Capturan señales electromagnéticas emitidas por transmisores. Dependiendo de la aplicación, pueden ser utilizadas en radio, televisión, telefonía móvil, Wi-Fi y otros sistemas de comunicación inalámbrica. Las antenas de recepción pueden incluir tecnología de cancelación de interferencias para mejorar la calidad de la señal.
- **Decodificadores:** Extraen información de señales transmitidas, como en televisión por cable y satelital. Permiten convertir las señales codificadas en contenido audiovisual accesible para los usuarios. En telecomunicaciones digitales, los decodificadores también pueden incluir soporte para compresión de video como H.264 y H.265.

6.1.3. CABLES Y CONECTORES EN TELECOMUNICACIONES

La infraestructura de telecomunicaciones depende en gran medida de los cables y conectores utilizados para transmitir señales de manera eficiente con la menor pérdida de calidad posible. A lo largo del tiempo, se han desarrollado cables con mejores características de transmisión y menor atenuación de la señal.

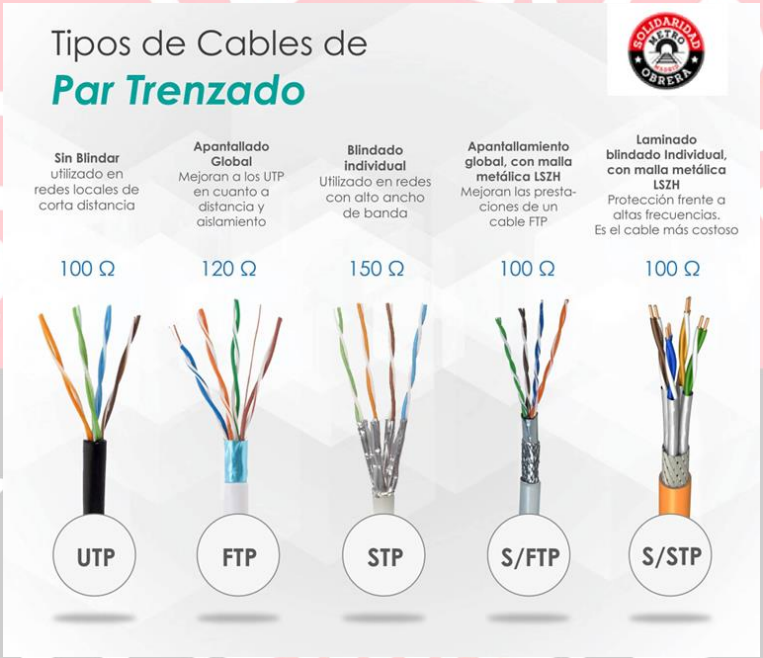
6.1.4. TIPOS DE CABLES EN TELECOMUNICACIONES

Los cables utilizados en telecomunicaciones se pueden clasificar en varias categorías según su medio de transmisión y su aplicación. A continuación, se describen los principales tipos de cables empleados en esta industria:

VER TAMBIÉN 9.1.3. MEDIOS DE TRANSMISIÓN

6.1.4.1. CABLES DE PAR TRENZADO

El cable de par trenzado es uno de los más utilizados en redes de datos y telefonía debido a su flexibilidad, costo accesible y capacidad para reducir la interferencia electromagnética. Su diseño consiste en pares de hilos de cobre entrelazados, lo que minimiza las interferencias externas y la diafonía entre pares adyacentes.



Tipos de cables de par trenzado:

- **Categoría 5e (Cat5e):** Soporta velocidades de hasta 1 Gbps y frecuencias de hasta 100 MHz. Se usa en redes Ethernet de hasta 100 metros.
- **Categoría 6 (Cat6):** Soporta hasta 10 Gbps a distancias menores a 55 metros y trabaja con frecuencias de hasta 250 MHz.
- **Categoría 6a (Cat6a):** Mejora la capacidad del Cat6 al extender la velocidad de 10 Gbps hasta 100 metros y operar en frecuencias de hasta 500 MHz.
- **Categoría 7 (Cat7):** Diseñado para soportar velocidades de hasta 10 Gbps con una mejor protección contra interferencias gracias a su blindaje individual por par y general.

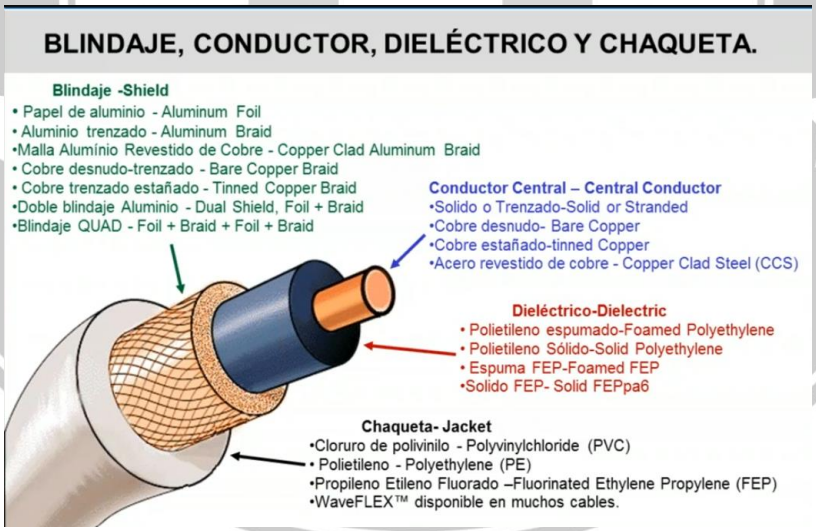
- **Categoría 8 (Cat8):** Utilizado en centros de datos y servidores de alta velocidad, soporta hasta 40 Gbps con una frecuencia de operación de 2000 MHz.

Estos cables son esenciales en redes de área local (LAN) y en aplicaciones de telecomunicaciones que requieren transmisión de datos estable y de alto rendimiento.

Internet Speed Ratio					
Type	Max. Data Rate (Ethernet)	Max. Frequency	Channel Length	Cabling Shielded / unshielded	Connector
Cat.8.1	**40Gbps** (incl. 25 Gbit/s)	**2 GHz**	**30m**	**Shielded**	**RJ45**
Cat.8.2	40Gbps (incl. 25 Gbit/s)	2 GHz	30m	Shielded	Non RJ45
Cat.7	10 GBit/s	600 MHz	100m	Shielded	Non RJ45
Cat.6A	10 GBit/s	500 MHz	100m	Both	RJ45
Cat.6	1 GBit/s	250 MHz	100m	Both	RJ45
Cat.5	1 GBit/s	100 MHz	100m	Both	RJ45

6.1.4.2. CABLES COAXIALES

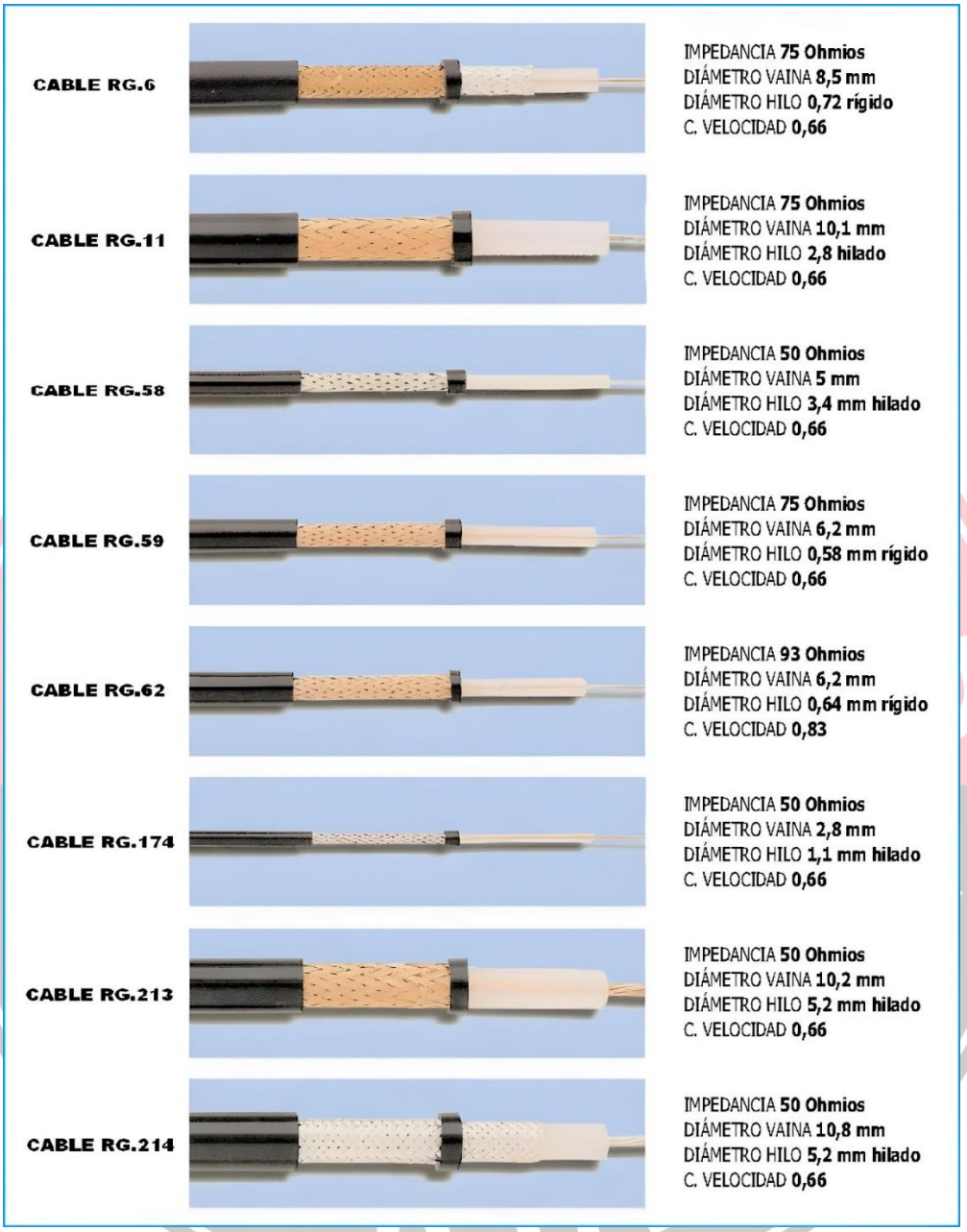
El cable coaxial es ampliamente utilizado en aplicaciones de telecomunicaciones, televisión por cable y sistemas de radiofrecuencia. Su estructura consta de un conductor central, un aislante dieléctrico, una malla conductora y una cubierta protectora externa.



Principales aplicaciones:

- **Televisión por cable y satélite:** Se utiliza para la transmisión de señales de televisión y servicios de Internet de banda ancha.
- **Redes de banda ancha:** Implementado en conexiones de alta velocidad en entornos residenciales y empresariales.

- **Comunicaciones de radio y sistemas CCTV:** Debido a su resistencia a interferencias electromagnéticas, es ideal para la transmisión de señales de radio y vigilancia por circuito cerrado.



Los cables coaxiales más comunes incluyen RG-6 y RG-11 para televisión y RG-58 y RG-59 en aplicaciones de radiofrecuencia.

6.1.4.3. FIBRA ÓPTICA

La fibra óptica es un filamento de **material dieléctrico**, como el vidrio o los polímeros acrílicos, capaz de conducir y transmitir impulsos luminosos de uno a otro de sus extremos. **Estos hilos pueden llegar a ser tan finos como un pelo** y por ellosse **transfiere una señal luminosa desde un extremo del cable hasta el otro**. Esta luz puede ser generada mediante un láser o un LED.

A día de hoy, su empleo más extendido es el de transportar datos a **grandes distancias**, ya que este medio tiene un ancho de banda mucho mayor que los cables metálicos, menores pérdidas y ofrece mayores velocidades de trasmisión. Además, es **inmune a las interferencias electromagnéticas.**

Gracias a estas cualidades, la fibra óptica se utiliza para la **transmisión de comunicaciones telefónicas, de televisión**, etc., a gran velocidad y distancia, sin necesidad de utilizar señales eléctricas, solamente señales de luz. Pero tiene más aplicaciones.

EL CABLE DE FIBRA ÓPTICA

Empecemos por el elemento clave de este avance que es el **cable de fibra óptica** y que consta de las siguientes partes:

- **Núcleo**: Es el elemento central de un cable de fibra óptica que no siempre está presente. Su función es simplemente la de **proporcionar un refuerzo** para evitar la rotura y deformación del cable.
- **Drenaje de humedad**: Este elemento tampoco está presente en todos los cables. Su función es la de **conducir posible humedad** que tenga el cable p**ara que salga a través de él**. Va enrollado en el núcleo.
- **Hilos de fibra**: es el elemento conductor, por ellos **viaja la luz y los datos en ella**. Están fabricados de **cristal de silicio** o **plástico de extrema calidad** que crean un medio en el que la luz pueda reflejarse y refractarse correctamente hasta llegar al destino.
- **Buffer y cladding (revestimiento)**: básicamente es el recubrimiento de los hilos de fibra óptica. Consiste en un **relleno de gel** de capa oscura para **evitar que los rayos de luz no se salgan de la fibra**. A su vez el buffer es el **recubrimiento externo** que contiene el gel y la fibra.
- **Cinta de Mylar y capas aislantes**: es un recubrimiento aislante que envuelve todos los buffers de fibra. En función del tipo de construcción tendrá varios elementos, todos ellos de **material dieléctrico** (no conductor).
- **Recubrimiento ignífugo**: si el cable es **resistente al fuego**, también necesitará un recubrimiento capaz de soportar las llamas.
- **Armadura**: la siguiente capa se trata de la armadura del cable, que en los de mayor calidad siempre están construida de **hilos de Kevlar**. Este material es liviano y de gran resistencia e ignífugo, lo podremos ver en chalecos antibala y cascos de pilotos.
- **Recubrimiento exterior:** como cualquier cable, se necesita un recubrimiento exterior, normalmente de plástico o PVC.

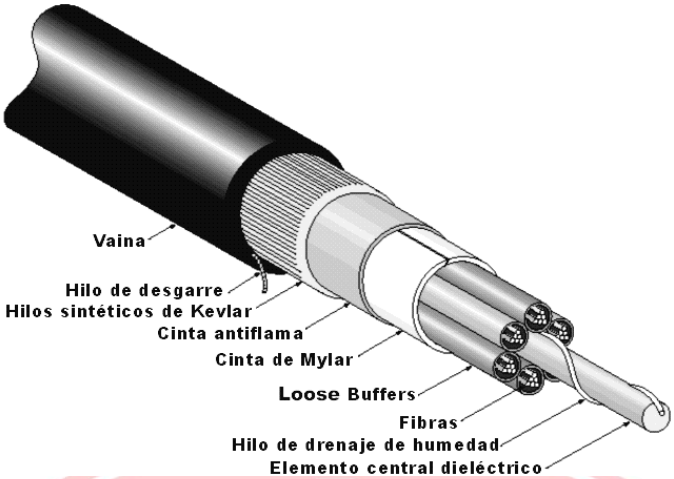


Imagen de los componentes de un cable de fibra óptica.

A grandes rasgos, podríamos resumir que el **cable de fibra óptica** tiene tres componentes principales: **núcleo o core, revestimiento o cladding y recubrimiento o coating.** La luz viaja a través del núcleo, el cual está envuelto por un revestimiento que evita la dispersión de la luz. El recubrimiento actúa de protección contra el deterioro y la humedad.

CÓMO FUNCIONA LA FIBRA ÓPTICA

Para entender cómo funciona la fibra óptica recurramos a la física. Al ser **cables por los que viaja una señal luminosa**, el modo de trasmisión no se basa en la transferencia de electrones a través de un material conductor, sino en los fenómenos físicos de la **reflexión y refracción de la luz.** Mediante ellos, la luz se irá transmitiendo a lo largo de cable de fibra hasta llegar a su destino.

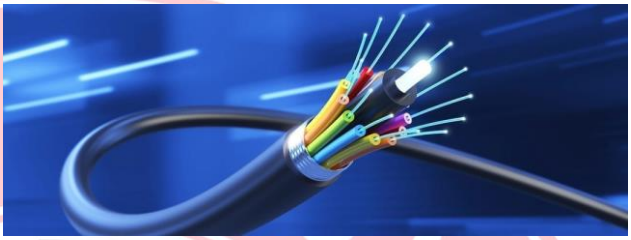
La reflexión de un haz de luz se produce cuando **éste incide sobre una superficie de separación de dos medios y se produce el cambio de dirección de la onda** que la lleva a tomar una dirección con un ángulo igual al de incidencia. Por ejemplo, si el haz luminoso incide en un ángulo de 90 grados sobre una superficie, este rebotará en dirección contraria, esto es lo que pasa cuando nos colocamos frente a un espejo. Si en otro caso el haz de luz incide sobre una superficie con 30 grados, el haz saldrá rebotado con esos mismo 30 grados.

La fibra óptica es un conductor de luz y su funcionamiento se basa en dos fenómenos físicos: la reflexión y la refracción

El otro fenómeno asociado es la **refracción**. Es cuando se produce un cambio de dirección y velocidad en una onda al pasar de un medio a otro. Por ejemplo, es lo que vemos cuando la luz pasa del aire al agua, veremos la misma imagen, pero en un ángulo diferente. O como cuando se sumerge un lápiz en un vaso con agua y el lapicero parece roto.

Explicado con otras palabras, **la fibra óptica no es más que un conductor de luz**. La luz queda atrapada en este conducto y se propaga a la máxima velocidad posible a lo largo del mismo. La velocidad de propagación de la luz depende del tipo de material transparente empleado, ya que **la máxima velocidad c = 299.792.458 m/s sólo se alcanza en el vacío**. En el resto de los medios la propagación se produce a menor velocidad, la relación entre la velocidad de la luz en el vacío y en otro medio, se conoce como índice de refracción del medio y es característico de cada material.

El motivo físico por el cual la luz queda atrapada dentro del conducto se basa en las **leyes de reflexión y refracción de la luz**, según las cuales, cuando un rayo atraviesa la frontera desde un medio físico transparente a otro también transparente, pero donde la velocidad de propagación es menor, la trayectoria del mismo varía, siguiendo una ley física conocida como Ley de Snell.



Más concretamente el fenómeno óptico en el que se fundamenta la transmisión de la luz en el conducto de fibra de vidrio se denomina **Reflexión Interna Total (TIR:Total Internal Reflection)**, según el cual, cuando un rayo de luz pasa de un medio hacia otro con menor índice de refracción, si incide sobre la frontera de los materiales con un ángulo determinado, no pasa ninguna luz a través de la frontera del material. El ángulo a partir del cual el rayo de luz queda totalmente atrapado se denomina **ángulo crítico de incidencia**.

Además de los cables, debemos tener en cuenta que un sistema de transmisión óptico consta de varios componentes esenciales: la fuente de luz, el medio de transmisión y el detector. En este sentido, el medio de transmisión es la propia fibra de vidrio, la fuente de luz suele ser un láser que ilumina el núcleo, y el receptor es un elemento fotosensible. **La información se codifica de modo que un pulso de luz indique un 1 y la ausencia del mismo un 0**. Vamos, que la luz se convierte en señales de datos digitales, viaja a lo largo del cable sin "filtrarse" al rebotar en las paredes de vidrio o plástico, que son como un espejo. La estructura del cable también contribuye a evitar que la luz se disperse.

DIFERENCIAS ENTRE LA FIBRA ÓPTICA Y BANDA ANCHA

Uno de los errores más comunes cuando se habla de **banda ancha** es confundirla con fibra óptica. Hay que entender que los servicios de banda ancha son aquellos que permiten, utilizando un terminal específico (ordenador, móvil, televisor, etc.) disponer de una **conexión de datos permanente y de capacidad de transmisión elevada**. Posibilitan el acceso a Internet y suelen comercializarse empaquetados con otros servicios de telecomunicaciones como telefonía fija y/o móvil y televisión.

En otras palabras, el término "banda ancha" describe las **conexiones de alta velocidad** que proporcionan capacidad para transmitir, con calidad suficiente, servicios

de telecomunicaciones como Internet, telefonía, televisión y aplicaciones multimedia. Es decir, **una autopista o red que permite transferir información digital multimedia a gran celeridad**. Y esta carretera no sólo es ADSL o fibra, como se pudiera pensar, también es 4G, 5G u otras redes móviles.

Así pues, banda ancha es una red o carretera que permite transmitir datos a gran velocidad y de forma consistente. Una de esas autopistas es la fibra óptica, pero no es la única.

TIPOS DE FIBRA ÓPTICA

Existen diferentes **tipos de fibra óptica** y cada uno tiene sus propias peculiaridades y siglas. Te contamos lo que los distingue.

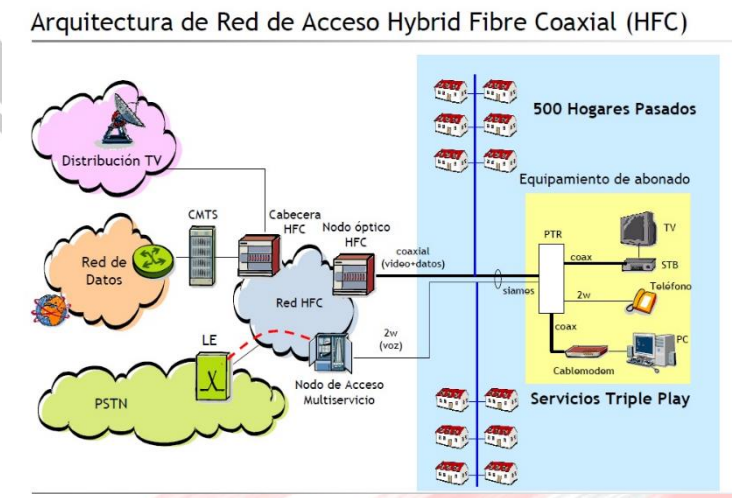
Diferencia entre HFC y FTTH

Las siglas HFC significan híbrido de fibra coaxial, es decir, el último tramo de cable que utiliza es cable coaxial. Es uno de los tipos de cable que pueden emplear las tecnologías FTN, FTC o FTB.

La principal diferencia entre la FTTH y la HFC es la velocidad y estabilidad de la conexión. Ambas utilizan fibra óptica, sin embargo, mientras la FTTH emplea cables de fibra en todo el recorrido hasta el interior de tu hogar, el HFC sustituye los últimos metros desde el nodo por cables coaxiales.

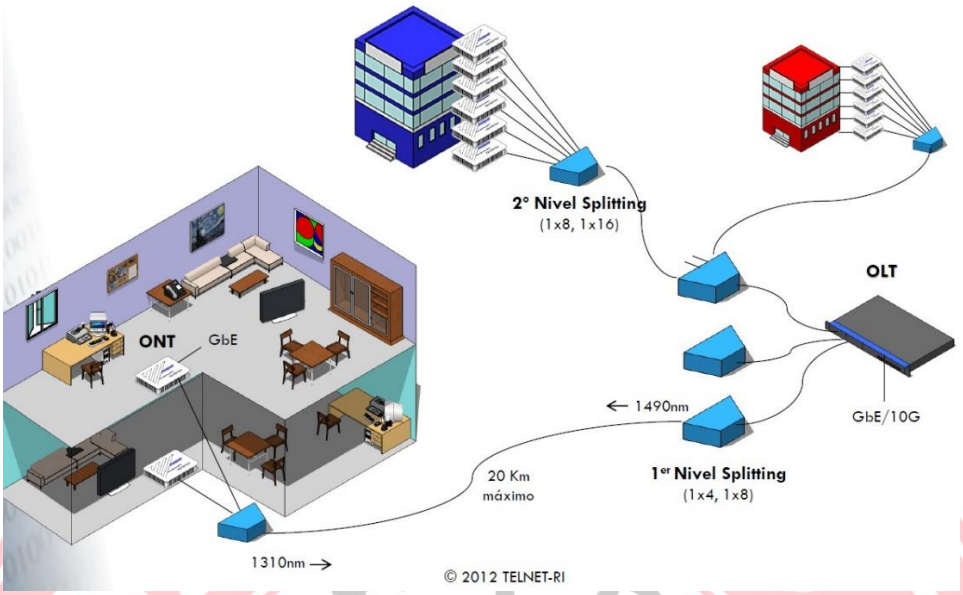
- **HFC**

HFC son las siglas de **Hybrid Fiber Coaxial** o Híbrido de Fibra-Coaxial o fibra óptica híbrida. Se trata de una modalidad híbrida de **fibra óptica** y **cable coaxial** y el cable que nos llega al router de casa es como el de una antena de televisión. Por lo tanto, esto no es fibra óptica pura, pero conviene saber de su existencia.



Arquitectura de la red HFC convencional, con uso del "par siamés"

- **FTTx:**



Arquitectura de una red FTTH, basada en el estándar GPON

Dentro de las tecnologías **FTTx** (Fiber To The…) podemos añadirles diferentes terminaciones o coletillas en función del destino final del cable. Así contamos con:

- **FTTH:** son las siglas, en inglés, de **Fiber To The Home o fibra hasta el hogar**. En este caso la conexión de fibra óptica comienza en la oficina central del operador de telecomunicaciones y nos llega directamente hasta el router de casa.
- **FTTB: Fibra hasta el edificio** oFiber to the building hace referencia al lugar al que llega el internet desde el punto inicial. Conecta principalmente la señal óptica a la caja de distribución principal del edificio de oficinas o edificio de apartamentos para realizar el acceso a la señal de fibra óptica.
- **FTTO: la fibra hasta la oficina.** La diferencia con FTTH se basa simplemente en los servicios ofrecidos por el proveedor, que están más orientados a un uso empresarial. Al igual que en FTTH, al cliente sólo se le deja una ONT (o dos, si contrata servicios de alta disponibilidad), y la distribución hasta los usuarios se hace con una red LAN, normalmente empleando Ethernet.
- **FTTC: Fibra hasta la cabina.** Hace alusión al empleo de fibra desde la central de la red del operador hasta un nodo intermedio como un pedestal o una central pequeña que da servicio a varias manzanas, el resto del trayecto habitualmente se emplea el par de cobre de telefonía o cable coaxial, que en este último caso también se conoce como HFC y se emplea tecnología DOCSIS. En otros términos, el cable de fibra cubre el tramo desde la oficina central hasta el armario de la calle, mientras que la conexión final desde el armario hasta el hogar utiliza cables de cobre.

- **FTTT: Fibra hasta la torre FTTT.** En este caso la conexión de fibra óptica enlaza la red primaria de telecomunicaciones con las torres de la red móvil.
- **FTTA: fiber to the antenna.** Es una arquitectura inalámbrica donde la fibra óptica se distribuye hasta la parte superior de la torre, de modo que sustituye gran parte de lo que, tradicionalmente, se solía completar con cableado coaxial más pesado.
- **FTTR: Fiber to the Room.** Se aplica especialmente a sectores concretos como hotelero, hospitalario, y otros como las residencias de mayores, centros de día, residencias universitarias, centros de formación y terapia ocupacional, etc. Consiste en llevar la conexión por fibra hasta la habitación, donde los usuarios van a usar la red principalmente para acceder a Internet. Debido a una cuestión de eficiencia en costes de servicio, en realidad el operador lleva la fibra hasta el edificio y es el cliente (hotel, hospital, etc.) quien despliega su red desde el RITI o sala de comunicaciones, hasta cada habitación.
- **FTTD:** Fibra hasta el escritorio. Muy similar al término anterior, pero aplicando a empresas, donde la densidad de puntos de terminación de red es mucho mayor, el uso de la conectividad es más intensivo en horas punta, el empleo de la red va mucho más allá de simple acceso a Internet. Además, en FTTD se requerirá el soporte de tecnología empresarial.
- **FTTM: Fiber to the Machine**. El concepto es similar a FTTR y FTTD, pero orientado a la Industria 4.0. La principal diferencia es que la tecnología de fibra se usa para proporcionar conectividad a las máquinas, lo que exige que los equipos que llevan la fibra en el último tramo estén rugerizados, tengan un determinado grado de protección IP, o cumplan directiva ATEX según el caso.
- **FTTN: Fibra óptica hasta el nodo** y se refiere al empleo de fibra desde la central principal de la red del operador hasta un nodo intermedio, es decir, una central secundaria del operador. Se puede considerar una central principal la que concentra la conectividad de una región, y las centrales secundarias las desplegadas en pueblos pequeños. Si la ciudad es grande, pueden existir varias centrales principales, y luego varias centrales secundarias por barrios.

Fibra óptica de plástico o de vidrio

Otra diferenciación que podemos hacer a la hora de categorizar la fibra óptica es por el material por el que está fabricado que puede ser **vidrio o cristal de silicio** que tiene un mayor diámetro, es más cara y se utiliza para recorrer distancias importantes. O de **plástico**, que suele ser empleada para la instalación en zonas urbanas y edificios. Así pues, aunque la red de fibra es vidrio, las instalaciones hasta el acceso a Internet a partir de cierto punto serán de fibra de plástico ya que esta última es menos gruesa y más manipulable, además se puede instalar junto con cables eléctricos compartiendo las mismas canalizaciones.

Fibra óptica monomodo y multimodo

Otras de las nociones que aparecen cuando hablamos de fibra óptica es la diferenciación entre monomodo y multimodo. Dentro de estas categorías, las fibras se identifican por sus **diámetros de núcleo y revestimiento expresados en micrones** (la millonésima parte de un metro), por ejemplo, fibra multimodo de 50/125 micrones. **La mayoría de las fibras tienen 125 micrones de diámetro exterior** (un micrón es la millonésima parte de un metro y 125 micrones son 0.005 pulgadas), un poco más que un cabello humano.

- **Fibra multimodo o MMF**

La fibra multimodo hace que **la luz viaje por el núcleo en muchos rayos**, llamados modos. O, dicho de otra manera, puede **transmitir varias señales de luz por un mismo cable**. Tiene un núcleo más grande (casi siempre de 50 o 62.5 micrones) que admite la transmisión de múltiples modos (rayos) de luz. Esta modalidad suele utilizarse con **fuentes LED** a longitudes de onda de 850 y 1300 nm para redes de área local (LAN) más lentas y láseres a 850 (VCSEL) y 1310 nm (láseres Fabry-Pérot) para redes que funcionan a gigabits por segundo o más.

También conocida como MMF, es un tipo de fibra óptica mayormente utilizada en el ámbito de la comunicación en distancias cortas, como por ejemplo en un edificio o un campus. Los enlaces multimodo típicos tienen una velocidad de datos desde los 10 Mbit/s a los 10 Gbit/s en distancias de hasta 600 metros.

- **Fibra monomodo o SMF**

La fibra monomodo tiene un núcleo mucho más pequeño, de sólo unos 9 micrones, por lo que **la luz viaja en un solo rayo (modo)**. Es decir, sólo se transmite un haz luminoso por el medio. Se utiliza para telefonía y CATV con fuentes láser a 1300 y 1550 nm porque tiene menos pérdidas y un ancho de banda prácticamente infinito.

También conocida por las siglas **SMF**, se utiliza para la transmisión a larga distancia. Transmite directamente señales ópticas en horizontal. Funciona a una velocidad de movimiento de 100 M/s o 1 G/s, y la distancia de transmisión puede alcanzar al menos 5 kilómetros.

- **Otras clasificaciones**

Además de estas diferenciaciones se pueden establecer otras categorizaciones de la fibra en función de la **longitud de onda o ventana de trabajo**, la **distribución del índice de refracción** (escalonado y gradual), **método de fabricación** o el **pulido**.

FIBRA ÓPTICA. MONOMODO O MULTIMODO

Es importante comprender las diferencias entre la fibra óptica monomodo y multimodo antes de seleccionar una u otra en el inicio de un proyecto. Sus diferentes características de ancho de banda, reflexión de la luz, emisor de luz, etc. hacen que sea adecuado usar monomodo o multimodo en diferentes situaciones.

Antes de entrar en la comparativa veamos algunos conceptos básicos acerca de la fibra óptica y qué elementos componen un cable de fibra óptica.

CONCEPTOS DE LA LUZ QUE AFECTAN A LA FIBRA ÓPTICA

1- Longitud de onda - Color de la luz.

2- Atenuación - Pérdida de luz.

3- Ancho de banda - Velocidad de transmisión.

4- Reflectancia - Cantidad de luz que rebota en la fibra hacia el emisor.

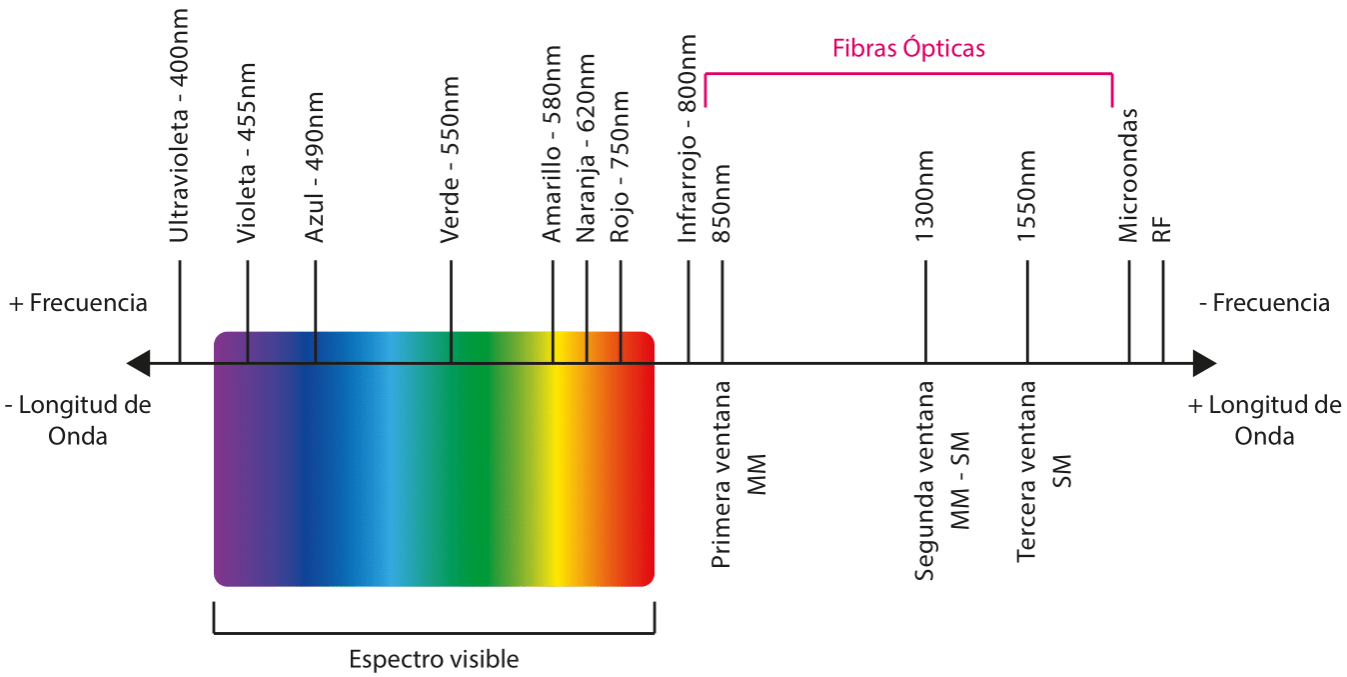
5- Reflexión - Cantidad de luz reflejada en la fibra.

6- Refracción - Cantidad de luz absorbida por el revestimiento de la fibra.

Longitud de onda

En los sistemas de comunicación convencionales (radio o cable) suele utilizarse la frecuencia, mientras que en las comunicaciones ópticas se utiliza la longitud de onda expresada en nanómetros.

Nos referimos a la longitud de onda como el color que tiene la luz, a diferente longitud de onda, distinto color. En el siguiente gráfico vemos como la luz que circula por un cable de fibra óptica está entre 850nm y 1550nm que es luz infrarroja invisible.



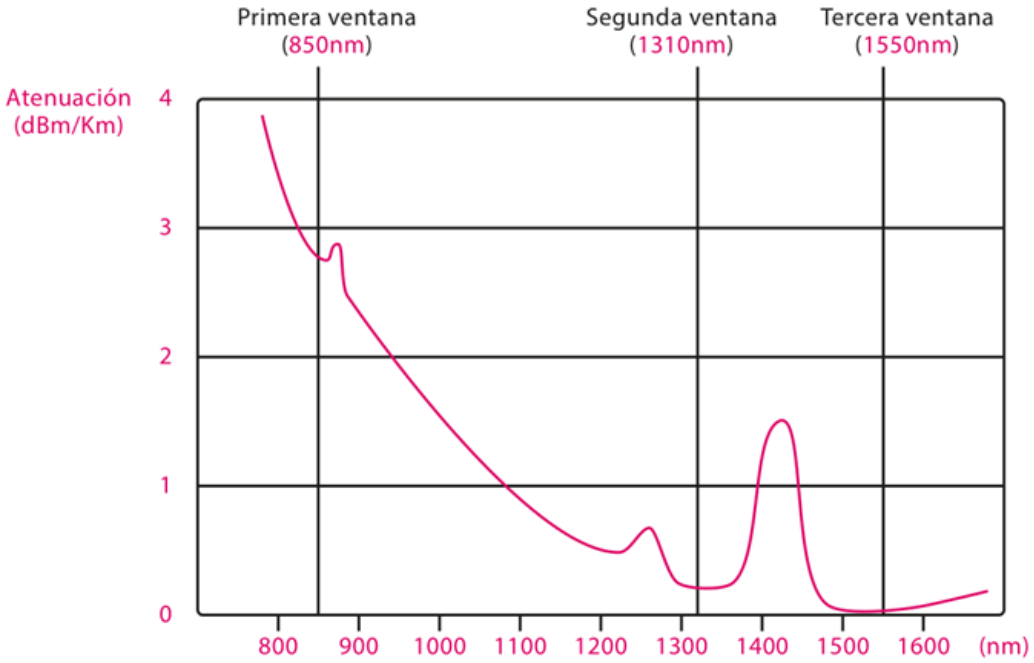
Las comunicaciones ópticas utilizan unas partes del espectro electromagnético que denominamos ventanas que corresponden a determinadas longitudes de onda: 850, 1300 y 1550nm.

Atenuación

Es la pérdida de luz a lo largo del cable expresada en dB/Km. Habitualmente la fibra óptica está hecha de sílice y no refleja de la misma forma todas las longitudes de onda.

Las longitudes de onda que mejor refleja el sílice son 850, 1300 y 1550nm, las que antes hemos denominado como ventanas.

Según la longitud de onda utilizada, la fibra óptica tendrá una cierta capacidad de propagación de la luz, y por tanto una longitud máxima aplicable.



Una atenuación de más de 3dB (lo que significa tener en la salida la mitad de la señal de entrada) no es admisib

Ancho de banda

Es la velocidad a la que se transmite la luz a través de la fibra óptica y se expresa en MHz por km.

Un ancho de banda de 500MHz-km indica que a 500MHz la señal pude ser transmitida una distancia de 1 km.

El ancho de banda para fibras multimodo suele ser de 500Mhz por Km y en las fibras monomodo está en el rango de los GHz, normalmente 100GHz por Km.

El ancho de banda es inversamente proporcional a la distancia.

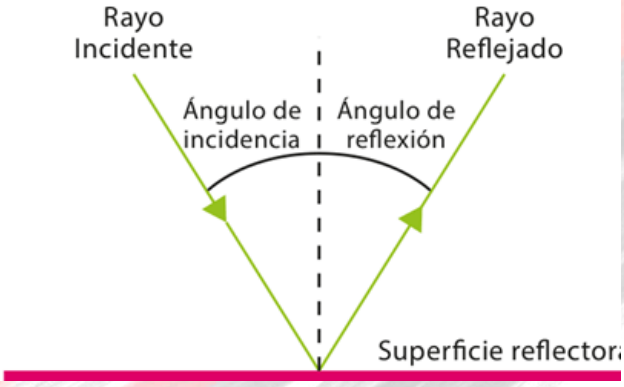
Reflectancia

Al incidir la luz sobre una superficie se genera una reflexión en sentido y ángulo contrario a la luz que incide.

En la fibra óptica, cuando incide el haz de luz, una parte se refleja en el propio material y regresa al emisor.

Por lo tanto si la luz reflejada, es en algún momento superior a la emitida, el emisor quedará cegado.

La reflectancia de la fibra óptica se expresa en dB.



Reflexión y Refracción

Para entender estos dos términos imaginemos un cable de fibra óptica como un túnel completamente redondo con las paredes cubiertas completamente de espejos.

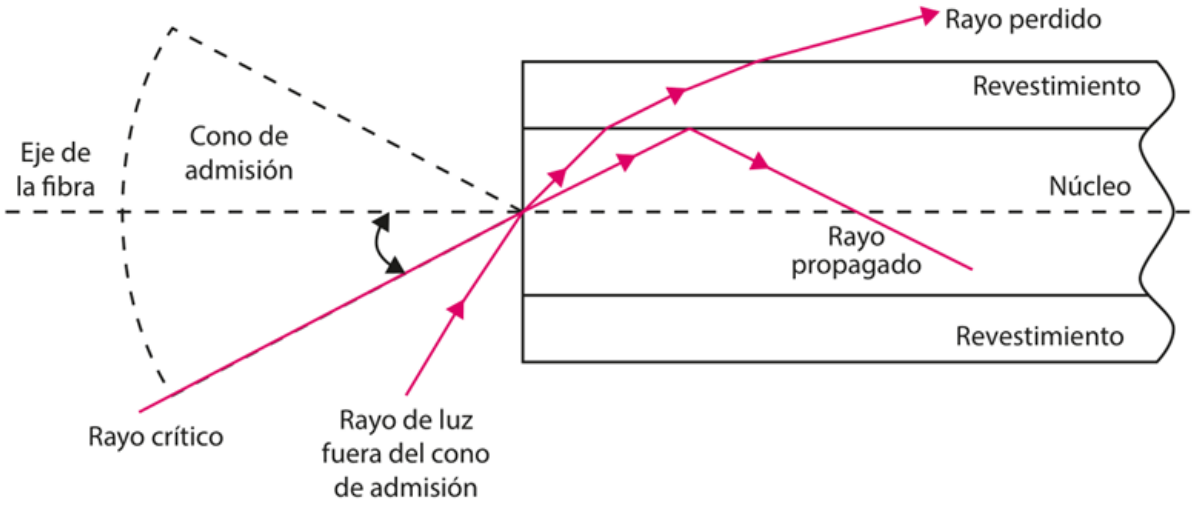
Estos espejos tienen una capacidad de reflexión del 95%, es decir, reflejan solo el 95% de la luz que les incide. El otro 5% es absorbido por el propio espejo, provocando una pérdida por reflexión.

La refracción sería la forma en cómo rebota la luz en el túnel de espejos dependiendo del ángulo con el que incide la luz sobre el espejo. Según la ley de Snell, si el ángulo sobre el que incide la luz es superior a 45º, la luz no se verá reflejada.

Por lo tanto, dependiendo del ángulo de incidencia, se producen pérdidas por refracción. Para que la luz se propague a lo largo de la fibra, tiene que llegar al extremo de la fibra dentro del límite llamado "cono de admisión".

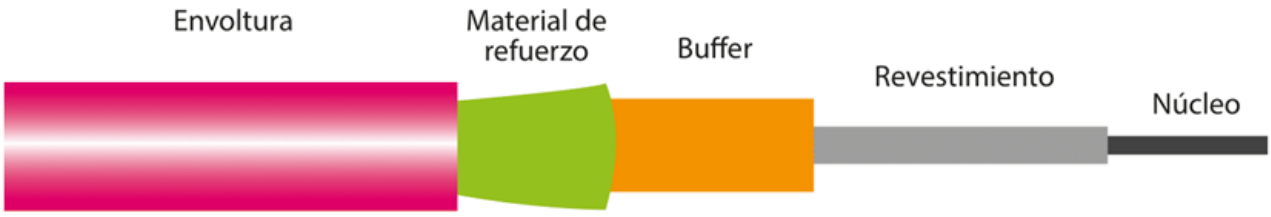
La luz que llega fuera de este cono se pierde en el revestimiento.

La mitad del ángulo del cono de admisión con respecto al eje de la fibra, es el ángulo máximo en el cual los rayos de luz aún son aceptados para la transmisión a través de la fibra. Este ángulo se denomina ángulo de admisión.



Es fundamental realizar los empalmes de fibra lo más rectos posibles y si se usan conectores, que estos sean de la máxima calidad posible con el objetivo de alinear al máximo los dos lados de la fibra.

PARTES DE UN CABLE DE FIBRA ÓPTICA



Núcleo - El centro del cable de fibra óptica es una fina pieza de cristal que proporciona el camino que siguen las señales de luz. El núcleo es muy pequeño en diámetro, tanto en monomodo como multimodo son 125 micras de diámetro exterior. El núcleo es macizo, no es un tubo.

Revestimiento - El núcleo está cubierto o rodeado de material óptico que también está hecho de cristal extremadamente puro al igual que el núcleo.

El trabajo del revestimiento es reflejar las señales de luz de nuevo hacia el núcleo. Al tener un índice de refracción diferente al núcleo, la luz atraviesa el núcleo pero rebota en el revestimiento, de manera que pueda viajar por el núcleo.

Buffer - Generalmente fabricado en plástico que protege mecánicamente a los dos anteriores.

Material de refuerzo - Pueden ser fibras de aramida o poliamida, según el tipo de cable.

Envoltura - Está hecho de poliuretano muy resistente (PVC) y protege los componentes interiores del cable de fibra óptica.

Para aumentar el ancho de banda de un cable de fibra óptica, un mismo cable puede estar formado por diversos buffers, que hacen que el conjunto pueda transportar cantidades muy altas de información (TBytes/segundo).

CONECTORES DE FIBRA ÓPTICA

MONOMODO O MULTIMODO

Monomodo

Es un tipo de fibra, que por su construcción (núcleo muy pequeño), sólo permite el paso de un haz de luz, este haz de luz, no rebota en las paredes, y viaja paralelo a la longitud del cable. Por ese motivo, las pérdidas por reflexión (distorsión modal), son menores, y por tanto la fibra puede ser más larga que en las multimodo.

Multimodo

Es un tipo de fibra, que por su construcción (mayor diámetro del núcleo) permite el paso de más de un haz de luz de diferente longitud de onda, y por tanto permite que varios "modos" de luz puedan entrar y salir de la fibra. Se basa en la reflexión contra sus paredes para la propagación de la luz.

El coste de fabricación de una fibra monomodo es superior por el emisor de luz que se utiliza. Son diodos láser con mayor potencia y direccionalidad que el diodo tipo LED que utiliza la fibra multimodo, que genera una luz más difusa.

Tipos de fibra OM1, OM2, OM3, OM4, OM5, OS1, OS2

El significado de OM, se aplica a la fibra óptica Multimodo (MM - Multi Mode), la numeración hace referencia al tipo de núcleo, distancia máxima, ventana de operación (longitud de onda) y ancho de banda.

Por ejemplo, la OM2 sería una fibra multimodo con un diámetro de núcleo de 50µm, un diámetro del revestimiento de 125µm, distancia máxima 550 m, longitud de onda 850 nm, atenuación máxima 3,5 dB/km y ancho de banda 500 Mhz-Km.

El significado de OS, se aplica a la fibra óptica monomodo (SM - Single Mode).

Por ejemplo, la OS1: sería una fibra monomodo con un diámetro de núcleo de 9µm, un diámetro del revestimiento de 125µm, longitud de onda 1310nm y una atenuación de 0.5 dB/Km.

A mayor número: OM1, OM2, OM3... mayor es la calidad del material y por tanto, mayor transparencia tiene y más lejos puede llegar la luz.

Fibra óptica y tipo de cable	Longitud de onda nm	Atenuación máxima (db/Km)	Ancho de banda modal overfilled (MHz • Km)	Ancho de banda modal efectiva (MHz • Km)
62,5/125µm Multimodo TIA 492AAAA (OM1)	850 1300	3,5 1,5	200 500	No requerido No requerido
50/125µm Multimodo TIA 492AAAB (OM2)	850 1300	3,5 1,5	500 500	No requerido No requerido
850nm Optimizado para láser 50/125µm Multimodo TIA 492AAAC (OM3)	850 1300	3,5 1,5	1500 500	2000 No requerido
850nm Optimizado para láser 50/125µm Multimodo TIA 492AAAD (OM4)	850 1300	3,5 1,5	3500 500	4700 No requerido
Monomodo interior/exterior TIA 492CAAA (OS1) TIA 492CAAB (OS2)	1310 1550	0,5 0,5	N/D N/D	N/D N/D
Monomodo planta interna TIA 492CAAA (OS1) TIA 492CAAB (OS2)	1310 1550	1,0 1,0	N/D N/D	N/D N/D
Monomodo planta externa TIA 492CAAA (OS1) TIA 492CAAB (OS2)	1310 1550	0,5 0,5	N/D N/D	N/D N/D

Comparativa

Especificación	Monomodo	Multimodo
Coste de la fibra	Más barata	Más cara
Equipo de transmisión	Más caro (Diodo láser)	Más barato (LED)
Atenuación	Baja	Alta
Longitud de onda	1260nm a 1640nm	850nm a 1300nm
Instalación	Conexiones más complejas	Núcleo grande, fácil de manejar
Distancia	Redes medias y largas (>200Km)	Redes locales (< 2Km)
Ancho de banda	Grande (>1Tb/s)	Limitado (10Gb/s en corta distancia)

TIPOS DE CONECTORES DE FIBRA Y DE PULIDO EN LA FIBRA ÓPTICA.

Los conectores más usados son los **SC, LC, FC y ST** , y los pulidos más comunes son **PC, UPC y APC**. Cuando compras un cable, vas a ver que tiene una combinación de ambas denominaciones. Por ejemplo un conector SC-APC (SC/APC) tiene conector SC y pulido APC.

Hoy os explicamos todo esto.

Tipos de conectores de fibra.

Los más usados son el SC y el LC, pero os hacemos un resumen de otros (y hay más).

- **Conector FC**: (*Ferrule Connector*) . De los primeros conectores, se usa en instalaciones con movimiento porque resiste bien las vibraciones. También en CATV y en instrumentos de precisión. Se usa en fibras monomodo principalmente aunque hay un modelo para multimodo. Pérdidas de inserción: 0,3 dB aprox. Colores: monomodo con soportes azules, APC con soportes verdes y PC Multimodo con soportes negras

- **Conector ST**: (*Straight Tip*). Se usa en redes corporativas, militares y entornos corporativos. Se usa en fibras multimodo. Pérdidas de inserción 0,25 dB aprox. Colores: monomodo con soportes amarillos, APC con soportes verdes y PC Multimodo con soportes negros o rojos

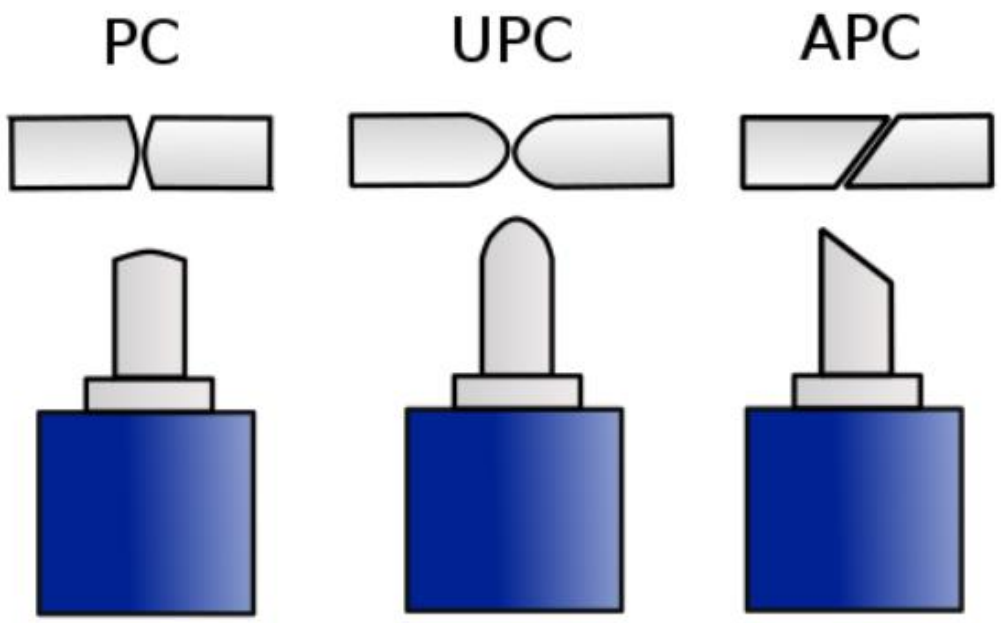
- **Conector LC**: (*Lucent Connector*). Se conecta de manera similar al RJ45 y es más delgado. Así que es perfecto para entornos de red con muchos conectores (racks, FTTH…). Se usa en fibras monomodo y multimodo. Pérdidas de inserción 0,10 dB aprox.
  Colores: azul (Monomodo), verde (Monomodo APC) y beige (Multimodo).

- **Conector SC**: (*Square Connector* o *Suscriptor Connector*). Por ser de bajo coste, es de los más usados. Se conecta rápidamente por presión. Usado en televisión, FTTH, telefonía… En fibras monomodo y multimodo. Pérdidas de inserción de 0,25 dB aprox.
  Colores: azul (Monomodo), verde (Monomodo APC) y beige (Multimodo).

Tipos de pulido.

Esto se refiere a cómo termina la estructura cerámica que contiene la fibra óptica en los diferentes tipos de conectores. Dicha estructura puede tener tres tipos de terminaciones:

- **PC**: Contacto físico (Physical Contact). Tienen una ligera curvatura, reduce el aire entre los conectores. Unas pérdidas de unos -40 dB.
- **UPC**: Contacto ultra físico (Ultra Physical Contact). Tiene forma de cúpula y unas pérdidas de unos -50 dB.
- **APC**: Contacto físico angular (Angled Physical Contact). Pulida a un ángulo de 8 grados, tiene unas pérdidas de -60 dB o mayores.

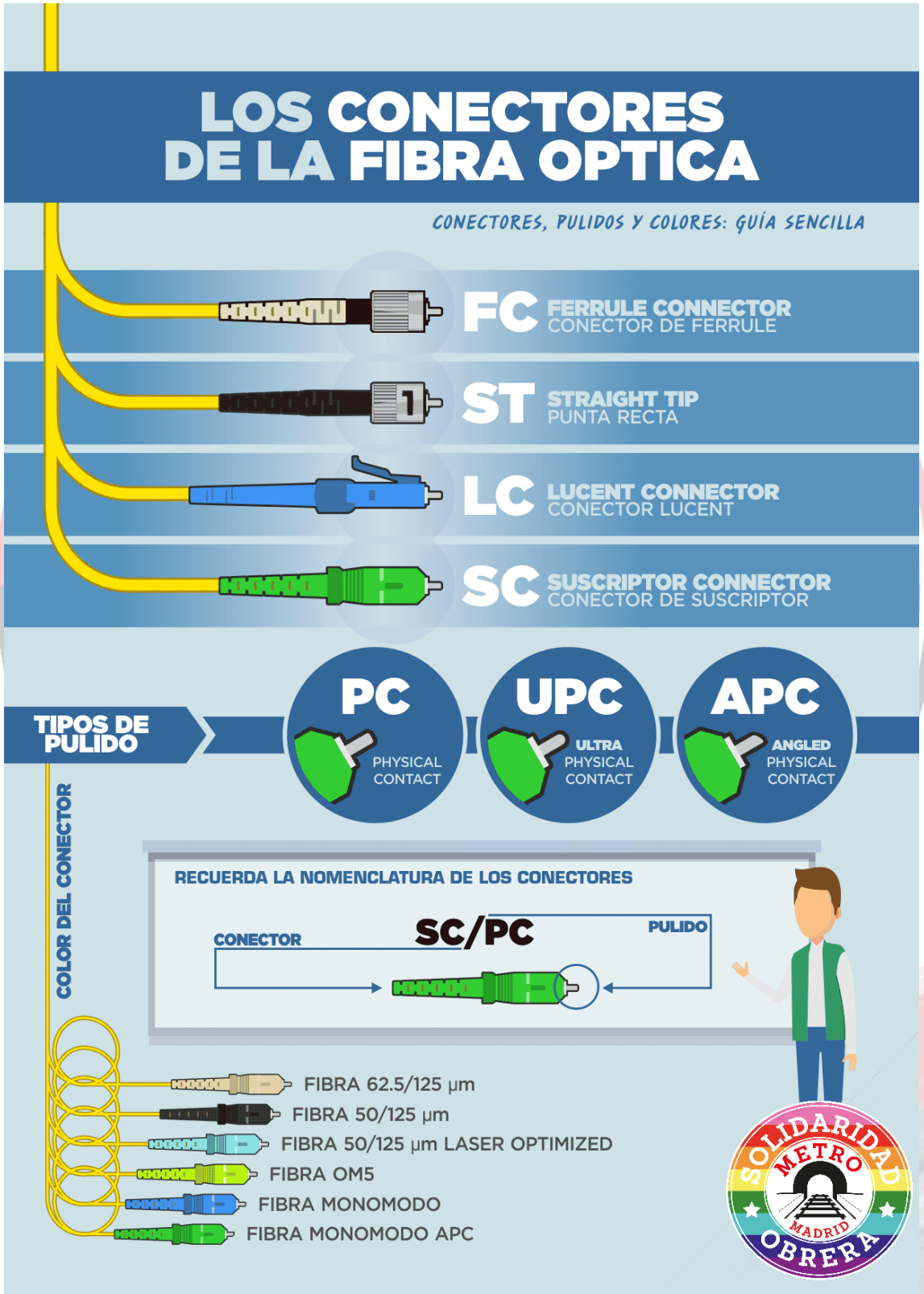


Realmente no hay conectores mejores que otros. Los PC y UPC se usan para Ethernet, telefonía y datos. Los APC son adecuados para sistemas multi-play, por ejemplo CATV, RF etc.
En líneas generales, para aplicaciones de precisión el APC. Para telecomunicaciones, telefonía y televisión PC o UPC.

Notas importantes:

- Los **APC no se pueden usar en módulos SFP y SFP+** (los usados en los aparatos de red como switches), porque los SFP tiene conexión plana y no angulada como los APC.

- **¿Se pueden conectar diferentes pulidos?** En principio **no debería**. Pero al ser UPC y PC planos si que se pueden conectar entre sí o indistintamente en un SFP. No se pueden conectar con APCs.



VENTAJAS DE LA FIBRA ÓPTICA

La fibra óptica ofrece grandes ventajas por eso se ha impuesto como principal tecnología de acceso a Internet en los hogares españoles. Estas sus beneficios principales:

- **Mayor velocidad**

La fibra óptica destaca porque permite la transmisión de datos a gran velocidad. Admiten una **baja atenuación y alta capacidad** para transportar datos de forma que pueden soportar gigabits y servicios simétricos de alta velocidad.

En concreto, las fibras transfieren la información a velocidades muy superiores a las velocidades actuales de DSL o de módem de cable. La misma fibra óptica por la que se proporciona el servicio de banda ancha puede brindar simultáneamente telefonía por Internet (VoIP, por sus siglas en inglés) y servicios de programación audiovisual, incluyendo vídeo a la carta o vídeo on demand. Asimismo, tienen **baja latencia**. Esta rápida transferencia de datos permite implantar, por ejemplo, sistemas de IA de auto-conducción para coches o drones, telemedicina, seguridad nacional o gestionar la seguridad en obras y zonas de trabajo.

La fibra óptica supuso una revolución en las telecomunicaciones, ya que ofrece la posibilidad de enviar multitud de datos y hacerlo además a gran distancia

Con la fibra óptica estamos hablando ya de que algunas operadoras ofertan 1.000 Mbps, es decir, 1 Giga. Pero algunas ya están **trabajando en los 50 Gbps**. Eso no es todo, combinando varias fibras ya se han visto varios proyectos y demos en los que se han alcanzado los **Terabits**.

Respecto a este apartado, hay que introducir otro concepto: la **fibra óptica simétrica**. Esta es la que funciona ofreciendo al usuario la misma velocidad de conexión de bajada que de subida.

- **Mayor ancho de banda**

Esta tecnología ofrece **mayor ancho de banda** que con otro tipo de cables o filamentos alcanzando mayores distancias que los sistemas eléctricos tradicionales y soportando más equipos conectados. Su mayor capacidad de albergar datos significa que **no se sobrecargan** tan fácilmente como las redes de cable de cobre, por lo que es más rápido descargar y transmitir películas u otro contenido en streaming. La estabilidad de la fibra significa también que el videojuego no se interrumpirá.

- **Menos pérdida de señal**

Otra de las ventajas de la fibra óptica frente a otras alternativas de conexión es que permite la transmisión de señales sin pérdidas gracias a que son **inmunes a las**

interferencias electromagnéticas. Y tampoco las produce. Esta característica de la fibra implica que se evitarán los problemas de cortes de conexión, bajadas de velocidad o los cruces de conversaciones telefónicas, etc.

- **Más segura y duradera**

La fibra óptica **soporta muy bien los cambios climáticos y temperaturas** porque es **más duradera frente** a la corrosión o factores externos. Asimismo, **es muy ligera**, al tratarse de elementos no metálicos. Es un cable más liviano pues su peso es ocho veces menor que el de un cable convencional. Estas características la hacen más segura y resiliente ya que las intrusiones son más difíciles de hacer y son fácilmente más detectables.

- **Más ecológica**

La fibra óptica es **más ecológica** que el cable de cobre porque es más eficiente a la hora de transmitir la energía, pudiendo acumular distancias de hasta 150 kilómetros sin necesidad de ningún repetidor. Esto las hace idóneas para la comunicación de alta velocidad entre ciudades o países.

DESVENTAJAS DE LA FIBRA ÓPTICA

A grandes rasgos y como desventaja general de la fibra óptica se podría mencionar que es **más delicada o costosa** si se compara con otras alternativas como el cable coaxial.

En cuanto al coste, no se trata del cable en sí sino más bien el de los **equipos láser** para trabajar con ella, los cuales son mucho más sofisticados que los necesarios para trabajar con hilos de cobre.

Así, fundamentalmente una de sus limitaciones es que los cables deben ser de **gran firmeza y estar muy bien protegidos**, para evitar la rotura de la fibra. Aunque se ha avanzado mucho en mejorar la fragilidad de las fibras con la creación de cables que pueden soportar ser doblados y manejados como cables de cobre sin problemas, siguen siendo delicadas.

Tampoco podemos transmitir electricidad, esto es lógico, así que todo elemento que necesite energía eléctrica deberá tener una fuente de alimentación cercana. Para grandes instalaciones esto significará tener que correr un cable eléctrico paralelo a los cables de fibra óptica para poder alimentar los repetidores o cualquier hub o splitter.

En cuando a la **instalación y empalme de cables de fibra** hay que mencionar que es un proceso bastante complejo y es necesaria gran precisión para que la señal se traslade de un cable a otro sin degradación de la señal.

Paralelamente, **los aparatos de transmisión y recepción también son mucho más caros y complejos**, y en la mayoría de las ocasiones se necesitan aparatos de conversión entre energía eléctrica y luminosa para que llegue a nuestros hogares.

Por último, podemos aludir a la **cobertura de fibra** de los operadores que, aunque se ha avanzado mucho, no llega al cien por cien de la población. Pero, siendo realistas, no llegará nunca porque hay sitios en los que resulta prácticamente imposible desplegarla haciendo zanjas y surcos como ocurre en zonas montañosas y remotas.

APLICACIONES DE LA FIBRA ÓPTICA

La fibra óptica tiene diferentes aplicaciones

- **Telecomunicaciones**

El principal uso de la fibra óptica es el de la transmisión de datos a baja latencia y a muy altas velocidades, y se usa tanto a nivel doméstico para llevar la conexión hasta los routers domésticos, como para conectar diferentes países con cables submarinos.

- **Medicina**

En medicina también tiene su aplicación la fibra óptica para el diagnóstico como endoscopios para observar el interior del cuerpo, utilizando la luz para crear una imagen. Asimismo, los dentistas los utilizan para iluminar la boca durante la cirugía dental.

- **Aplicaciones militares**

Los militares utilizan redes de fibra óptica de alta potencia para los sistemas de control de misiones, el intercambio de datos de alta velocidad y la planificación de vuelos.

- **Uso artístico**

La fibra óptica también tiene un uso artístico. Algunos artistas han visto en ella un original material para crear composiciones lumínicas de gran belleza.

- **Iluminación**

conexiones de audio de alta calidad. Además, también es una **fuente de iluminación para proporcionar** visibilidad en espacios reducidos e incluso para productos de decoración, por ejemplo, en árboles de navidad y cosas similares

- **Otras industrias**

La industria del automóvil utiliza fibras ópticas para iluminar tanto el interior de un coche como sus luces exteriores. También se emplea para llevar a cabo inspecciones en zonas de difícil acceso añadiendo un cable de fibra óptica a una cámara diminuta.

- **La fibra óptica en España**

En España se lleva desplegando fibra muchos años. Una **gran inversión** privada -de pequeños y grandes operadores- y pública -con planes de ayuda del Gobierno que incentivaron la inversión-, permitió hacer grandes instalaciones convirtiendo a nuestro país en una de las regiones del mundo con mayor porcentaje de usuarios conectados por esta vía. Estos esfuerzos han llevado a que el **89,87% de los hogares nuestro país esté**

iluminado por fibra. Y eso a fecha del 30 de junio de 2022, según datos del **Ministerio para la Transformación Digital y de la Función Pública**.

Además, somos pioneros en Europa. De acuerdo con el **Informe de la Década Digital 2023 de la Comisión Europea,** España está a la vanguardia del despliegue de fibra en la UE, situándose 35 puntos por encima de la media comunitaria.

De hecho, el país es líder en adopción de la banda ancha ultrarrápida –principalmente con fibra óptica-; más del 87% de la población con acceso a banda ancha dispone de estas prestaciones (más de 100 Mbps). Igualmente, España ocupa la primera posición entre las grandes economías europeas en **cobertura de redes de muy alta capacidad**: el 93% de los individuos tenían acceso a redes fijas de muy altas capacidades (más de 100 Mbps), 20 puntos más que la media de la UE.

España también es pionera en otro aspecto: en 1986 entró en servicio uno de los **primeros cables ópticos submarinos del mundo**, este conectaba Las Palmas de Gran Canaria y Candelaria, Tenerife.

6.2. MODULACIÓN Y DEMODULACIÓN DE SEÑALES

La modulación y demodulación son procesos fundamentales en los sistemas de telecomunicaciones, permitiendo la transmisión eficiente y confiable de señales a través de distintos medios, como el aire, cables de cobre o fibra óptica. Estos procesos son esenciales para garantizar que la información pueda ser transportada a largas distancias sin pérdidas significativas ni interferencias que degraden la calidad de la señal.

La **modulación** es el proceso mediante el cual una señal portadora, de alta frecuencia y características conocidas, es modificada en función de la señal de información o señal moduladora. Esto permite adaptar la señal de información para su transmisión a través del canal de comunicación seleccionado.

Por otro lado, la **demodulación** es el proceso inverso, donde se extrae la señal original contenida en la señal modulada, recuperando la información transmitida.

6.2.1. TIPOS DE MODULACIÓN

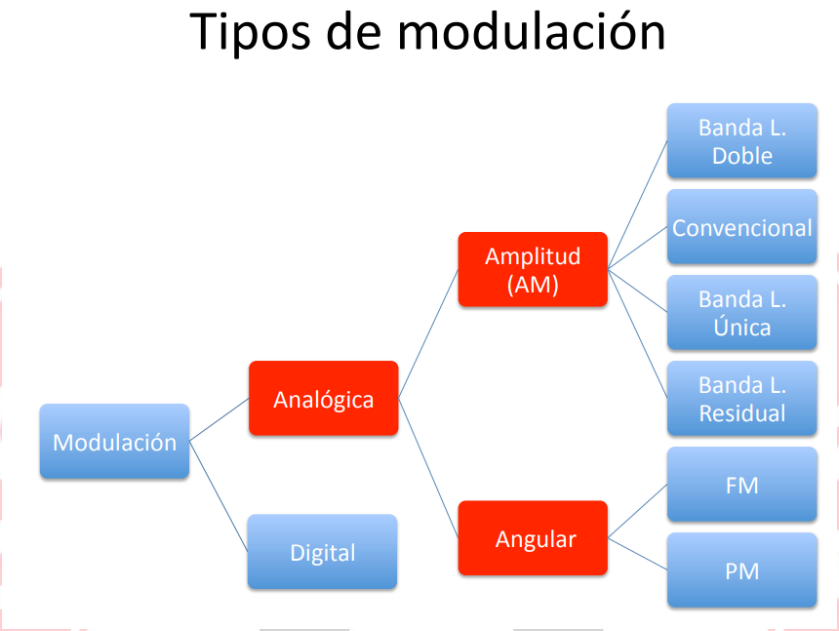
¿Qué es la Modulación?

La modulación es el proceso mediante el cual se modifica una señal portadora (que es una onda de alta frecuencia) con el fin de que transporte la información de la señal de mensaje o señal modulante. La señal portadora es generalmente una onda sinusoidal

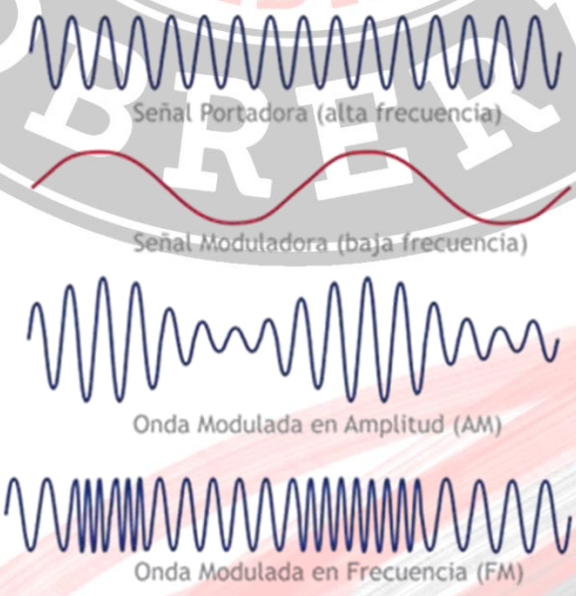
que se altera en uno o más de sus parámetros (amplitud, frecuencia o fase) según la información que se desee transmitir.

Existen diferentes tipos de modulación, los cuales se clasifican en dos grandes categorías: **modulación analógica** y **modulación digital**.

6.2.1.1. MODULACIÓN ANALÓGICA



La modulación es un proceso fundamental en el ámbito de las telecomunicaciones, siendo esencial para la transmisión de señales de información a través de distintos medios, ya sea el aire, cables o fibra óptica. En este artículo, nos centraremos en dos de las técnicas de modulación más comunes: la Modulación de Amplitud (AM) y la Modulación de Frecuencia (FM), explorando cómo funcionan, sus aplicaciones, y las diferencias entre ambas.



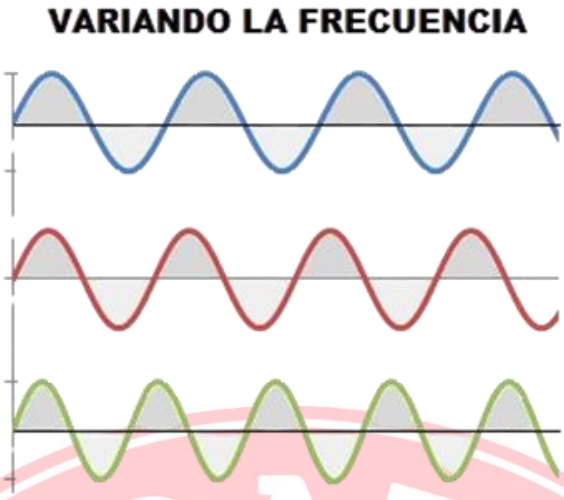
Modulación de Amplitud (AM):

La Modulación de Amplitud (AM, por sus siglas en inglés) es una técnica en la que la amplitud de la señal portadora varía en proporción a la amplitud de la señal modulante (la señal de información). A continuación, te explico cómo funciona:

1. **Señal Portadora y Señal Modulante**: En AM, la señal portadora tiene una frecuencia constante. La señal modulante, que contiene la información (por ejemplo, audio), modula la amplitud de esta portadora.
2. **Proceso de Modulación**: La amplitud de la señal portadora aumenta o disminuye en función de la señal modulante. Si la amplitud de la señal modulante es mayor, la amplitud de la portadora aumentará, y si es menor, la amplitud de la portadora disminuirá.
3. **Aplicaciones de AM**: La modulación AM es ampliamente utilizada en la radiodifusión de radio de onda media (AM radio), donde la transmisión de voz es suficiente, y la calidad del sonido no es tan crítica como en otros servicios.
4. **Ventajas y Desventajas**: La principal ventaja de AM es su simplicidad. Sin embargo, es más susceptible a interferencias y ruido, ya que cualquier variación en la amplitud de la señal debido al ruido afecta directamente la información transmitida.

Modulación de Frecuencia (FM):

La Modulación de Frecuencia (FM, por sus siglas en inglés) es una técnica en la que la frecuencia de la señal portadora varía en función de la amplitud de la señal modulante. Veamos cómo se realiza:



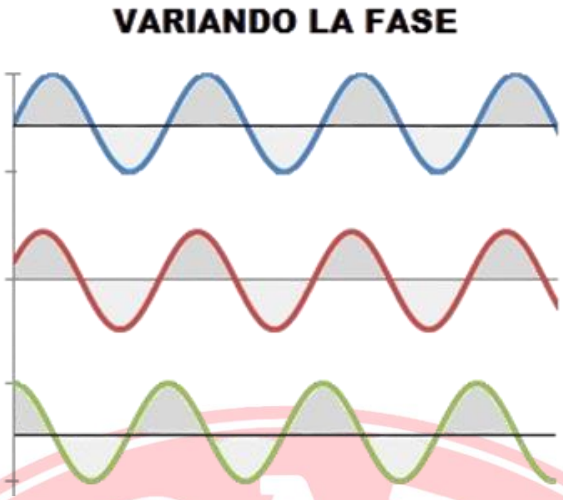
1. **Señal Portadora y Señal Modulante**: En FM, la señal portadora tiene una amplitud constante, pero su frecuencia cambia dependiendo de la señal modulante.
2. **Proceso de Modulación**: Cuando la amplitud de la señal modulante aumenta, la frecuencia de la portadora aumenta. De manera inversa, cuando la amplitud de la señal modulante disminuye, la frecuencia de la portadora también disminuye.
3. **Aplicaciones de FM**: La modulación FM se utiliza principalmente en la transmisión de radio de alta calidad (FM radio), televisión y otros servicios que requieren una mejor calidad de sonido y menos susceptibilidad al ruido.
4. **Ventajas y Desventajas**: FM es menos propensa a interferencias y ruido en comparación con AM, ya que el ruido afecta principalmente la amplitud de la señal y no su frecuencia. Sin embargo, FM ocupa un ancho de banda mayor y es más compleja de implementar.

Además de la Modulación de Amplitud (AM) y la Modulación de Frecuencia (FM), existen varios otros tipos de modulación que se utilizan en diferentes aplicaciones de telecomunicaciones. A continuación, te presento algunos de los más comunes:

Modulación de Fase (PM)

• **Descripción**: En la Modulación de Fase (PM), la fase de la señal portadora se varía en función de la señal modulante. A diferencia de AM y FM, en PM ni la amplitud ni la frecuencia de la portadora cambian, sino que es la fase la que se ajusta para transportar la información.

• **Aplicaciones**: Se usa en aplicaciones como la transmisión de datos digitales y en la tecnología de radar, en sistemas de comunicaciones satelitales y tecnologías como Bluetooth.

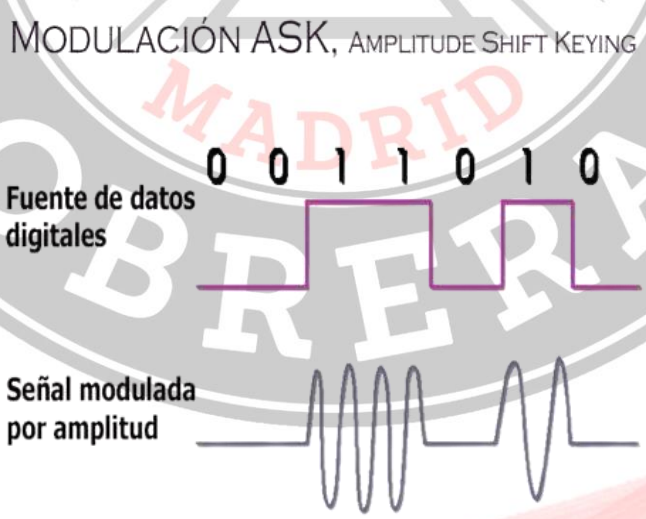


6.2.1.2. MODULACIÓN DIGITAL

La modulación digital es ampliamente utilizada en los sistemas de telecomunicaciones modernos, ya que permite la transmisión eficiente y confiable de datos a través de diferentes medios. A diferencia de la modulación analógica, en la modulación digital, la señal de información es discreta (binaria), lo que significa que se representa mediante una serie de bits (0 y 1). Esta característica permite una mayor robustez frente al ruido y la interferencia, así como una mejor utilización del ancho de banda disponible.

TIPOS DE MODULACIÓN DIGITAL

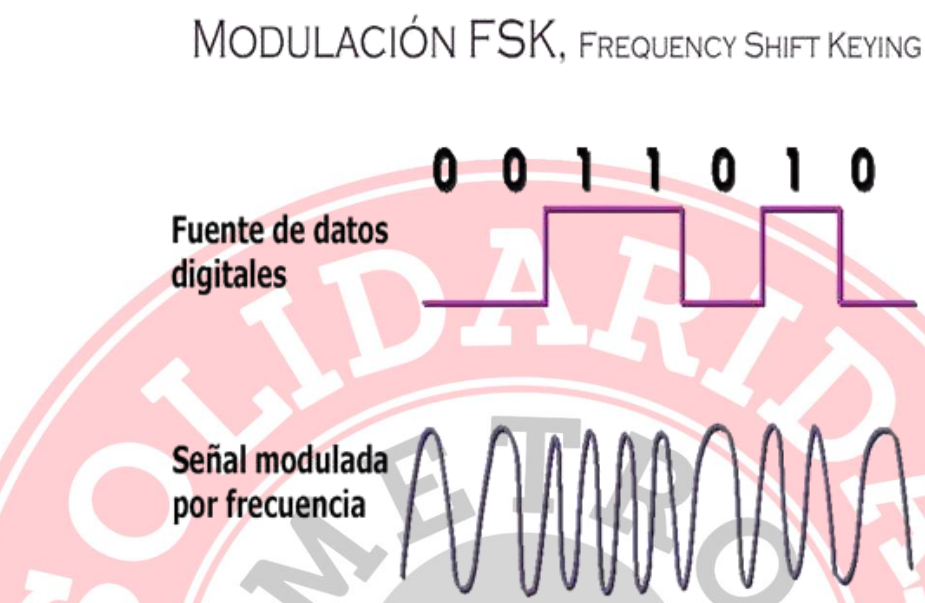
- **MODULACIÓN POR DESPLAZAMIENTO DE AMPLITUD (ASK, AMPLITUDE SHIFT KEYING):**



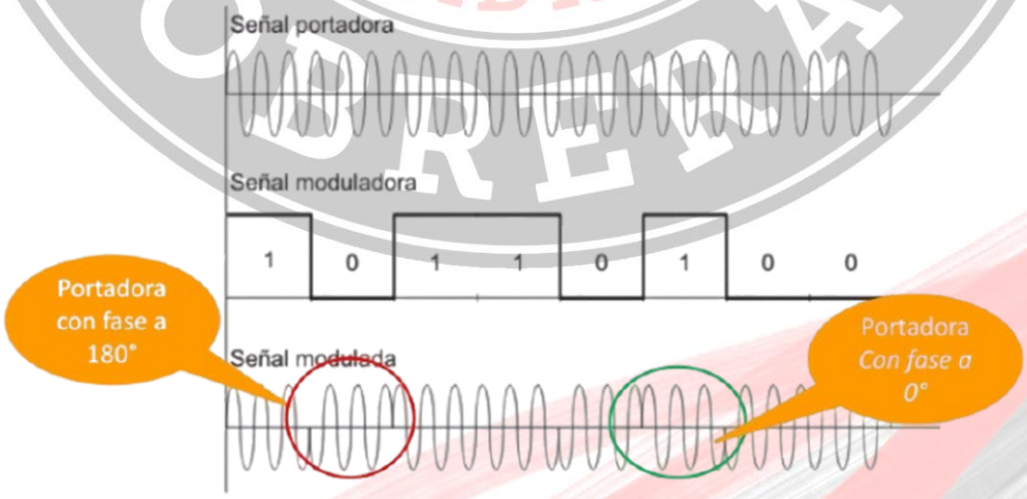
- En ASK, la amplitud de la señal portadora cambia en función de los datos digitales transmitidos.
- Un nivel de amplitud representa un bit '1' y otro nivel de amplitud representa un bit '0'.

- Es un método sencillo y fácil de implementar, pero es altamente susceptible al ruido y las interferencias.
- Se usa en aplicaciones de comunicación óptica y algunos sistemas RFID.

- **MODULACIÓN POR DESPLAZAMIENTO DE FRECUENCIA (FSK, FREQUENCY SHIFT KEYING):**



- La frecuencia de la señal portadora cambia en función de los datos digitales transmitidos.
- Un bit '1' se representa con una frecuencia y un bit '0' con otra frecuencia.
- Es menos susceptible al ruido que ASK, pero requiere mayor ancho de banda.
- Se utiliza en comunicaciones inalámbricas, módems y sistemas de radio digital.



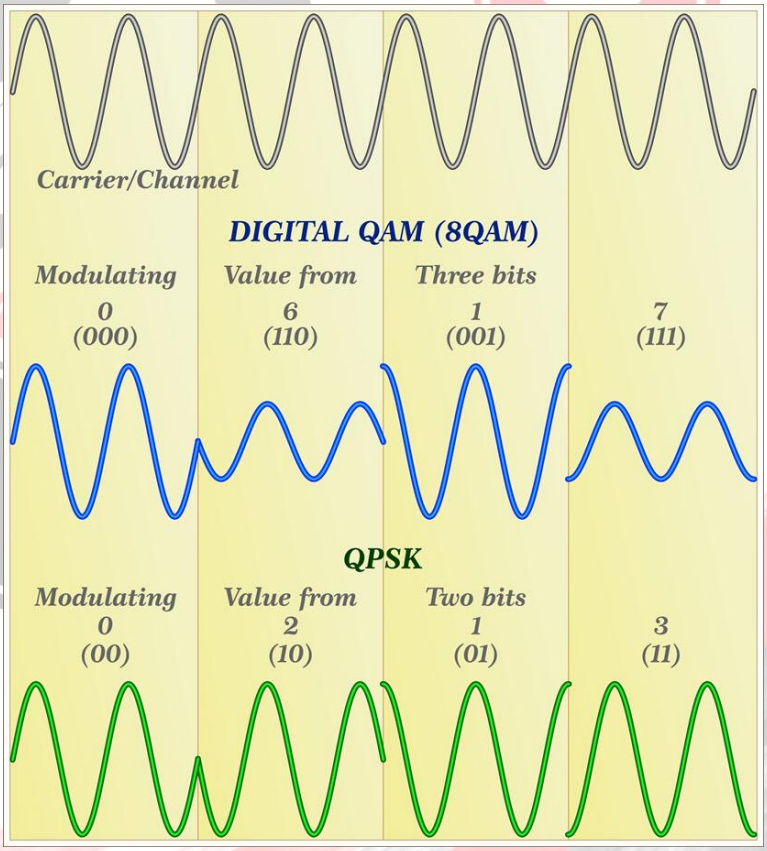
- **MODULACIÓN POR DESPLAZAMIENTO DE FASE (PSK, PHASE SHIFT KEYING):**

  - La fase de la señal portadora se modifica en función de los bits transmitidos.
  - Es más robusta frente al ruido y más eficiente en términos de ancho de banda en comparación con ASK y FSK.
  - Algunas variantes de PSK incluyen:

    - **BPSK (Binary Phase Shift Keying)**: Utiliza dos estados de fase para representar 0 y 1.
    - **QPSK (Quadrature Phase Shift Keying)**: Usa cuatro fases diferentes para representar dos bits por símbolo, aumentando la eficiencia del ancho de banda.
    - **8-PSK, 16-PSK y versiones superiores**: Utilizan múltiples estados de fase para transmitir más bits por símbolo, pero son más sensibles al ruido.

- **MODULACIÓN DE AMPLITUD EN CUADRATURA (QAM, QUADRATURE AMPLITUDE MODULATION**

  - Combina la modulación de amplitud y fase para transmitir múltiples bits por símbolo.
  - Se pueden usar diferentes niveles, como 16-QAM, 64-QAM y 256-QAM, para aumentar la eficiencia espectral.
  - Es ampliamente utilizada en sistemas de televisión digital, Wi-Fi, LTE y otras aplicaciones de banda ancha.



Ventajas de la Modulación Digital

- Mayor inmunidad al ruido y las interferencias en comparación con la modulación analógica.
- Uso eficiente del espectro mediante técnicas avanzadas de codificación y multiplexación.
- Facilidad para la encriptación y el procesamiento digital de señales.
- Permite el uso de técnicas de corrección de errores para mejorar la calidad de la comunicación.

Aplicaciones de la Modulación Digital

- **Telefonía móvil (2G, 3G, 4G, 5G)**: Utiliza técnicas avanzadas de PSK y QAM para mejorar la velocidad de transmisión de datos.
- **Wi-Fi y Bluetooth**: Emplean variantes de FSK, PSK y QAM para garantizar una comunicación confiable y de alta velocidad.
- **Televisión digital y radio satelital**: Utilizan QAM y PSK para mejorar la calidad de transmisión.
- **Redes ópticas**: ASK y QAM se usan en comunicaciones ópticas de alta velocidad para maximizar la eficiencia del ancho de banda.

6.2.2. PROCESO DE DEMODULACIÓN

El término demodulación1 engloba el conjunto de técnicas utilizadas para recuperar la información transportada por una onda portadora, que en el extremo transmisor fue modulada con dicha información.

En telecomunicaciones, este término es el opuesto a modulación. Así, en cualquier telecomunicación normalmente existirá al menos una pareja modulador-demodulador (módem), uno en cada extremo de la comunicación.

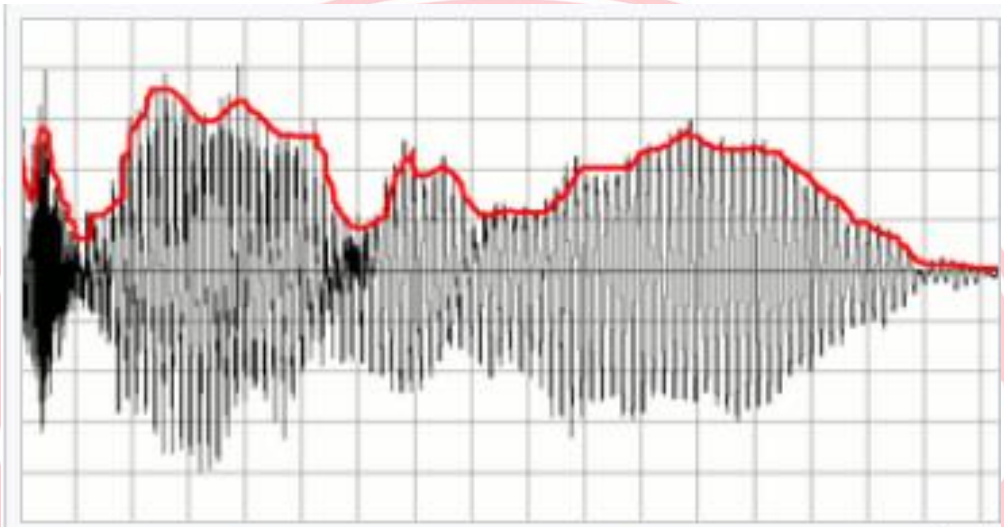
El diseño del demodulador dependerá del tipo de modulación empleado en el extremo transmisor.

6.2.2.1. DEMODULACIÓN DE SEÑALES ANALÓGICAS

Demodulación de AM (Modulación en Amplitud):

Una señal AM codifica la información en la onda portadora variando su amplitud a la vez que la señal analógica para ser enviada. Hay dos métodos utilizados para demodular las señales de AM:

El **detector de envolvente** es un método muy sencillo de desmodulación. Muchas sustancias naturales exhiben este comportamiento de rectificación, razón por la cual fue la primera técnica de modulación y desmodulación utilizada en la radio. Consta de un rectificador (cualquier cosa que pueda pasar en una sola dirección) y un filtro pasa bajo. El rectificador puede ser de un solo diodo, o puede ser más complejo. El filtro es generalmente de tipo RC pasa bajo, pero la función de filtro puede lograrse a veces apoyándose en la respuesta de frecuencia limitada del rectificador de los circuitos. La radio de galena explota la simplicidad de la modulación AM para producir un receptor con muy pocas piezas, con el cristal como el rectificador y la respuesta de frecuencia limitada de los auriculares como el filtro.



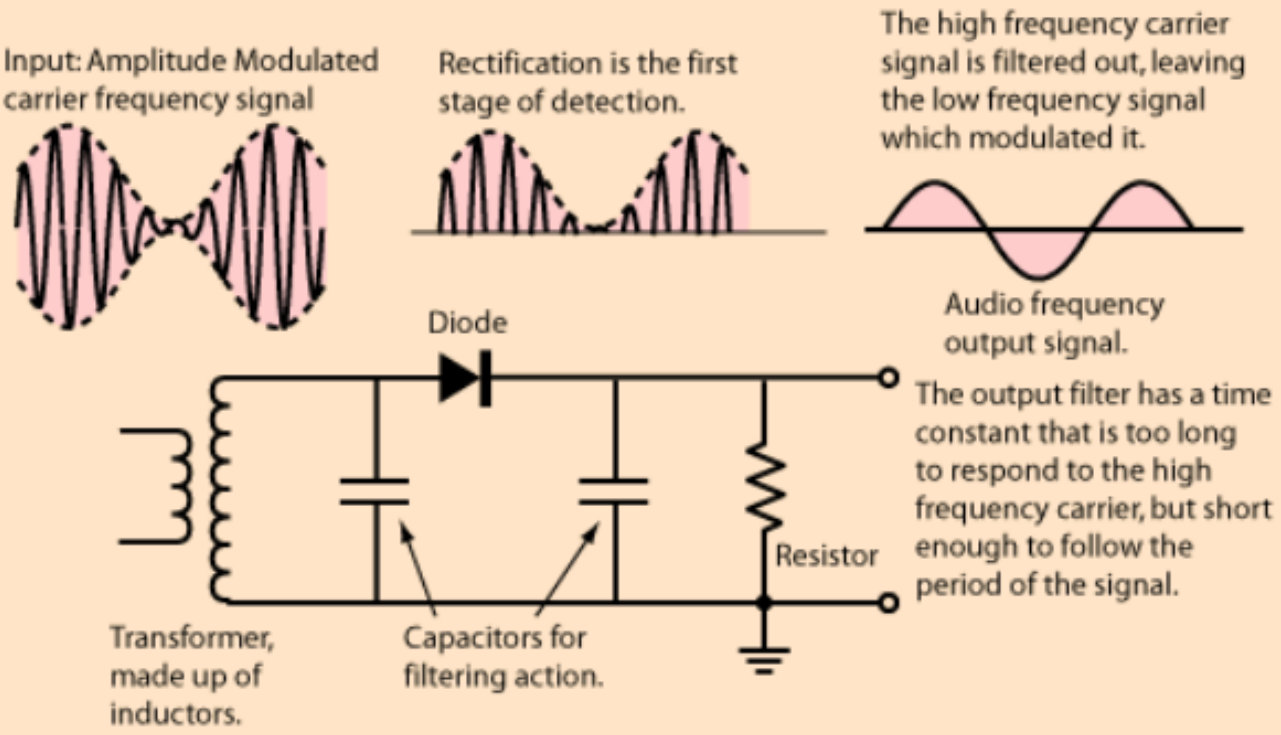
Una señal y su envolvente marcada en rojo.

El "detector de producto" multiplica la señal entrante por la señal de un oscilador local con la misma frecuencia y fase que la señal entrante del portador. Después de filtrar, se producirá la señal de audio original. Este método descifra tanto AM como SSB, pero si la fase no se puede determinar se requerirá una configuración más compleja.

Una señal AM puede rectificarse sin necesidad de un demodulador bv coherente. Por ejemplo, la señal puede pasar por un detector de envolvente (un rectificador de diodo y un filtro de pasa bajo). La señal de salida seguirá la misma curva que la señal de entrada. Hay señales AM en las que la portadora se reduce o suprime totalmente. Estas requieren la desmodulación coherente.

Detector de AM

La detección de las señales de radio AM es una aplicación de diodo.



La onda portadora de AM ya modulada se recibe en la antena del receptor de radio, y se rectifica por la acción de un diodo detector. Luego, la señal rectificada pasa a través de un filtro paso bajo, cuya constante de tiempo es demasiado larga para responder a las altas frecuencias de la onda portadora de AM. Las portadoras de AM están en el rango de 600 a 1400 kHz. La frecuencia de la señal que modula es mucho mas baja, de 0,02 a 5 kHz, y puede pasar a través de filtro.

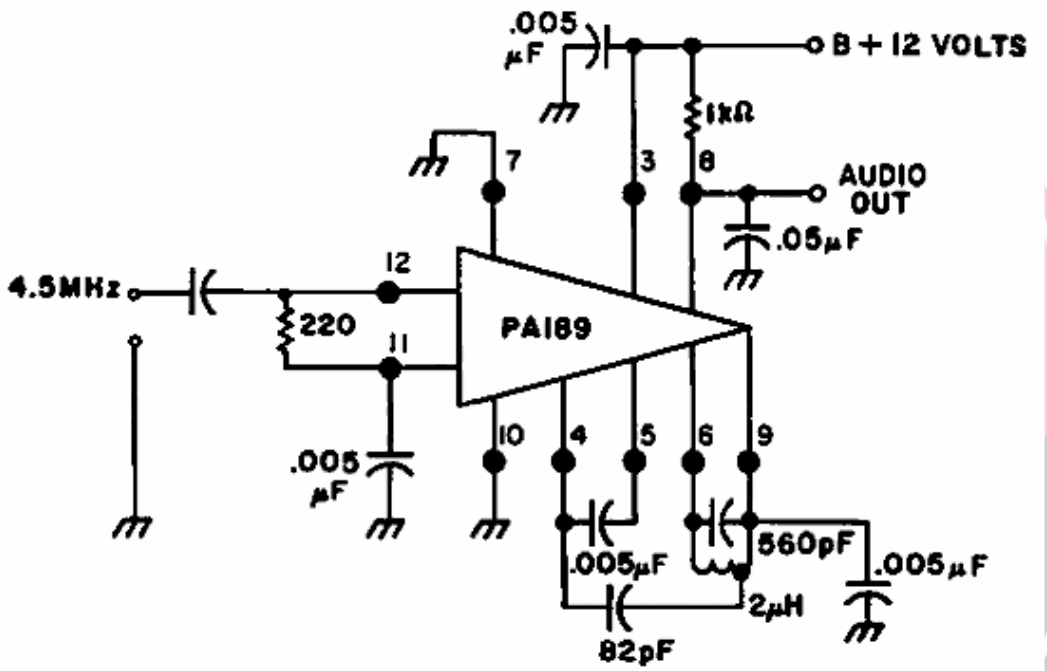
El detector de AM que se muestra aquí, sería adecuado para captar solamente una estación de radio AM, la elegida con los valores de los condensadores e inductancias. Una radio AM práctica utiliza un proceso llamado heterodino para desplazar la frecuencia portadora de cada estación de radio a una frecuencia simple llamada Frecuencia Intermedia IF, de modo que se pueda usar un simple circuito sofisticado de detección AM, para recibir todas las estaciones de radio AMl.

Demodulación de FM (Modulación en Frecuencia):

La modulación de frecuencia (FM) tiene numerosas ventajas sobre la modulación AM, como mejor fidelidad e inmunidad de ruido. Sin embargo, es mucho más complejo modular y demodular una onda portadora con FM.

Hay varios tipos comunes de demodulador de FM:

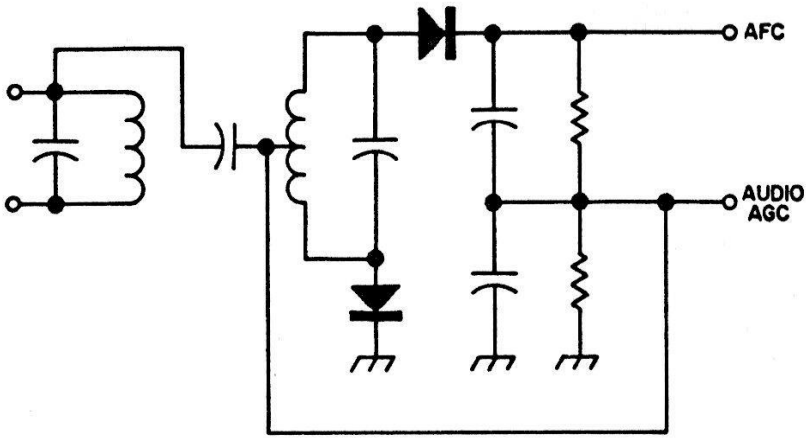
- El **detector de cuadratura**, en el que la fase de la señal cambia 90 grados y se multiplica con la versión entrante. Uno de los términos que se retira de esta operación es la señal de información original, que es seleccionada y amplificada.



Un detector de cuadratura utiliza un desplazador de fase de 90° y un detector de producto para demodular las señales de FM. El desplazador de fase de 90° produce una señal que está en cuadratura con las señales de IF recibidas

- La señal se alimenta en un PLL y la señal de error se utiliza como la señal demodulada.

- El más común es un "**discriminador Foster-Seeley**". Está formado por un filtro electrónico que disminuye la amplitud de algunas frecuencias en relación con otras, seguido por un demodulador de AM. Si la respuesta del filtro cambia linealmente con la frecuencia, la salida analógica final será proporcional a la frecuencia de entrada.

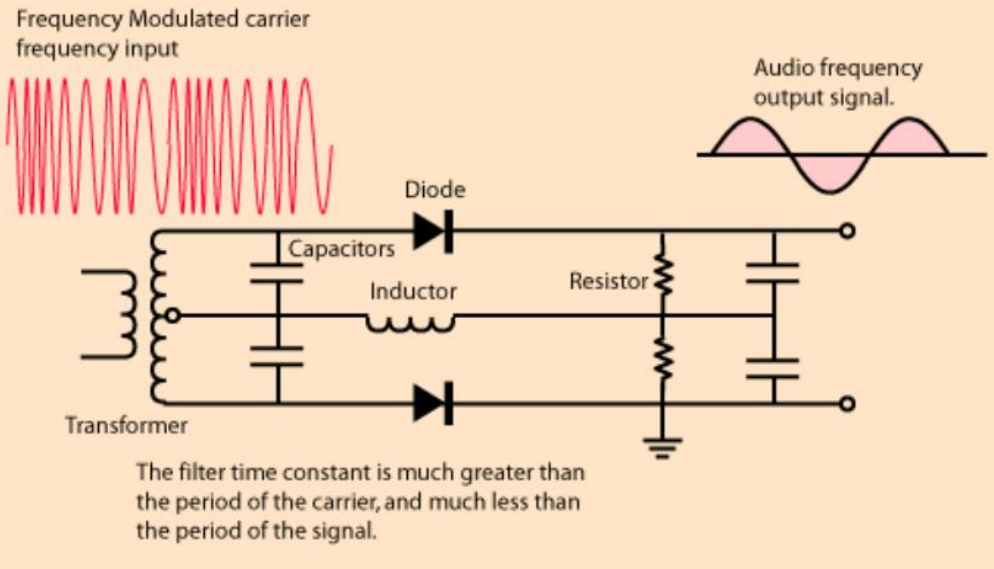


Esta es una configuración tradicional de **detector o discriminador para señales de FM** que recibe su nombre de sus desarrolladores **Foster y Seeley**. El circuito se encontró en la documentación de la década de 1980. Los diodos que se usan son comunes de germanio.

- Una variante de la discriminadora de Foster-Seeley llamada el **"detector de relación"**.
- Otro método utiliza dos **demoduladores de AM**, uno había sintonizado en el extremo superior de la banda y el otro en el extremo inferior y alimentan las salidas en un amplificador de diferencia.
- Usando un procesador digital de señal, como se utiliza en una radio definida por software.

Detector de FM

La detección de las señales de radio FM es una aplicación de diodo.



Demodulación de PM (Modulación en Fase):

- Se requiere un circuito especializado capaz de detectar los cambios de fase de la señal modulada y traducirlos en una señal de información recuperada.
- Es menos común en aplicaciones analógicas, pero se usa en algunos sistemas de comunicación especializados.

6.2.2.2. DEMODULACIÓN DE SEÑALES DIGITALES

Para recuperar los datos transmitidos en una señal modulada digitalmente, se emplean diferentes métodos según el tipo de modulación utilizada:

- **Demodulación de ASK (Amplitude Shift Keying):**
  - Se emplea un detector de amplitud que analiza los cambios de la amplitud de la portadora para reconstruir los datos binarios originales.
  - Es un método simple, pero susceptible a interferencias.
  - Se usa en aplicaciones de transmisión de datos en redes ópticas y RFID.
- **Demodulación de FSK (Frequency Shift Keying):**
  - Se emplean discriminadores de frecuencia que detectan las distintas frecuencias utilizadas para representar los bits 0 y 1.
  - Ofrece mayor resistencia al ruido que ASK y es utilizado en módems, radiocomunicaciones y transmisiones inalámbricas.
- **Demodulación de PSK (Phase Shift Keying):**
  - Se requiere un detector de fase que identifique los cambios en la fase de la portadora y los convierta en información binaria.
  - Métodos avanzados, como la detección coherente, mejoran la exactitud de la reconstrucción de la señal.
  - Usado en comunicaciones satelitales, redes Wi-Fi y telefonía móvil.
- **Demodulación de QAM (Quadrature Amplitude Modulation):**
  - Se emplean detectores de correlación que analizan tanto la fase como la amplitud de la señal para reconstruir los datos transmitidos.
  - Es una técnica muy eficiente en términos de espectro y se usa en televisión digital, redes LTE y sistemas de transmisión de datos de alta velocidad.

TÉCNICAS DE DEMODULACIÓN AVANZADAS

Con el avance de la tecnología, se han desarrollado técnicas sofisticadas de demodulación para mejorar la eficiencia y la resistencia al ruido:

- **Demodulación coherente:**
  - Se sincroniza un oscilador local con la señal portadora recibida para mejorar la precisión de la detección.
  - Es común en PSK y QAM para minimizar errores de transmisión.
- **Demodulación no coherente:**
  - No requiere sincronización con la señal portadora, lo que simplifica el diseño, pero puede introducir errores en ciertas condiciones.
  - Se emplea en sistemas ASK y FSK de baja complejidad.
- **Corrección de errores y detección de señal:**
  - Se aplican algoritmos de corrección de errores, como códigos de detección y corrección de errores (FEC, Forward Error Correction), para mejorar la calidad de la señal recibida.
  - Se utilizan técnicas como la ecualización adaptativa y la modulación adaptativa para optimizar la transmisión en tiempo real.

Conclusión

La demodulación es un proceso esencial en cualquier sistema de telecomunicaciones, ya que permite recuperar la información transmitida con la mayor fidelidad posible. La elección del método de demodulación adecuado depende del tipo de modulación utilizada, las condiciones del canal de transmisión y la calidad de señal deseada. Con el avance de la tecnología, los sistemas de demodulación han evolucionado para ofrecer soluciones más eficientes, seguras y resistentes al ruido, permitiendo la mejora continua en las comunicaciones modernas.

6.3. EQUIPOS DE MEDIDA EN TELECOMUNICACIONES

Los equipos de medida en telecomunicaciones permiten analizar la calidad de las señales, la integridad de los cables y el correcto funcionamiento de los dispositivos de transmisión y recepción. Estos instrumentos son esenciales para la instalación, mantenimiento y optimización de las redes de telecomunicaciones.

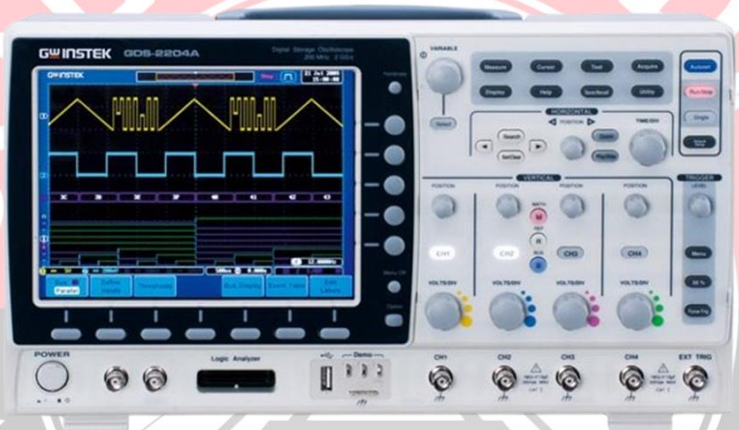
6.3.1. INSTRUMENTOS DE MEDICIÓN UTILIZADOS EN TELECOMUNICACIONES

La instrumentación en telecomunicaciones es fundamental para garantizar la correcta transmisión y recepción de señales. Para ello, se emplean diversos equipos de medición que permiten analizar la calidad de las señales, detectar interferencias y verificar el correcto funcionamiento de los sistemas de comunicación.

INSTRUMENTOS DE MEDICIÓN UTILIZADOS EN TELECOMUNICACIONES

Los instrumentos de medición son esenciales para la instalación, mantenimiento y diagnóstico de redes de telecomunicaciones. Algunos de los equipos más comunes incluyen:

Osciloscopios



- Son dispositivos que permiten analizar la forma de onda de las señales eléctricas en función del tiempo.
- Ayudan a visualizar fenómenos transitorios, ruidos e interferencias en circuitos de telecomunicaciones.
- Se utilizan en el análisis de señales analógicas y digitales, facilitando la detección de distorsiones y fallos en la transmisión.
- Existen diferentes tipos de osciloscopios, como los analógicos, digitales y de muestreo.

Medidores de potencia de RF

- Se emplean para medir la intensidad de las señales de radiofrecuencia, lo que permite evaluar la eficiencia de los transmisores y ajustar niveles óptimos de transmisión.
- Existen diferentes tipos de medidores, incluyendo medidores de potencia de diodo, térmicos y de sonda de campo.
- Son esenciales en sistemas de transmisión inalámbrica, comunicaciones satelitales y radiodifusión.

Analizadores de espectro

- Herramientas que permiten visualizar la distribución de frecuencias en una señal y detectar interferencias, ruido y anomalías en la transmisión.
- Son utilizados para evaluar la calidad de señales en sistemas de radiocomunicaciones, televisión digital y redes móviles.
- Permiten la identificación de fuentes de interferencia en entornos con múltiples transmisores.

Certificadores de cableado

- Se utilizan para verificar la integridad y calidad de los cables de red y fibra óptica.
- Permiten la certificación de cables según estándares internacionales como TIA/EIA y ISO/IEC.
- Analizan parámetros como la atenuación, la diafonía y la continuidad de los cables.

Medidores de pérdida óptica

- Dispositivos empleados en redes de fibra óptica para medir la atenuación de la señal a lo largo del cable.
- Ayudan a identificar problemas en la infraestructura de transmisión, como empalmes defectuosos o conectores sucios.
- Se utilizan junto con reflectómetros ópticos (OTDR) para evaluar la calidad de las fibras y detectar fallos.

Otros Instrumentos Importantes

- **Reflectómetros en el dominio del tiempo (TDR y OTDR):** Localizan fallos en cables de cobre y fibra óptica.

- **Generadores de señal:** Se emplean para probar la respuesta de sistemas de telecomunicaciones ante distintas señales de entrada.

- **Analizadores de redes:** Permiten evaluar el rendimiento de redes IP y diagnosticar problemas de conectividad.

- **Medidores de relación señal/ruido (SNR):** Determinan la calidad de una señal en presencia de ruido.

Importancia de la instrumentación en telecomunicaciones

El uso de estos instrumentos permite a los ingenieros de telecomunicaciones:

- Garantizar la calidad y confiabilidad de las transmisiones.
- Diagnosticar y corregir fallos en sistemas de comunicación.
- Optimizar el rendimiento de las redes y minimizar interferencias.
- Cumplir con normativas y estándares de calidad en telecomunicaciones.

Conclusión

La instrumentación en telecomunicaciones es clave para la instalación, mantenimiento y optimización de redes. El uso adecuado de equipos de medición permite garantizar la eficiencia y confiabilidad de los sistemas de comunicación, asegurando un desempeño óptimo en distintos entornos y aplicaciones.

Importancia de la calibración y mantenimiento de equipos de medida

Los equipos de medición deben mantenerse calibrados para garantizar lecturas precisas y confiables. La calibración periódica asegura que los dispositivos proporcionen mediciones exactas, comparables con estándares internacionales. El mantenimiento regular previene el desgaste de los componentes y permite detectar fallos antes de que afecten el rendimiento de las telecomunicaciones.

6.4. APLICACIONES EN REDES DE DATOS Y VOZ

Las redes de datos y voz desempeñan un papel crucial en la comunicación moderna, facilitando la transmisión de información entre dispositivos y personas. Estas redes han evolucionado con el tiempo, integrando tecnologías más avanzadas que optimizan la eficiencia, la velocidad y la calidad de la comunicación. En este apartado, se analizan las principales aplicaciones de las técnicas de modulación y demodulación en redes de datos y voz.

6.4.1. REDES DE DATOS

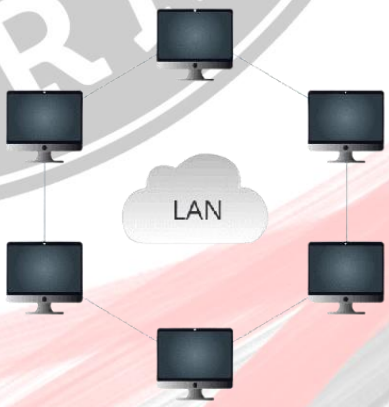
Las redes de datos permiten la transferencia de información digital entre computadoras, servidores y dispositivos inteligentes. Estas redes utilizan diversas tecnologías de transmisión, y la modulación desempeña un papel fundamental en la eficiencia y seguridad de la comunicación. Algunas aplicaciones clave incluyen:

6.4.1.1. INTERNET Y REDES DE ÁREA LOCAL (LAN, WAN, MAN): ¿CUÁL ES LA DIFERENCIA?

Entre los tipos de redes más comunes se encuentran: la red de área local (LAN), la red de área metropolitana (MAN) y la red de área amplia (WAN). Estas redes definen el alcance de los mensajes, la velocidad y otros parámetros que intervienen en la comunicación entre dispositivos. En este artículo describiremos tres tipos de red típicas, así como sus diferencias.

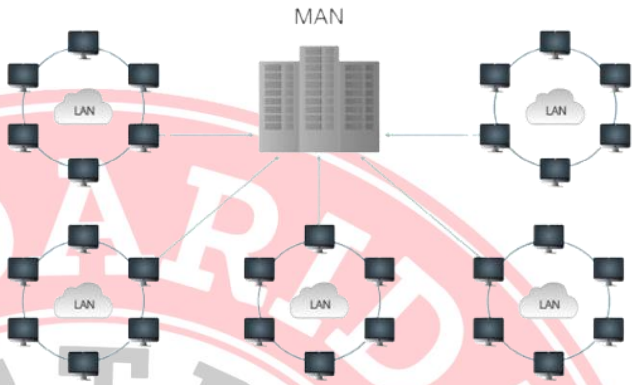
¿Cuál es la red LAN?

La Red de Área Local o LAN (Local Area Network, por sus siglas en inglés), es una red de informática que cubre áreas geográficas pequeñas con un alcance de 1-5 km. Estas áreas incluyen hogares, oficinas, escuelas, o un grupo de edificios donde hay ordenadores, servidores y dispositivos periféricos tales como impresoras, escáneres, proyectores y otros componentes de almacenamiento. Las conexiones entre los servidores se realizan frecuentemente con cables Ethernet para que los dispositivos finales se comuniquen entre sí, por medio de una conexión inalámbrica, es decir: Wi-Fi. Entre los protocolos LAN más comunes se encuentran: Ethernet, Token Ring, e interfaz de datos distribuidos por fibra o FDDI (Fiber Distributed Data Interface, por sus siglas en inglès). La mayoría de los protocolos inalámbricos que se utilizan hoy en día son: 802.11a, 802.11b, 802.11gy 802.11n.



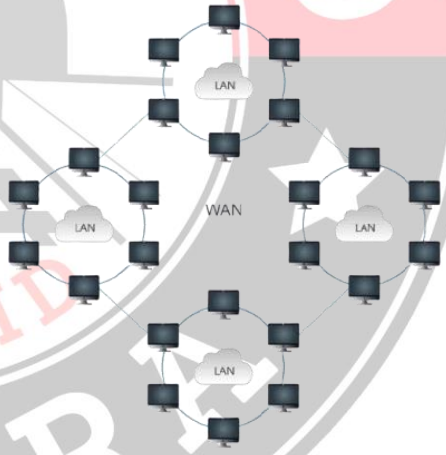
¿Cuál es la red MAN?

La red de área metropolitana o MAN (Metropolitan Area Network, por sus siglas en inglés), como su nombre indica, se emplea a menudo en ciudades y otros lugares que cubren un rango de 50-60 km. Las MAN son redes de conexión de alta velocidad que interconectan varias redes de área local en una sola gran red a través de un puente común, (líneas troncales). Este puente es establecido generalmente con fibra óptica para aumentar la velocidad de transferencia de datos. En resumen, la red MAN puede considerarse como un conjunto de una o más redes LAN conectadas entre sí a través de un solo cable. Los protocolos más utilizados para la transmisión de datos en la red MAN son: RS-232, X-25, Frame Relay y ATM.



¿Cuál es la red WAN?

La red de área amplia o WAN (Wide Area Network, por sus siglas en inglés) es una red informática que cubre una zona geográfica de gran escala con un diámetro de aproximadamente 100-1000 km, es decir, una red de comunicaciones cuyo enlace atraviese las fronteras metropolitanas, regionales o nacionales. Los dispositivos involucrados son más diversificados en comparación con los utilizados en los otros tipos de redes, abarcando routers, switches, módems firewalls, etc. Empresas como FS u otras compañías internacionales emplean la conexión WAN para comunicarse con sus diferentes filiales a través de satélites de microondas. Algunos de los protocolos WAN más comúnmente utilizados son: Frame Relay, X-25, red digital de servicios integrados o ISDN (Integrated Services Digital Network, por sus siglas en inglés) y el protocolo punto a punto o PPP.



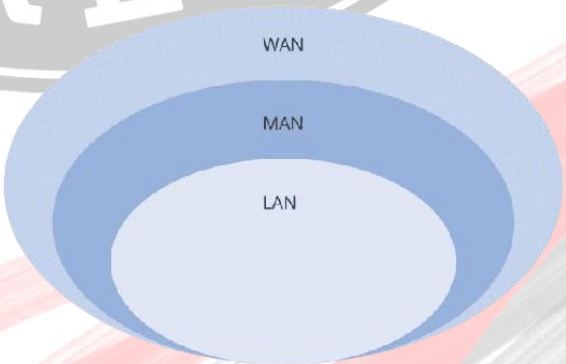
¿Cual es la diferencia entre las redes LAN, MAN, y WAN?

El mecanismo de comunicación es básicamente el mismo. Sin embargo, hay importantes diferencias con respecto a estos tres tipos de redes. Algunas de estas diferencias las explicaremos en la siguiente tabla.

Parámetros	LAN	MAN	WAN
Propiedad de la red	Privada	Privada o pública	Privada o pública
Área geográfica cubierta	Pequeña	Moderada	Muy grande
Diseño y mantenimiento	Fácil	Difícil	Difícil
Banda ancha	Baja	Moderada	Baja
Tasas de transferencia de datos	Alta	Moderada	Baja
Congestión	Menor	Mayor	Mayor
Aplicación	Universidades, escuelas, hospitales	En pueblos pequeños, y a nivel ciudad	En un país y a nivel continental

El alcance geográfico

Las redes LAN cubren la distancia más corta, seguidas de la red MAN y por último las redes WAN. Como la red LAN tiene la menor cantidad de nodos de red, es mucho más fácil de diseñar y de mantenerse a comparación con las redes MAN y WAN.



Despliegue y aplicación

Una empresa puede configurar una red LAN para denegar el acceso a los usuarios no autorizados, con el fin de garantizar la seguridad. Uno de los ejemplos con conexión MAN más conocidos es la red de televisión por cable disponible en muchas ciudades. La red MAN ha sido adoptada por varios organismos gubernamentales o empresas privadas para la interconectividad entre las oficinas de sus departamentos que se encuentran ubicadas en diferentes lugares o distritos. Las redes WAN se utilizan para reservas de ferrocarriles y líneas aéreas con modo de transmisión satelital, dado que estas operaciones requieren una red de alta seguridad para su comunicación.

Medios de transmisión de datos

Los medios empleados para la transmisión de datos en las redes LAN, MAN, y WAN más destacados se mencionan a continuación: La red LAN generalmente emplea cables WiFi y Ethernet para establecer la comunicación a velocidades de datos de aproximadamente 100 o 1000 Mbps. La red MAN incorpora módems y cables que permiten la transmisión de 100Mbps. La comunicación entre los diferentes usuarios mediante la red WAN se establece por medio de líneas telefónicas arrendadas o enlaces satelitales, cables ópticos y microondas. La velocidad de transmisión de datos de la red WAN es generalmente mucho más baja que la de otros tipos de redes de área.

Conclusión

En este artículo hemos descrito las características de los sistemas de redes informáticas LAN, MAN y WAN, al igual que sus diferencias. Los tres tipos de sistemas de redes poseen características propias según los diversos ámbitos. Es fundamental determinar en qué consisten estas redes y en qué se diferencian para desplegarlas de manera efectiva.

6.4.1.2. COMUNICACIONES MÓVILES Y REDES: QUÉ SON, CÓMO FUNCIONAN Y QUÉ TIPOS EXISTEN.

Aunque el uso de **redes móviles** es algo muy habitual hoy en día, hace algunas décadas apenas sabíamos de su existencia. Si nos vamos a los datos, en 1993 solo el 1 % de la población chilena tenía acceso a un teléfono móvil, mientras que en 2022 se contabilizaron 26,3 millones de teléfonos conectados, es decir, 1,3 celulares por habitante.

Con el 4G y 5G a la cabeza, las ventajas que ofrecen actualmente las comunicaciones inalámbricas han creado una sociedad cada vez más digitalizada, donde las empresas pueden ofrecer servicios más innovadores que aumentan la eficiencia de sus

actividades. En este artículo podrás entender qué son las **redes móviles**, cómo funcionan, qué tipos existen y cómo están influyendo en la sociedad moderna.

¿Qué son las redes móviles?

Podemos definir las **redes móviles** como una infraestructura de telecomunicaciones inalámbrica que habilita el intercambio de datos entre dispositivos a través de señales de radio de baja potencia. El uso de antenas conectadas de forma permanente a una centralita permite a los usuarios comunicarse sin necesidad de conectarse a una línea fija.

Las primeras **redes móviles** de uso generalizado aparecieron en los años 80 en Japón y Estados Unidos. A pesar de ser tecnológicamente limitada, la red móvil 1G inició la era de la telefonía móvil y las llamadas internacionales sin necesidad de cables. Con el paso de los años, el uso de **redes móviles** fue evolucionando hasta lo que conocemos hoy en día, donde el **5G** ofrece una alta velocidad de intercambio de datos y un sin fin de posibilidades.

Las **redes móviles** actuales ofrecen una conexión a Internet de alta velocidad, lo cual ha abierto un mundo de posibilidades para las empresas, destacando la Industria 4.0, el Internet of Things o la independencia geográfica.

¿Cómo funcionan las redes móviles?

Aunque el funcionamiento de las **redes móviles** es complejo, se puede resumir de forma sencilla. Todo parte de una centralita telefónica digital que posee el equipamiento necesario para comunicarse con los dispositivos móviles. La centralita es el centro de operaciones donde se procesan los datos, se transmiten y reciben las señales provenientes de cualquier antena. Los paquetes de datos viajan hasta la centralita, son procesados y distribuidos a sus destinatarios.

Las antenas distribuidas por todo el mundo ofrecen zonas de cobertura a las que los dispositivos se conectan utilizando un protocolo de comunicación. Cada vez que nos conectamos a internet o realizamos una llamada telefónica, el emisor envía paquetes de datos a las antenas más cercanas, la cual, a su vez, replica dicha información hacia otras

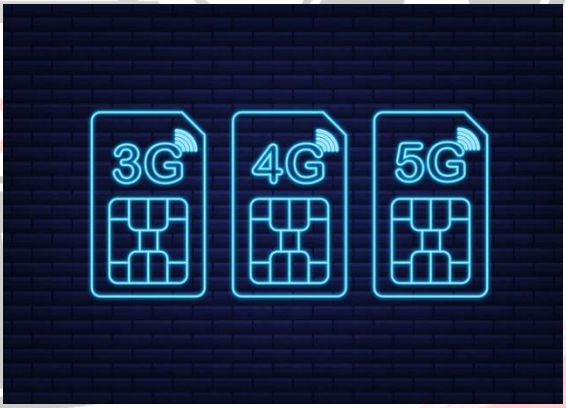
antenas hasta llegar a una centralita. Cada antena cubre una pequeña área a su alrededor llamada celda.

Una vez en la centralita, los paquetes de datos son procesados y enviados a su receptor, pudiendo ser este otro usuario o un servidor web, por ejemplo. De esta forma se establece una conexión donde emisor y receptor intercambian paquetes de datos a una gran velocidad hasta alguno de los participantes finaliza la transmisión.

¿Qué tipos de redes existen?

Con el paso del tiempo han ido apareciendo diferentes tipos de **redes móviles** que han sido habilitadas para diferentes usos, ya que poseen características distintas y optimizadas según el caso de uso. Podemos ver diferencias entre:

- **Red 1G**: primera generación de **redes móviles** que fue lanzada por la compañía japonés NTT en 1979. Empleaba tecnología analógica que permitió realizar por primera vez llamados de voz de baja calidad sin necesidad de cables.
- **Red GSM o 2G**: la segunda generación permitía realizar llamadas telefónicas de alta calidad, pero seguía siendo inadecuada para navegar por internet, aunque sí aceptaba el envío de mensajes de texto (SMS). Fue la primera red móvil completamente digital.
- **Red GPRS o 2.5G**: evolución de la anterior red que aumentó levemente la velocidad, lo que permitió por primera vez navegar por Internet empleando un dispositivo móvil. A pesar de ello, navegar por Internet era aún demasiado lento. Como punto positivo, el consumo de batería estaba optimizado.



- **Red UMTS o 3G**: con la aparición del 3G, las conexiones móviles dieron un gran salto. La velocidad de transmisión era mucho mayor, lo que permitió disfrutar, por primera vez, de videollamadas en tiempo real, navegación por Internet, redes sociales o mensajería instantánea. Sin embargo, consumía mucha más batería.
- **Red LTE o 4G**: el 4G ha sido una auténtica revolución en las **redes móviles**. Esta no solo ofrece una velocidad muy alta de transmisión de datos, sino que también ofrece una alta estabilidad y bajo consumo de batería comparada con la generación anterior. Esta permitió un mayor volumen de usuarios conectados a

una misma celda, acceso a internet a altas velocidades, consumo de contenido en streaming o juegos online.

- **Red 5G**: la quinta generación es el nuevo estándar en **redes móviles**, permitiendo un mayor ancho de banda y mayores velocidades de transmisión. Esta generación ofrece un uso más eficiente, tanto en el ancho de banda como en el consumo energético. El 5G abre la puerta a un mundo conectado sin apenas latencia (retardo temporal en el envío y recepción de datos), amplias zonas de cobertura y un mayor volumen de usuarios conectados simultáneamente.

¿Cómo han cambiado las redes móviles el mundo?

Si damos un poco marcha atrás en el tiempo, podemos decir que, sin lugar a duda, las **redes móviles** han cambiado el mundo. Las telecomunicaciones inalámbricas han cambiado, no solo la forma en la que nos comunicamos, sino también la forma en la que nos comportamos, accedemos a la información, trabajamos o nos relacionamos.

Todas las **redes móviles** han contribuido a unir el mundo, donde ahora podemos comunicarnos sin tener en cuenta fronteras geográficas o nacionales. Ahora, la mayoría de la actividad económica se realiza desde cualquier parte del mundo sin tener en cuenta el lugar donde estés.

Asimismo, las **redes móviles** han habilitado otras tecnologías que permiten la automatización de procesos, la inteligencia artificial, el acceso a nuevos datos, el teletrabajo, etc. En cuestión de negocios, estas han abierto un sin fin de posibilidades de las empresas, siendo la base de innovación de cientos de miles de proyectos en todo el mundo y sectores de mercado.

Y precisamente esta es la misión de Entel, ofrecer **redes móviles** de última generación para que todas las empresas disfruten de una conexión rápida, segura y estable. Gracias a los distintos planes, así como el soporte del equipo de Entel, tu empresa podrá seguir innovando y creciendo.

¿Cuál fue la primera red móvil?

La primera red móvil comercial fue lanzada por la compañía NTT en Japón en el año 1979. Esta empleaba tecnología analógica y solo ofrecía llamadas de voz de baja calidad y poca seguridad. La velocidad de transmisión de datos alcanzaba como máximo los 2,4 Kbps.

¿Qué son las redes 1G, 2G, 3G, 4G y 5G?

Las siglas 1G, 2G, 3G, 4G, 5G hacen referencia a las diferentes generaciones de **redes móviles** que han ido apareciendo desde su aparición en los años 80. Desde entonces, estas han ido evolucionando para ofrecer un mayor ancho de banda y velocidad de transferencia, permitiendo la comunicación inalámbrica entre dispositivos.

6.4.1.3. SISTEMAS DE COMUNICACIÓN POR SATÉLITE:

VER TAMBIEN 7.1.2.2 MEDIOS INALÁMBRICOS:

En las **comunicaciones por satélite**, las señales directas son enviadas y recibidas en el espacio por satélites artificiales situados en órbita alrededor de la Tierra.

Un satélite actúa como un repetidor situado en el espacio: recibe las señales enviadas desde la estación terrestre y las reemite a otro satélite o de vuelta a los receptores terrestres. En realidad, hay dos tipos de satélites de comunicaciones: solo que es más conocida como comunicaciones satélites.

- **Satélites pasivos.** Se limitan a reflejar la señal recibida sin llevar a cabo ninguna otra tarea.
- **Satélites activos.** Amplifican las señales que reciben antes de reemitirlas hacia la Tierra. Son los más habituales. Satélites y sus órbitas Los satélites son puestos en órbita mediante cohetes espaciales que los sitúan circundando la Tierra a distancias relativamente cercanas fuera de la atmósfera.

Satélites y sus órbitas

Los satélites son puestos en órbita mediante cohetes espaciales que los sitúan circundando la Tierra a distancias relativamente cercanas fuera de la atmósfera. Los tipos de satélites según sus órbitas son:

- **Satélites LEO (*Low Earth Orbit*, órbita terrestre baja).** Orbitan la Tierra a una distancia de 160-2000 km y su velocidad les permite dar una vuelta al mundo en 90 minutos. Se usan para proporcionar datos geológicos sobre movimiento de placas terrestres y para la industria de la telefonía por satélite.
- **Satélites MEO (*Medium Earth Orbit*, órbita terrestre media).** Son satélites con órbitas medianamente cercanas, de unos 10 000 km. Su uso se destina a comunicaciones de telefonía y televisión, y a las mediciones de experimentos espaciales.
- **Satélites HEO (*Highly Elliptical Orbit*, órbita muy elíptica).** Estos satélites no siguen una órbita circular, sino que su órbita es elíptica. Esto supone que alcanzan distancias mucho mayores en el punto más alejado de su órbita. A menudo se utilizan para cartografiar la superficie de la Tierra, ya que pueden detectar un gran ángulo de superficie terrestre.
- **Satélites GEO (*Geosynchronous Equatorial Orbit,* órbita geoestacionaria).** Tienen una velocidad de traslación igual a la velocidad de rotación de la Tierra, lo que supone que se encuentren suspendidos sobre un mismo punto del globo terrestre. Por eso se llaman satélites geoestacionarios. Para que la Tierra y el satélite igualen sus velocidades es necesario que este último se encuentre a una distancia fija de 35 800 km sobre el Ecuador. Se destinan a emisiones de televisión y de telefonía, a la transmisión de datos a larga distancia, y a la detección y difusión de datos meteorológicos.

Antenas parabólicas

Las antenas utilizadas preferentemente en las comunicaciones vía satélites son las antenas parabólicas, cada vez más frecuentes en las terrazas y tejados de nuestras ciudades. Tienen forma de parábola y la particularidad de que las señales que inciden sobre su superficie se reflejan e inciden sobre el foco de la parábola, donde se encuentra el elemento receptor.

Son antenas parabólicas de foco primario. Es importante que la antena esté

correctamente orientada hacia el satélite, de forma que las señales lleguen paralelas al eje de la antena. Son muy utilizadas como antenas de instalaciones colectivas.

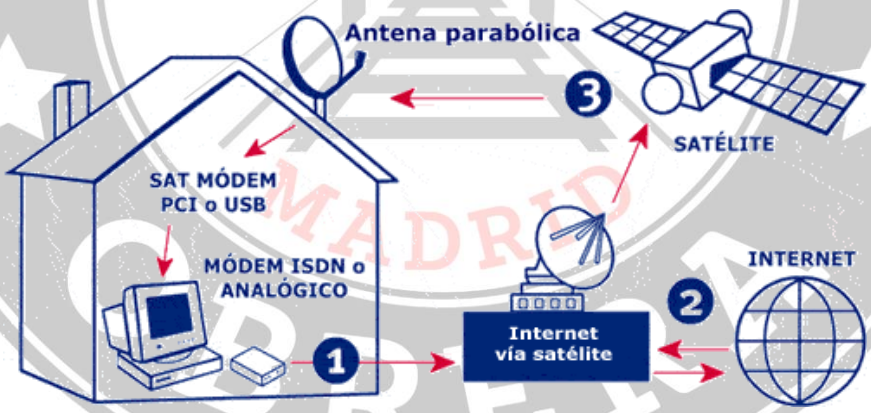
Una variante de este tipo de antena parabólica es la antena *offset*; este tipo de antena tiene un tamaño más reducido, y obtiene muy buen rendimiento. La forma parabólica de la superficie reflectante hace que las señales, al reflejarse, se concentren en un punto situado por debajo del foco de parábola. Por sus reducidas dimensiones se suelen utilizar en instalaciones individuales de recepción de señales de TV y datos vía satélite.

Otro tipo particular es la antena Cassegrain, que aumenta la eficacia y el rendimiento respecto a las anteriores al disponer de dos reflectores: el primario o parábola más grande, donde inciden los haces de señales es un primer contacto, y un reflector secundario (subreflector).

El acceso a Internet a través de satélite se consigue con las tarjetas de recepción de datos vía satélite. El sistema de conexión que generalmente se emplea es un híbrido de satélite y teléfono. Hay que tener instalada una antena parabólica digital, un acceso telefónico a Internet (utilizando un módem RTC, RDSI, ADSL o por cable), una tarjeta receptora para PC, un software específico y una suscripción a un proveedor de satélite.

Utilización de la línea telefónica estándar es necesaria para la emisión de peticiones a Internet ya que el usuario (salvo en instalaciones especiales) no puede hacerlas directamente al satélite.

Internet por satélite



Con el canal ascendente las peticiones (páginas web, envío de correos electrónicos, etc) a través de un módem de RTC, RDSI, ADSL o por cable, dependiendo de tipo de conexión del que se disponga. Estas peticiones llegan al proveedor de Internet que los transmite al centro de operaciones de red y que a su vez dependerá del proveedor del acceso vía satélite. Los datos se envían al satélite que los transmitirá por el canal descendiente directamente al usuario a unas tasas de transferencia de hasta 400 Gbytes/s.

Local Multipoint Distribution System (LMDS) es un sistema de comunicación inalámbrica de punto a multipunto, que utiliza ondas radioeléctricas a altas frecuencias, en torno a 28 y 40 GHz. Con estas frecuencias y al amplio margen de operación, es

posible conseguir un gran ancho de banda de comunicaciones, con velocidades de acceso que pueden alcanzar los 8 Mbps.

Este sistema de conexión da soporte a una gran variedad de servicios simultáneos: televisión multicanal, telefonía, datos, servicios interactivos multimedia.

La arquitectura de red LMDS consiste principalmente de cuatro partes: centro de operaciones de la red (NOC), infraestructura de fibra óptica, estación base y equipo del cliente (CPE).

El Centro de Operaciones de la Red (Network Operation Center – NOC) contiene el equipo del Sistema de Administración de la Red (Network Management System – NMS) que está encargado de administrar amplias regiones de la red del consumidor.

La infraestructura basada en fibra óptica, típicamente consiste de Redes Ópticas Síncronas (SONET), señales ópticas OC-12, OC-3 y enlaces DS-3, equipos de oficina central (CO), sistemas de conmutación ATM e IP, y conexiones con la Internet y la Red Telefónica Pública (PSTNs).

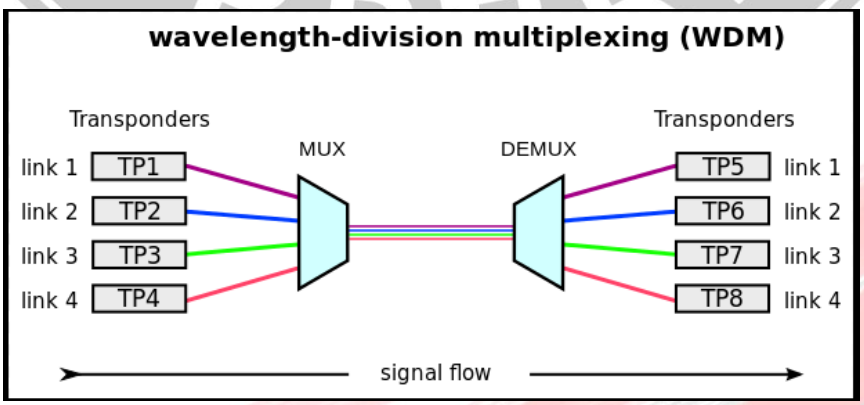
En la estación base es donde se realiza la conversión de la infraestructura de fibra a la infraestructura inalámbrica.

El sistema opera así, en el espacio local mediante las estaciones base y las antenas receptoras usuarias, de forma bidireccional. Se necesita que haya visibilidad directa desde la estación base hasta el abonado, por lo cual pueden utilizarse repetidores si el usuario está ubicado en zonas sin señal.

Los costes de reparación y mantenimiento de este tipo de conexión son bajos, ya que al ser la comunicación por el aire, la red física como tal no existe. Por tanto, este sistema se presenta como un serio competidor para los sistemas de banda ancha.

6.4.1.4. REDES ÓPTICAS Y FIBRA ÓPTICA:

Utilización de modulación avanzada en sistemas WDM (Multiplexación por División de Longitud de Onda):



La tecnología WDM es avanzada Tecnología de comunicación, conocida como multiplexación por división de longitud de onda. Implica transmitir luz de diferentes tasas mezcladas dentro de una sola fibra óptica, donde las señales digitales llevadas por estas señales de luz de diferentes longitudes de onda pueden ser de la misma velocidad y formato, o diferentes tasas y formatos de datos.

En el extremo receptor, estas señales combinadas de diferentes longitudes de onda se separan utilizando un demultiplexor y se procesan adicionalmente para restaurar las señales originales, que luego se envían a diferentes terminales. Por lo tanto, esta tecnología se llama multiplexación de división de longitud de onda óptica, abreviada como WDM óptico.

Se puede comparar con una carretera "de varios carriles". Los sistemas TDM tradicionales solo utilizan un carril de este camino, y aumentar la velocidad de bits es similar a acelerar en ese carril para aumentar la capacidad de transporte por unidad de tiempo. El uso de la tecnología de multiplexación de división de longitud de onda densa (DWDM) es similar a utilizar los carriles no utilizados en esta carretera para aprovechar la vasta capacidad de transmisión sin explotar de la fibra óptica.

La tecnología WDM es de gran importancia para la expansión y la actualización de la red, el desarrollo de servicios de banda ancha, aprovechando la capacidad de ancho de banda de las fibras ópticas y el logro de la comunicación de ultra alta velocidad.

1. Composición básica de los sistemas WDM

La composición básica de los sistemas WDM incluye principalmente dos tipos: transmisión unidireccional de doble fibra y transmisión bidireccional de una sola fibra. WDM unidireccional implica que todos los canales ópticos se transmiten en la misma dirección a través de una sola fibra óptica. En el extremo de transmisión, las señales ópticas moduladas con diferentes longitudes de onda, cada una con varias información, se combinan utilizando un multiplexor óptico y se transmiten unidireccalmente a través de una fibra óptica. Dado que cada señal se transporta por la luz de una longitud de onda diferente, no se mezclan. En el extremo receptor, un demultiplexor óptico separa las señales ópticas de diferentes longitudes de onda, completando la transmisión de múltiples señales ópticas, mientras que la dirección inversa se transmite a través de otra fibra óptica.

WDM bidireccional significa que los canales ópticos se transmiten simultáneamente en dos direcciones diferentes en una sola fibra óptica, con las longitudes de onda utilizadas separadas para lograr una comunicación dúplex.

Un sistema WDM generalmente comprende cuatro componentes: un transmisor óptico, un amplificador de repetidor óptico, un receptor óptico y un canal de supervisión óptica.

Transmisor óptico:

Como el equipo central del sistema WDM, en el extremo de transmisión, primero convierte la salida de señales ópticas del equipo terminal en señales con longitudes de onda específicas estables utilizando un transpondedor óptico, luego sintetiza señales ópticas multicanal utilizando un multiplexor y amplifica la salida a través de un amplificador de potencia óptica.

Amplificador de repetidor óptico:

Después de la transmisión de fibra óptica de larga distancia (80 ~ 120 km), la señal óptica debe amplificarse. En los sistemas WDM, la tecnología de aplanamiento de ganancia debe usarse para garantizar que el amplificador de fibra dopado con erbio (EDFA) proporcione la misma ganancia de amplificación para señales ópticas de diferentes longitudes de onda y que la competencia de ganancia de los canales ópticos no afecta el rendimiento de la transmisión.

Receptor óptico:

En el extremo receptor, la señal del canal principal, que ha sido atenuada por la transmisión, se amplifica por un preamplificador óptico. Se utiliza un demultiplexor para separar el canal óptico de una longitud de onda específica de la señal óptica del canal principal. El receptor debe cumplir con los requisitos para parámetros como la sensibilidad de la señal óptica y la potencia de sobrecarga, y debe poder resistir las señales con cierto ruido óptico.

Canal de supervisión óptica:

El canal de supervisión óptica se utiliza para monitorear los sistemas de transmisión óptica WDM. El ITU-T recomienda usar una longitud de onda de 1510 nm con una capacidad de 2 mbit/s. Todavía puede funcionar normalmente con una alta sensibilidad de recepción (mejor que -48 dbm) a velocidades bajas. Sin embargo, debe eliminarse de la ruta óptica antes del EDFA y agregar a la ruta óptica después del EDFA.

A lo largo de todo el sistema WDM, el multiplexor óptico y el demultiplexor son los componentes clave de la tecnología WDM, y su rendimiento es decisivo para la calidad de transmisión del sistema. Un dispositivo que combina señales de diferentes longitudes de onda de fuente de luz y las genera a través de una sola fibra óptica de transmisión se llama multiplexor de división de longitud de onda.

Por el contrario, un dispositivo que descompone señales de longitud de onda múltiple que llegan desde la misma fibra óptica de transmisión en longitudes de onda individuales para la salida se denomina demultiplexor. En principio, este dispositivo es bidireccional, lo que significa que si la salida y los extremos de entrada del demultiplexor se invierten, se convierte en un multiplexor. Los indicadores de rendimiento para los multiplexores de división de longitud de onda óptica incluyen pérdida de inserción y diafonía, con requisitos de baja pérdida y desplazamiento de frecuencia, pérdida de inserción por debajo de 1. 0 ~ 2.5dB, diafonía de canales bajas, alta aislamiento e interferencia mínima entre señales de diferentes longitudes de onda.

2. Ventajas de los sistemas WDM:

Capacidad ultra-grande y transmisión de distancia ultra larga:

Actualmente, las fibras ópticas ordinarias pueden transmitirse a través de un ancho de banda amplio, pero su tasa de utilización sigue siendo muy baja. El uso de la tecnología de multiplexación de división de longitud de onda densa (DWDM) puede aumentar la capacidad de transmisión de una sola fibra óptica varias veces, docenas de veces o incluso cientos de veces en comparación con la transmisión de longitud de onda única. El sistema de transmisión de fibra óptica de más alta capacidad actualmente es de 3.2tbit/s.

Transmisión de datos transparentes:

Dado que los multiplexes y demultiplexes del sistema DWDM basados en diferentes longitudes de onda óptica y es independiente de la velocidad de señal y el método de modulación eléctrica, es "transparente" a los datos. El sistema WDM realiza transmisión transparente; Para las señales de capa de "servicio", cada canal de longitud de onda óptica en el sistema WDM actúa como una fibra óptica "virtual".

Alta flexibilidad, economía y confiabilidad en la composición de la red:

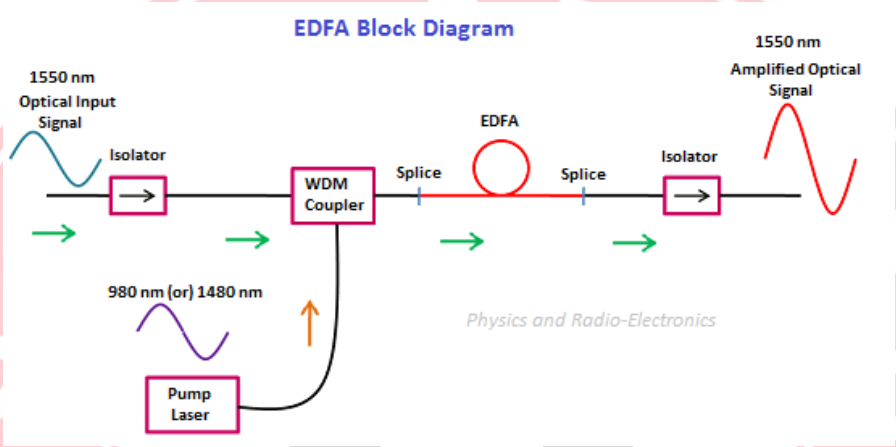
La nueva red de comunicación formada con tecnología WDM es más simple en estructura y más jerárquica en comparación con las redes compuestas por tecnología de multiplexación de división de tiempo eléctrica tradicional. La programación de varios servicios se puede lograr ajustando la longitud de onda de la señal óptica correspondiente. La flexibilidad, la economía y la confiabilidad resultantes de la red son evidentes.

Implementación de modulación de fase coherente para mejorar la eficiencia en redes de alta velocidad:

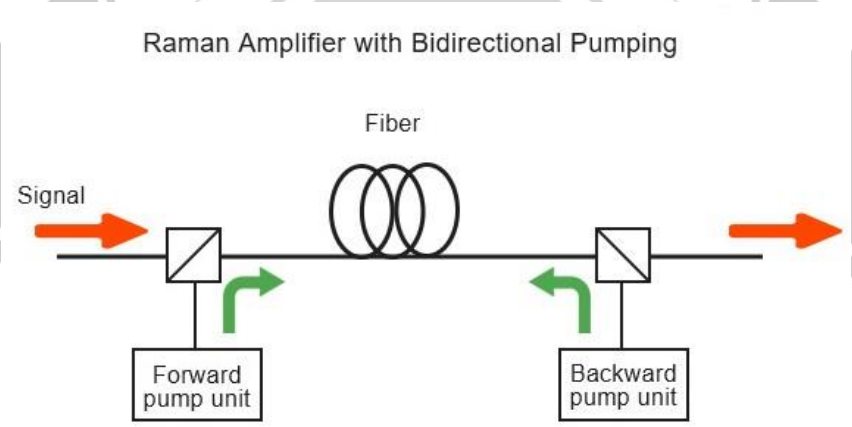
- La modulación de fase coherente permite mejorar la capacidad de transmisión mediante el uso de detección coherente, lo que incrementa la sensibilidad de los receptores ópticos.
- Métodos como **QPSK (Quadrature Phase Shift Keying)** y **16-QAM (Quadrature Amplitude Modulation)** permiten transmitir múltiples bits por cada símbolo modulado, optimizando el uso del ancho de banda.
- Se implementa en redes de fibra óptica de larga distancia y en infraestructuras de redes troncales de alto rendimiento.

Uso de amplificadores ópticos para extender la distancia de transmisión sin degradación de la señal:

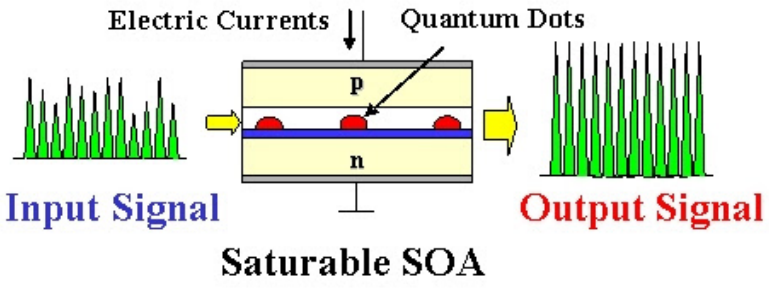
- La atenuación en la fibra óptica puede limitar la distancia de transmisión, por lo que se emplean amplificadores ópticos para regenerar la señal sin necesidad de convertirla en señal eléctrica.
- Existen tres tipos principales de amplificadores ópticos:
  - **EDFA (Erbium-Doped Fiber Amplifier):** Utiliza fibra dopada con erbio y es ampliamente utilizado en telecomunicaciones de larga distancia.



  - **Raman Amplifier:** Se basa en la dispersión Raman para amplificar la señal en la fibra óptica.



  - **SOA (Semiconductor Optical Amplifier):** Ofrece amplificación óptica con menor costo, aunque con mayores niveles de ruido.



- Estos amplificadores se utilizan en redes troncales de telecomunicaciones, conexiones de fibra hasta el hogar (FTTH) y en redes submarinas de alta capacidad.

6.4.2. REDES DE VOZ

Las redes de voz permiten la comunicación auditiva entre personas a través de diversos medios, incluyendo telefonía fija, móvil y VoIP. La calidad y fiabilidad de estas redes dependen en gran medida de las técnicas de modulación y demodulación utilizadas. Algunas de sus aplicaciones incluyen:

6.4.2.1. TELEFONÍA TRADICIONAL (PSTN) Y VOIP:

PSTN

- **¿Cuál es la definición de PSTN?**

PSTN son las siglas para Public Switched Telephone Network en inglés (Red Telefónica Pública Conmutada) que proporciona la infraestructura física necesaria para hacer y recibir llamadas (y transportar el tráfico de datos) entre los usuarios.

- **¿Cómo funciona?**

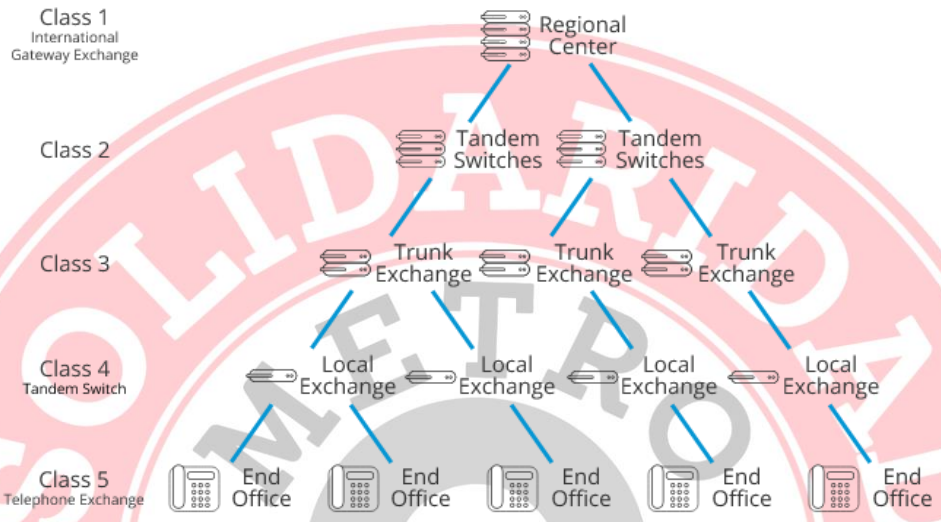
Las compañías telefónicas que operan a nivel internacional, nacional o regional, todas ellas crearon una red de cables interconectados. Las interconexiones se llaman “nodos”. Cuando un usuario levanta un teléfono y marca los dígitos, mandando una señal DTMF a los nodos para que sepan el destino de la llamada telefónica.

- **¿Qué es una señal DTMF?**

DTMF son las siglas para Dual tone multi-frequency (doble tono multifrecuencia) y son los sonidos generados por un teléfono cuando se presionan los números. Cuando el usuario presiona los números, el equipo de los nodos escuchan los tonos y entienden su significado para decodificarlos en comandos. El comando dirá al nodo donde enviar el tráfico de voz del llamante.

- **Arquitectura PSTN**

Originalmente, la red de PSTN fue construída utilizando cables de cobre pero ahora la PSTN es casi completamente digital en su núcleo de red al utilizar cables de fibra óptica, enlaces de satélite, y centros de cambio de alta tecnología. La topología de la red de PSTN es increíblemente compleja pero puede simplificarse en una configuración jerárquica. Cada línea de los usuarios se conecta a una central local que, a su vez, se conecta a centrales troncales y así sucesivamente.



- **¿Puede añadir una línea PSTN a una Central Telefónica?**

Sí. Una PSTN e ISDN pueden configurarse dentro de los sistemas de una centralita telefónica con tan solo añadir una pieza adicional al hardware, conocido como gateway. Estos habilitan las llamadas sobre líneas PSTN al utilizar tecnología que convierte la señal analógica a tráfico digital que puede ser gestionado por el software de la centralita.

- **El apagado de PSTN**

De forma internacional, muchas de las compañías telefónicas nacionales ya han empezado a desconectar la red de PSTN de cobre antigua incluyendo los servicios ISDN. Las compañías ya no ofrecerán servicios de cables de cobre a las instalaciones de empresas con el único propósito de hacer y recibir llamadas telefónicas. Esto se debe a la proliferación de servicios basados en IP como troncales SIP y VoIP que traen con ellos grandes beneficios adicionales.

VOIP

- **¿Qué es un teléfono VoIP?**

Un teléfono VoIP (protocolo de voz a través de Internet, por sus siglas en inglés) es un sistema de telefonía en Internet que facilita llamadas de voz, vídeo y multimedia mediante la conexión a Internet. A diferencia de los sistemas telefónicos analógicos, los

sistemas VoIP no requieren software telefónico. Permiten al usuario llamar a cualquier línea fija o móvil o incluso de ordenador a ordenador con un portátil, PC, Tablet o móvil conectado a Internet.

Al VoIP también se lo conoce por otros nombres como llamadas en Internet, telefonía de Internet, telefonía IP, red de voz, telefonía de banda ancha o servicio telefónico de banda ancha, entre muchos otros.

- **Los tres tipos de teléfonos VoIP**

El VoIP es un sistema de telefonía a través de Internet increíblemente versátil. Dependiendo del uso que se les dé, los sistemas telefónicos VoIP pueden clasificarse en los siguientes tipos:

Adaptador telefónico analógico (ATA)

¿Qué ocurre si quiere usar su antiguo sistema telefónico para realizar llamadas de VoIP? Un adaptador telefónico analógico (ATA) puede ayudarle a hacerlo. El sistema tendrá un puerto Ethernet que estaría conectado a una línea de red que permitiría una conexión VoIP. Algunos dispositivos también podrían incluir centrales externas FXS y más puertos FXO, los cuales proporcionan acceso al servicio telefónico tradicional.

De ordenador a teléfono

Los sistemas de llamadas VoIP de ordenador a teléfono son similares a los ATA con la diferencia de que están conectados a un ordenador o a su rúter. Se utilizan principalmente en call centers en los que los usuarios tienen que usar tanto el dispositivo telefónico para las operaciones de telefonía como los ordenadores para obtener información.

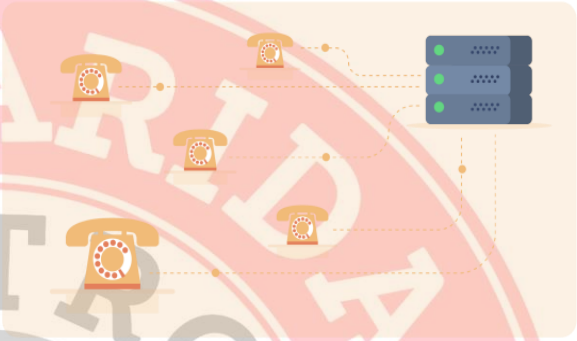
De ordenador a ordenador

Los teléfonos VoIP que adoptan la forma de software de ordenador o aplicaciones móviles permiten a los usuarios llamar y recibir llamadas directamente desde la interfaz del software. Estos teléfonos VoIP también pueden integrarse con sistemas ERP u otras herramientas de terceros para obtener información. Un ejemplo sería el software CRM.

- **¿Cómo funciona un teléfono VoIP?**

Un teléfono VoIP funciona gracias al poder de la conectividad a Internet y no siempre requiere hardware como o cables telefónicos. A continuación, puede ver una descripción detallada de su modelo de funcionamiento.

Cómo funcionan los teléfonos analógicos



Para entender mejor el funcionamiento de un teléfono VoIP, primero se ha de comprender cómo funciona un sistema telefónico analógico. Este está conectado mediante cables y convierte las señales de voz en señales eléctricas que recorren una cierta distancia antes de llegar al otro extremo de la línea.

Los sistemas analógicos pueden ofrecer una comunicación bidireccional, la cual permite hablar pero también escuchar lo que dice la persona al otro extremo de la línea. Si alguno de los usuarios no tiene una conexión telefónica activa, la conversación no puede tener lugar.

Una mirada detallada al VoIP

Un sistema de telefonía VoIP también funciona sobre el mismo principio que un sistema telefónico tradicional, salvo que los cables telefónicos y el hardware asociados no forman parte de la maquinaria. Además, en lugar de una conexión telefónica, necesita una conexión a Internet, la cual se la puede proporcionar un ISP (proveedor de servicios de Internet). De hecho, los dispositivos móviles con capacidad de red LTE, 4G o 5G también pueden transmitir voz a través de redes de datos.

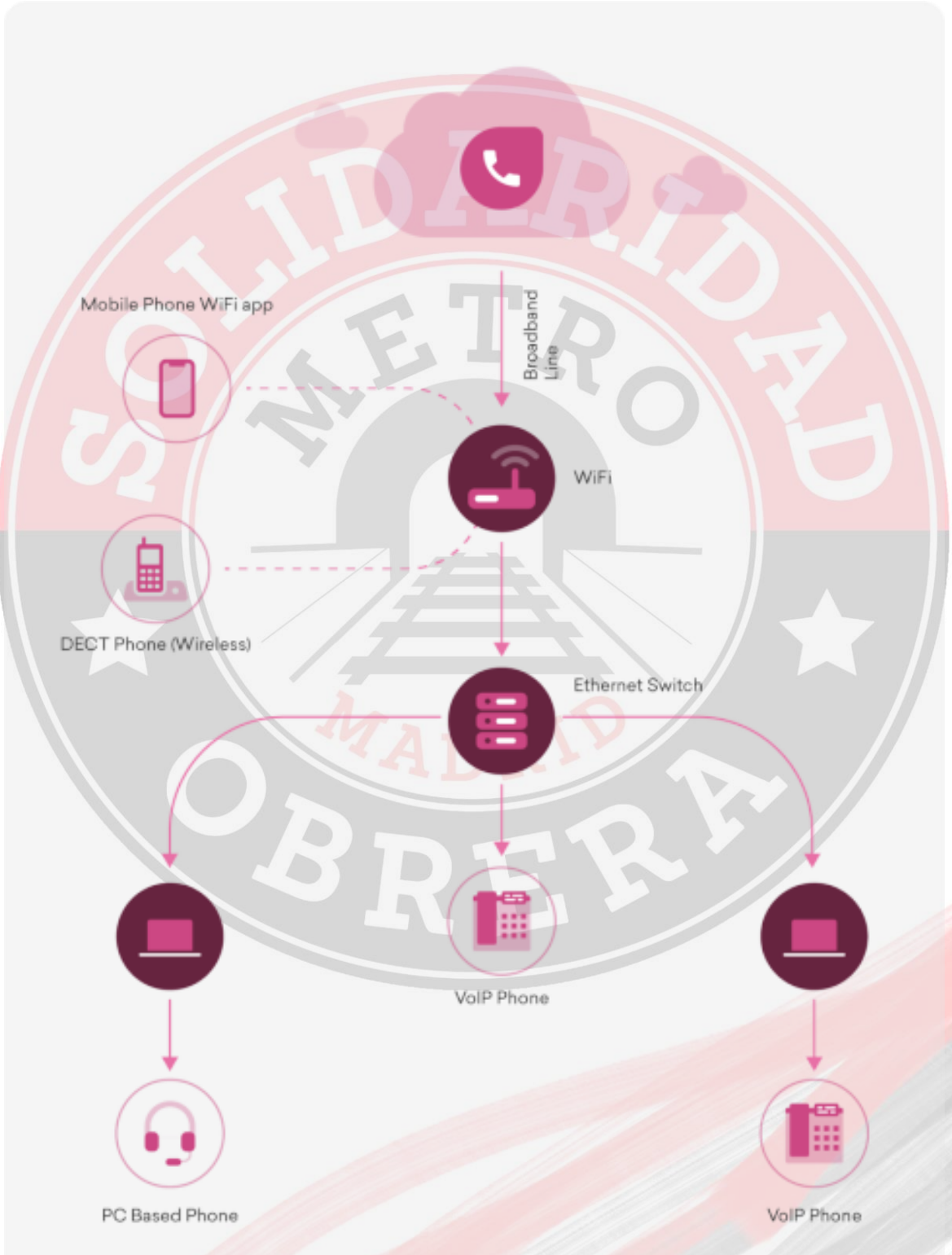
En el VoIP, las señales de voz se convierten en señales digitales. Estas señales digitales se descomponen en cientos de paquetes de datos que se transmiten a través de Internet.

Para simplificar la transferencia de los datos, estos se codifican y ensamblan en paquetes y se distribuyen de un modo aleatorio. Estos paquetes de datos distribuidos después se recomponen en su forma original al llegar a su destino.

En comparación con la conmutación de circuitos de los sistemas telefónicos tradicionales, la conmutación de paquetes de los teléfonos VoIP garantiza una mayor claridad de la voz y un uso eficiente de la red, así como posibilita realizar llamadas a larga distancia sin deficiencias técnicas.

Puede llamar a cualquier línea fija, móvil o número IP desde un sistema VoIP. Para ello no es necesario que el destinatario tenga una conexión VoIP; este puede recibir llamadas en su teléfono analógico como cualquier llamada corriente.

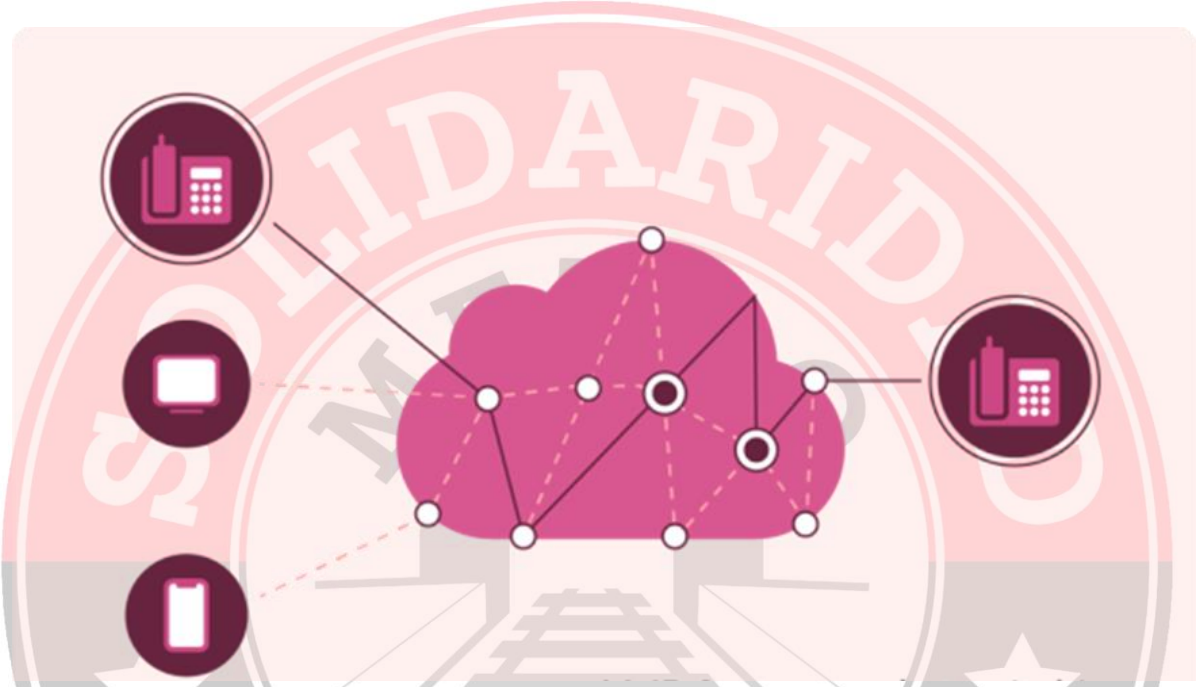
Por ejemplo, mediante el protocolo VoIP usted puede llamar a un amigo que utilice un teléfono fijo o un móvil y su amigo también puede llamarlo a usted desde su fijo o móvil.



En qué consiste la conmutación de paquetes

Los sistemas con tecnología VoIP emplean la conmutación de paquetes, la cual es una forma inteligente de dirigir los paquetes de datos a través de la ruta más eficiente. De hecho, la conmutación de paquetes es la espina dorsal de los teléfonos VoIP. Esta permite el envío de datos de voz a través de redes geográficamente distantes en milisegundos y también evita que los paquetes de datos se rompan o pierdan durante la transmisión.

Como el tamaño de los paquetes ronda los kilobytes, incluso una conexión de Internet de banda ancha puede proporcionar una gran calidad de voz.



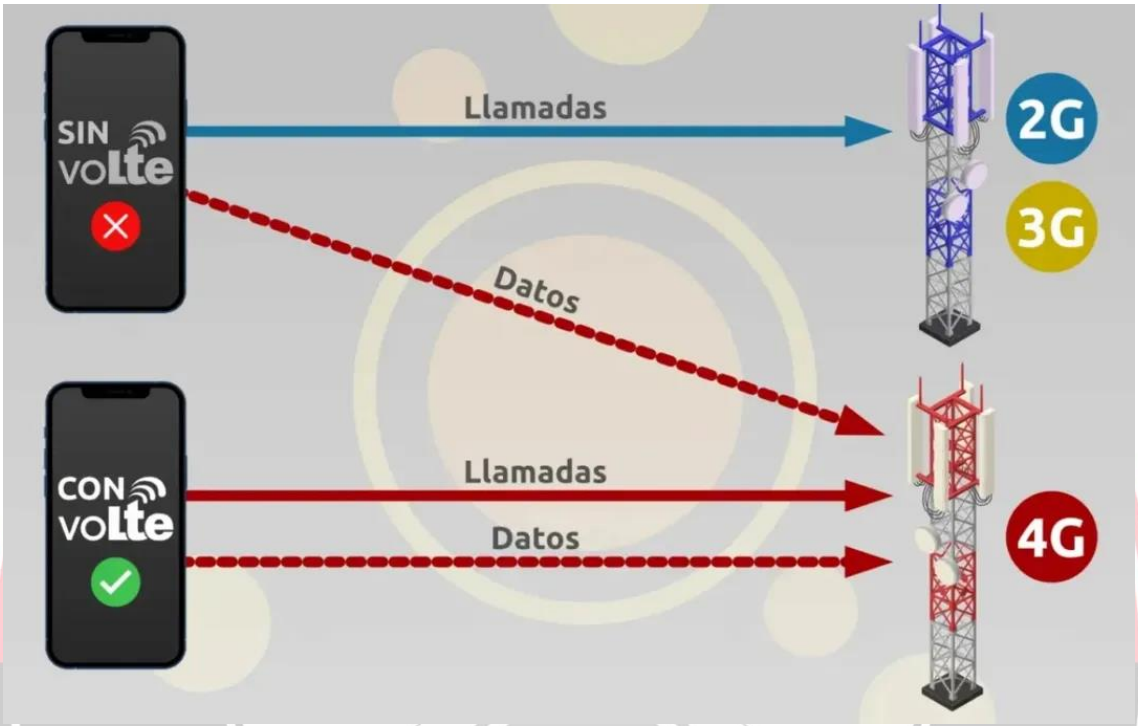
Teléfono VoIP vs. teléfono analógico vs. PBX en la nube

Los sistemas telefónicos tradicionales utilizaban una red de conmutación de circuitos para conectar a quienes realizaban las llamadas con sus destinatarios. Con el protocolo VoIP, este tipo de llamadas empezó a transmitirse en forma de paquetes IP a través de una red de conmutación de paquetes. A continuación, puede ver las diferencias en características y prestaciones de los teléfonos VoIP, de los analógicos y de los PBX en la nube.

Características	TELÉFONO VOIP	Teléfono analógico	PBX en la nube
Conectividad	Internet de banda ancha	Cables de cobre	Internet de banda ancha, 5G, LTE, etc.
Sistema de servidores	PBX en la nube o alojado	PBX físico local	Servidor en la nube
Requisito de ancho de banda	10 kbps	64 kbps	10 kbps
Soporte multimedia	Permite voz, audio, vídeo y cualquier otro medio a través de Internet	Solo voz	Permite voz, audio, vídeo y cualquier otro medio a través de Internet
Capacidades	Buzón de voz, integraciones de software, aplicaciones móviles, etc.	Incapaz de contar con buzón de voz o integraciones	Usado como el medio que permite llamadas de VoIP, establecer números virtuales, flujos de llamadas, etc.
Actualizaciones del sistema	Actualizaciones OTA o de software	Instalación y mantenimiento manuales	Actualizaciones de software OTA
Instalación	Usando un PC, portátil o smartphone	PBX, cajas de circuitos, teléfonos fijos, conexiones de líneas y cables de cobre	Normalmente por suscripción como producto SaaS
Idóneo para	Empresas de todo tipo y tamaño	Equipos cercanos y siempre físicamente disponibles	Empresas de todo tipo y tamaño

6.4.2.2. REDES MÓVILES Y VOLTE:

Las redes móviles han evolucionado significativamente en las últimas décadas, permitiendo mejorar la calidad y velocidad de la transmisión de voz y datos. VoLTE (Voice over LTE) es una de las innovaciones más relevantes en este ámbito, ofreciendo llamadas de alta definición y mayor eficiencia espectral en comparación con tecnologías anteriores como 2G y 3G.



Evolución de las Redes Móviles y la Introducción de VoLTE

1. **Redes 2G y 3G:**
   - En las primeras generaciones de redes móviles, la transmisión de voz se realizaba mediante tecnología de conmutación de circuitos, lo que limitaba la calidad del audio y la eficiencia del espectro.
   - La llegada de 3G permitió la introducción de tecnologías de conmutación de paquetes, mejorando el uso del ancho de banda y facilitando servicios de datos más avanzados.
2. **Transición a 4G y el Nacimiento de VoLTE:**
   - Con el despliegue de LTE (Long Term Evolution), se buscó optimizar la capacidad de la red y mejorar la eficiencia en la transmisión de datos.
   - VoLTE permite que las llamadas de voz se realicen a través de la red 4G sin necesidad de cambiar a 3G, lo que reduce la latencia y mejora la calidad del audio.

Características y Ventajas de VoLTE

- **Mayor calidad de voz:**
  - Utiliza códecs de audio avanzados como **AMR-WB (Adaptive Multi-Rate Wideband)** para proporcionar sonido en alta definición.
  - Reduce la latencia en las llamadas, lo que mejora la experiencia del usuario.
- **Eficiencia espectral:**
  - Aprovecha el espectro de manera más eficiente en comparación con 2G y 3G, permitiendo una mayor cantidad de llamadas simultáneas con menor consumo de recursos.
  - Facilita la coexistencia de servicios de voz y datos en la misma red LTE.
- **Menor consumo de batería:**
  - A diferencia de las llamadas en 3G, que requieren cambios de red durante la llamada, VoLTE permite que los dispositivos permanezcan en 4G sin interrupciones, optimizando el consumo energético.
- **Soporte para llamadas en redes IP:**
  - VoLTE es completamente compatible con servicios de telefonía IP, permitiendo una integración más fluida con plataformas como VoIP y llamadas Wi-Fi.

Desafíos y Limitaciones de VoLTE

- **Compatibilidad de dispositivos:**
  - No todos los teléfonos móviles son compatibles con VoLTE, lo que puede limitar su adopción en algunos mercados.
- **Cobertura de red LTE:**
  - En regiones donde la cobertura LTE aún es limitada, las llamadas VoLTE pueden no estar disponibles, obligando a los dispositivos a retroceder a redes 3G para realizar llamadas.
- **Interoperabilidad entre operadores:**
  - En algunos casos, los operadores móviles pueden no tener acuerdos de interconexión VoLTE, lo que puede afectar la calidad y disponibilidad del servicio en llamadas entre distintas redes.

Futuro de VoLTE y su Integración con 5G

- Con la llegada de las redes **5G**, VoLTE seguirá desempeñando un papel clave en la transición hacia **VoNR (Voice over New Radio)**, que permitirá mejorar aún más la calidad y eficiencia en la transmisión de voz.
- Se espera que VoLTE siga siendo la base para la voz en las redes móviles hasta que 5G esté completamente implementado a nivel global.

Conclusión

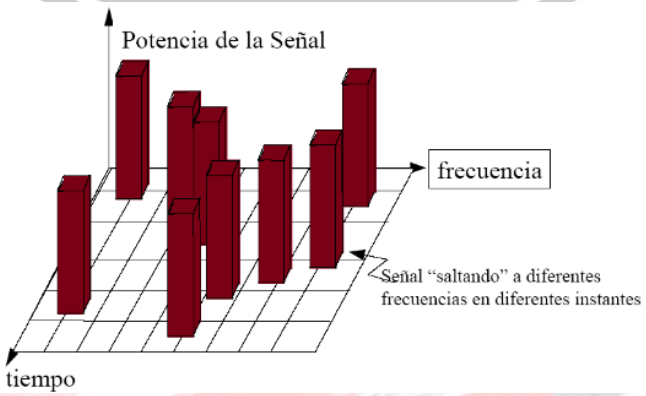
Las técnicas de modulación y demodulación son esenciales para el funcionamiento eficiente de las redes de datos y voz. Gracias a los avances en la tecnología de telecomunicaciones, la calidad de las comunicaciones ha mejorado significativamente, permitiendo la transmisión de información con mayor velocidad, menor latencia y mayor seguridad. La continua evolución de estas tecnologías permitirá nuevas aplicaciones en el futuro, impulsando la conectividad global y la digitalización de la sociedad.

6.4.2.3. SISTEMAS DE RADIOCOMUNICACIONES:

Los sistemas de radiocomunicaciones permiten la transmisión de información mediante ondas electromagnéticas en diferentes rangos de frecuencia. Estos sistemas son fundamentales para la comunicación en sectores como la seguridad pública, el transporte, la industria y la defensa. Su correcto funcionamiento depende del uso de técnicas avanzadas de modulación y demodulación para optimizar el uso del espectro radioeléctrico.

6.4.2.4. Aplicaciones en Seguridad y Defensa

- **Aplicaciones militares, policiales y de seguridad:**
  - La modulación digital es clave en estos sistemas para mejorar la privacidad y la resistencia a interferencias.
  - Se emplean técnicas de cifrado avanzadas y sistemas como **salto de frecuencia (FHSS)** para evitar la interceptación de señales.



- Redes de radio tácticas permiten la comunicación segura en operaciones militares y de emergencia.

- **Uso de técnicas como FSK y PSK en sistemas de radio bidireccional:**
  - **FSK (Frequency Shift Keying):** Se usa en radios digitales para garantizar comunicación estable y sin errores en entornos con ruido.
  - **PSK (Phase Shift Keying):** Ofrece mejor eficiencia espectral y se utiliza en sistemas de radiocomunicación satelital y encriptada.

VER EN 6.2.1.2. MODULACIÓN DIGITAL

- **Implementación de protocolos como DMR (Digital Mobile Radio) para mejorar la interoperabilidad:**
  - DMR permite la comunicación segura entre distintas agencias de seguridad y emergencias.
  - Utilizado en bomberos, policía y organismos de respuesta rápida para garantizar conectividad en tiempo real.

6.4.2.5. APLICACIONES EN SERVICIOS DE EMERGENCIA:

Los servicios de emergencia dependen de sistemas de comunicación confiables y robustos para garantizar una respuesta eficiente en situaciones críticas.

- **Redes de telecomunicaciones críticas con modulación robusta:**
  - Se utilizan esquemas de modulación avanzados para mantener la comunicación en entornos con alta interferencia.

- Redes privadas de radio y comunicaciones satelitales aseguran conectividad en desastres naturales.

- **Tecnologías como TETRA y P25:**

- **TETRA (Terrestrial Trunked Radio):**

Las redes de comunicación por **radio TETRA** se han probado en diferentes campos, por lo que se ha demostrado que consiguen funcionar de manera óptima en caso de que sea necesario tener una comunicación alternativa a la actual. Sin embargo, no todo el mundo conocer qué es y para qué sirve esta red en particular.

Por esto mismo, en RedesZone os explicaremos desde cero en qué consiste y para qué se puede utilizar, ya que puntos como, la seguridad y confiabilidad, son algunas de sus principales características. De esta manera tendrás la oportunidad de conocer más a fondo en qué cosiste este tipo de tecnología en concreto y para qué sirve.

Qué es TETRA, presente y futuro

TETRA viene de la siglas en inglés Trans European Trunked Radio. Nos encontramos con un estándar definido por el Instituto Europeo de Normas de Telecomunicaciones. Esta normativa se creó por decisión de la Unión Europea. Su **finalidad** es **unificar diversas alternativas de interfaces de radio digitales para la comunicación** entre los **profesionales de los servicios de emergencias y servicio público**.

En términos generales, esta tecnología es tanto segura, confiable como robusta y llena de todo tipo de funcionalidades. Además de que hay que contar que se puede ampliar sin problemas. Por ejemplo, los servicios de emergencia en Europa utilizan las siguientes frecuencias:

Servicios de Emergencia		
Número	Pareja de frecuencias (MHz)	
	Banda 1	Banda 2
1	380-383	390-393
2	383-385	393-395

El congreso **Critical Communications World** se celebra todos los años para tratar estos temas relacionados con las comunicaciones de emergencias. En la edición 20 celebrada en Berlín se vio como el 4G/LTE se estaba haciendo hueco poco a poco dentro de este sector y hoy ya es una realidad. También **el estándar abierto MCOP** se sigue preparando por si un día puede llegar a sustituir a TETRA.

Actualmente **TETRA** continúa siendo la **red que más equipos de comunicación críticos utilizan**. En cuanto a futuro, como veremos más adelante, ya se han hecho pruebas con 5G, aunque todavía queda mucho camino por recorrer. La cobertura 5G en muchas grandes ciudades es una realidad, pero todavía queda bastante trabajo por realizar.

Principales características

Este estándar, que se trata de un sistema móvil digital de radio, cuenta con una serie de **características clave** que hay que conocer para tener una idea más a fondo de lo que consiste y, sobre todo, para tener en cuenta cómo puede trabajar posteriormente la red TETRA. Por lo tanto, estas son las especificaciones más relevantes que se deben conocer:

- Uno de los primeros puntos es que la infraestructura de esta red es propia, es decir, está diferenciada completamente de las redes móviles de nuestro país, ya que las estaciones repetidoras trabajan a mayor distancia.
- Hay que tener en cuenta que esta red puede ponerse en modo terminal a terminal si se da algún problema en las comunicaciones.
- Se trata de un sistema digital que está más modernizado que GSM.
- Ofrece una calidad de sonido por encima de GFM, el motivo es que puede usar sistemas más modernos a la hora de comprimir los datos.
- Puede aprovechar mejor el canal. Esto se basa a que permite comunicaciones semidúplex como es el ejemplo de la radio convencional o hasta dúplex como el teléfono. Así que puede hacer uso de canales que estés desocupados.
- La capacidad que ofrece para la transmisión de datos están ya definidas por el estándar inicial y únicamente se pueden comparar al patrón GPRS.
- Tiene una menor saturación, por lo que se encarga de garantizar una capacidad por defecto que está por encima de los canales de comunicación más convencionales.
- Ofrece comunicaciones grupales.
- Cuenta con terminales específicos.
- Tiene encriptación para las comunicaciones.

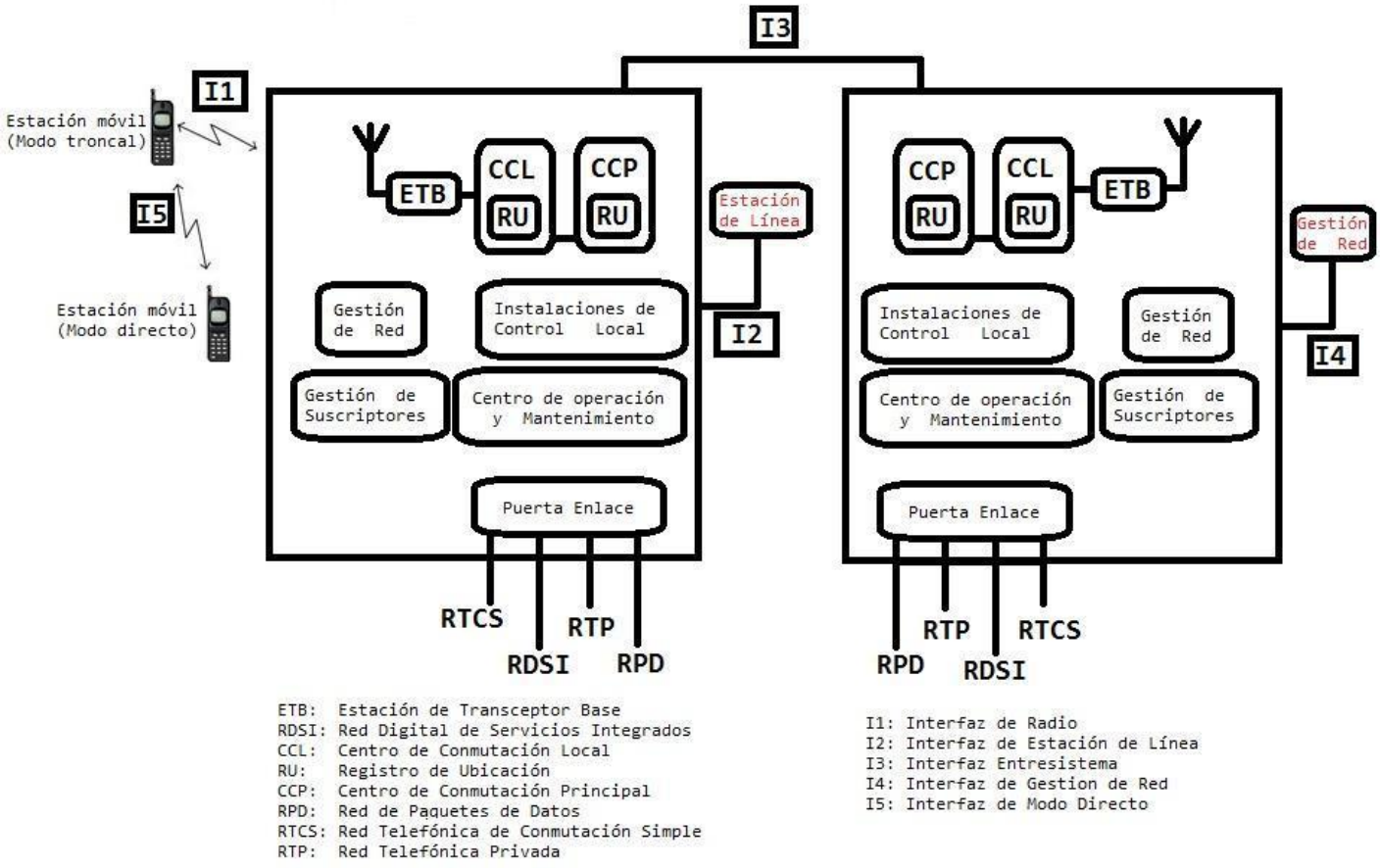
Cómo trabaja la red TETRA

El **ETSI,** cuyas siglas traducidas al español significan **Instituto Europeo de Estándares de Telecomunicación** en el periodo de los años 90 se propuso como objetivo el desarrollo de un estándar abierto para comunicaciones críticas para sustituir a las radios analógicas. Así con este objetivo en el ámbito europeo se creó TETRA, que terminó

desbancando a **Proyect 25**, otro estándar de comunicaciones por radio empleado en Estados Unidos y Canadá.

Actualmente TETRA **opera en más de 100 países repartidos por todo el mundo**. La respuesta al porqué está presente en tantos países es fácil de entender. TETRA, debido a las ventajas que nos ofrece frente a las otras infraestructuras para redes críticas existentes, ha llevado a administraciones y organizaciones privadas a decantarse por ella.

Una de las razones que les ayudó a ganar esta lucha fue que **la mayoría de los países del mundo tienen reservada una banda para comunicaciones críticas** que suele estar



en torno a los 380-400 MHz como se puede observar en la tabla que pusimos en el primer apartado. Además, esto ofrece otra ventaja adicional, al estar usando una frecuencia tan baja, permite alcanzar una mayor cobertura por cada una de las antenas instaladas. Esto mismo también se podrá aplicar al 5G cuando se utilicen los 700 MHz frente a bandas de frecuencias más altas.

También otra ventaja muy importante es que **no tenemos una dependencia absoluta de la red para poder comunicarse con terminales TETRA**. Así, en eventos de emergencias como los de catástrofes naturales, las infraestructuras de comunicación como las redes móviles pueden sufrir daños y caer. El peligro es que para que vuelvan a funcionar bien de nuevo pueden tardar días e incluso semanas.

Por otra parte, con **TETRA es posible la comunicación punto a punto sin necesidad de tener una red en pie.** Hay que señalar que no va a ser con el mismo alcance, pero al menos tendremos comunicación entre usuarios en unos momentos que pueden ser críticos.

Los equipos de comunicación TETRA que utilizamos para tener una comunicación lo más instantánea y casi en tiempo real serían:

- Radios tipo walkie-talkie.
- Terminales fijos.
- Algunos smartphones

Algunos incorporan un botón push-to-talk que nos pone casi de inmediato en comunicación con el resto de los equipos que pulsan el mismo botón. Esta comunicación se produce en menos de un segundo. Además, las transmisiones siempre van a estar protegidas gracias a un cifrado **end-to-end**. Este tipo de comunicaciones se utilizan generalmente para voz, aunque también permiten datos, eso sí a una velocidad muy baja de unos 10 Kbps. Por ese motivo, el de la muy baja velocidad de transferencia de datos se está planteando dar un salto hacia nuevas tecnologías.

Territorio de la red TETRA

La **cobertura de la red TETRA** puede variar según el despliegue y la infraestructura implementada en cada región. Esta utiliza tecnología de radio digital que opera en diferentes frecuencias. Las frecuencias pueden variar en diferentes países y regiones, ya que están asignadas por los organismos reguladores correspondientes. Las bandas de frecuencia asignadas para TETRA suelen estar en la gama de 380 MHz a 430 MHz, aunque también se utilizan otras frecuencias en algunas áreas.

En términos de cobertura geográfica, la red TETRA puede tener alcance local, regional o nacional, dependiendo de la infraestructura desplegada por el operador de la red. Por lo general, se espera que **una red TETRA** proporcione cobertura confiable dentro de su área de servicio designada.

Es por esto mismo por lo que, en áreas urbanas densamente pobladas, donde la demanda de comunicaciones es alta, es común encontrar una **amplia cobertura** de la red TETRA, especialmente en áreas metropolitanas importantes. Esto se logra mediante la instalación de múltiples estaciones base que brindan cobertura a los usuarios en diferentes ubicaciones de la ciudad. En áreas rurales o menos densamente pobladas, la cobertura de la red TETRA puede ser más limitada. Esto se debe a que la infraestructura de la red puede estar más concentrada en áreas urbanas donde la demanda es mayor. En estos casos, es posible que se utilizan repetidores o estaciones base adicionales para ampliar la cobertura en áreas remotas.

Es importante tener en cuenta que la cobertura de la red TETRA puede variar incluso dentro de una región determinada. Factores como el relieve del terreno, la densidad de

la vegetación y la presencia de obstáculos físicos pueden afectar la calidad de la señal y la cobertura de la red. Por lo tanto, es posible que algunas áreas geográficas específicas experimenten áreas con señal más débil o falta de cobertura. Dificultando así las comunicaciones.

Ventajas de TETRA

El uso de la red TETRA lo cierto es que da una serie de beneficios. Y es que, como toda tecnología, este tipo de comunicación alternativa tiene una serie de puntos a favor por las que se considera como una buena opción. Entre ellos, nos encontramos los siguientes aspectos:

- Puede ofrecer una cobertura a nivel local, regional o nacionales.
- Los costes de esta red son bajos, además de que no tiene tarifas de tiempo como puede ser el caso de otras tecnologías como la telefonía móvil.
- Ofrece un alto grado de control, ya que permite, entre otros puntos, configuraciones más personalizadas del sistema.
- Las comunicaciones son de calidad, tanto en la transmisión de datos como de voz.
- La seguridad es uno de sus puntos fuertes, dado que cuenta con un sistema de cifrado y autenticación mutua.
- Tiene una infraestructura propia, la cual está separada de las redes móviles.
- Buena capacidad: hay que tener en cuenta que este sistema en particular se ha diseñado para ofrecer una comunicación sin problemas. Cuenta con espectro licenciado dedicado y un tamaño ideal para cada caso.

Desventajas de TETRA

Pese a que todo parecen ventajas gracias a este sistema de comunicación de emergencia, sí que existen desventajas que no lo hacen ideal, y que deberíamos conocer, entre las que se encuentran las siguientes:

- **Velocidad de transmisión de datos reducida:** Este tipo de redes proporcionan velocidades relativamente bajas, por lo que será complicado mantener una comunicación fluida con ciertas aplicaciones que requieren un ancho de banda mayor.
- **Costes de implementación y mantenimiento:** Como es de suponer, mantener e instalar este tipo de sistemas no es nada barato, pese a ser necesarios, por lo que, en comparación con dispositivos de comunicación convencionales, tendremos un coste mucho mayor.

- **Problemas de interoperabilidad:** Aunque TETRA sí está diseñado para ser interoperable, en la práctica, su integración con otros sistemas no es tan sencillo, pudiendo no solo ser complicada, sino costosa, lo que hace que, con otros proveedores, no sea muy rápido y fácil de realizar.

- **Vulnerabilidades de seguridad**: Recientemente, se han identificado vulnerabilidades en los algoritmos de cifrado de TETRA, como la debilidad intencionada en el cifrado TEA1, que reduce su seguridad efectiva y podría permitir la interceptación de comunicaciones.

- **Cobertura limitada:** En áreas rurales, al igual que otras redes, TETRA puede tener problemas de señal, lo que dificulta la comunicación, y por tanto, requiere de infraestructuras especiales, lo que no siempre es posible, además de costoso.

- **Tecnología antigua:** Pese a que a día de hoy sigue siendo efectiva, este tipo de tecnología es bastante antigua, lo que hace que no se adapte rápidamente a las innovaciones actuales y pueda tener problemas de compatibilidad con aplicaciones.

Existen otro tipo de desventajas, aunque estas serían las más importantes y que no está mal conocer para saber un poco más sobre su funcionamiento.

La transición tecnológica al 4G y 5G

En la CCW, Critical Communications World, durante los últimos años se han presentado terminales TETRA de lo más variado. Aquí, tendríamos desde las clásicas radios hasta los smartphones que combinan TETRA con el 4G. Así tras más de 20 años de funcionamiento TETRA continúa dominado y todos los pronósticos apuntan a que no parará de crecer al menos hasta el año 2023.

Una prueba de la buena salud del negocio es Motorola Solutions que domina este mercado a nivel global. En el primer trimestre del 2021 obtuvo un beneficio de casi 1800 millones de dólares, un 7% más que el del año anterior. No obstante, tras las novedades presentadas en el CCW, vemos el sector de las comunicaciones críticas en plena transición tecnológica. Por ejemplo, ya estamos viendo cómo se han hecho las primeras pruebas con 5G.

Motorola Solutions, en las últimas ediciones del en el CCW no solo ha centrado sus esfuerzos únicamente en las comunicaciones críticas TETRA. Alguna de las novedades más interesantes de la empresa americana ha sido un **smartphone compatible con la red crítica TETRA que además es compatible con LTE y ofrece una red LTE portable**. Esta red portátil es **capaz de ser iniciada y puesta en marcha en cinco minutos y** tiene capacidad para **dar cobertura muy fiable hasta a 100 dispositivos en un radio de un kilómetro.** Otra empresa que también ha estado ofreciendo algo parecido en 4G en cuanto sistema de comunicaciones críticas multimedia es el eLTE MCCS de Huawei.

Las cosas están cambiando y ahora el 4G y el 5G es ya una necesidad, se trata de un requisito con el que quieren contar los usuarios de TETRA en un único dispositivo. En

este caso quieren contar con las ventajas de las últimas generaciones de redes móviles debido a la baja velocidad de transmisión de datos en TETRA y conservar la seguridad que ofrece el viejo estándar.

¿Qué aplicaciones tiene Tetra?

Actualmente, la aplicación más extensa de TETRA es la red de seguridad nacional que incorporan los cuerpos de policía, esto ocurre así en prácticamente todos los países de la Unión Europea. Si nos fijamos en Finlandia, esta red cubre 350.000Km² de su territorio, país en la cual es denominada como **VIRVE**.

Además del anterior punto, si seguimos en los países nórdicos llegamos a Suecia, donde disponen de un plan para cubrir los 450.000Km² de su territorio con TETRA. Si nos acercamos un poco más a España, podemos fijarnos en Bélgica, que disponen de una red llamada ASTRID, que puede cubrir a 10 millones de personas. Ya si salimos de Europa, podemos ver en Beijing, que pueden cubrir a 14 millones de habitantes. En nuestro territorio, gran parte de España está cubierta por esta red.

Como hemos comentado, Tetra está en gran parte de los países de la Unión Europea. Entre ellos, podemos encontrar 17, crearon un grupo de cooperación de la policía, con la finalidad de mejorar la interoperatividad e intercambio de datos entre los centros de control y los diferentes cuerpos. A este sistema se le llama **TETRAPOL**, por la cual se intercambian datos de forma rápida y sencilla. Incluso para ser más segura, en cuanto a ciertas comunicaciones, para evitar interferencias, estas comunicaciones pueden cambiar rápidamente las frecuencias de emisión, de forma que interferir se vuelve muy complicado.

Uno de los grandes problemas, es que el rango de frecuencias que tiene asignado, no es demasiado grande, y puede dividirse en zonas. Por supuesto, entre estas nos podemos mover. El ancho de banda reservado con fines militares es del 29% de las frecuencias disponibles, este porcentaje contrasta con el 0,9% que se usa con fines de seguridad como tal. Como el intervalo de frecuencias es de un tamaño reducido, obliga a los sistemas digital a ser muy efectivos.

Seguridad

La red TETRA se caracteriza por proporcionar más seguridad de tres modos, los cuales son diferentes pero que se encuentran bien interconectados. Esto hace que no haya otras tecnologías que presenten el mismo nivel de seguridad. También se encuentra especialmente diseñada para garantizar la comunicación. Estos modos son:

- **Disponibilidad:** La red está diseñada para responder incluso bajo mínimos, los cuales pueden ser causados por caídas eléctricas, cortes de comunicaciones, problemas estructurales de toda la infraestructura o inconvenientes que pueden aparecer en las estaciones base.

- **Confidencialidad:** Se trata de una red blindada. Esto quiere decir que está totalmente protegida ante escuchas o a que esta sea interceptada. Para ello utiliza algoritmos de cifrado de extremo a extremo entre todos los terminales. Lo cual resulta muy efectivo, ya que no existen registros de que en algún momento se consiguiera interceptar ninguna señal de esta red.

- **Integridad:** Solo los terminales autorizados pueden acceder a este sistema, en parte es porque de este modo se puede verificar que todo el sistema es el adecuado, y no se generan puntos de conflicto. Otra de las ventajas, es que se pueden controlar y crear registros de los tiempos que se tarda en enviar los mensajes y otros datos que pueden circular por ella.

El cifrado con el que cuenta, es muy complicado de establecer en los sistemas de comunicación, y el principal motivo es la capacidad de encriptación. Este protege los terminales de la extracción de claves de seguridad y de cifrado, las cuales son almacenadas también cifradas en entornos de confianza. Algunas de las medidas que esta red integra son:

- **Autenticación:** De esta forma se asegura que los dispositivos están autorizados y tiene acceso.

- **Cifrado de la interfaz aire (AIE):** Establece una protección del tráfico de vos, señalización e identidad en un tramo del radio de la comunicación, el cual va por aire.

- **Deshabilitado de terminales:** Asegura que en el caso de que un terminal se pierda, este no se pueda conectar a TETRA. Lo cual puede ser una amenaza para la integridad de la conexión.

- **Cifrado E2EE:** Protege todos los datos y señalización en toda la línea de comunicación.

MCOP como alternativa a Tetra

A TETRA se le está complicando el camino por el LTE y el futuro 5G. En ese aspecto cada país tiene sus frecuencias reservadas para el despliegue de redes TETRA públicas (policía, ambulancias, bomberos…) y privadas (industrias, redes de metro y más). Por esa razón, tanto las administraciones públicas como empresas privadas tienen que cubrir los gastos del despliegue de estas redes. Si el recinto a cubrir es pequeño tendrá un coste pequeño, pero a medida que se amplía el rango a cubrir también aumenta ese gasto.

La Policía Nacional y la Guardia Civil utilizan SIRDEE (Sistema de Radiocomunicaciones Digital de Emergencia del Estado), sistema al que se han adherido policías locales de distintas ciudades desde otros sistemas TETRA. Por poner un ejemplo, en el País Vasco la red basada en TETRA de titularidad pública se llama Enbor-Sarea y es utilizada por la Ertzaintza y las policías locales. Al final, todo acaba en una mezcla de proveedores y diferencias entre redes que acaban atrapando a las administraciones en un proveedor,

con el sobrecoste que ello supone. El programa SIRDEE en el año 2020 cumplió 20 años y atiende a más de 4 millones de llamadas al año provenientes de ciudadanos que necesitan la atención de la Policía Nacional o de la Guardia Civil.

MCOP quiere liberalizar los sistemas de comunicaciones críticas facilitando la elección de proveedores gracias al uso de código abierto y el desarrollo de soluciones a medida. El alto coste de los despliegues y de los equipos TETRA se reparte entre pocas empresas, por ese motivo nació Mission Critical Open Platform (MCOP). Nos encontramos con una iniciativa financiada por el Departamento de Comercio de Estados Unidos y liderada por la Universidad del País Vasco.

MCOP acaba de publicar el kit de desarrollo de software open source y una aplicación de muestra para el desarrollo de aplicaciones de pulsar y hablar basadas en las especificaciones del 3GPP. Ahora las decisión estará en las empresas y administraciones que podrían ahorrar costes y romper las cadenas que atan a proveedores TETRA si se pasan a MCOP.

El 5G va a cambiar el panorama

El 5G va a cambiar mucho el sector de las comunicaciones críticas debido al **Network Slicing**. Gracias a él los operadores con redes móviles de quinta generación no tendrán una única red, podrán trocearla en subredes con distintos propósitos y ser semi independientes entre sí.

Anteriormente las comunicaciones críticas no habían podido confiar en las redes 3G o 4G por su vulnerabilidad ante grandes aglomeraciones de usuarios. En grandes eventos con mucha gente conectada a una misma antena suele ser bastante común no poder hacer llamadas. El 5G tendrá un cauce dedicado a las comunicaciones críticas y va a hacer que las cosas cambien.

El **Network Slicing** que llegará al 5G permitirá crear un sistema de pequeñas redes paralelas, de manera que si una de ellas se obstruye las demás puedan seguir funcionando. Una de las redes que se separaría sería la de comunicaciones críticas del resto.

La cobertura 5G cada es mayor sobre todo en grandes ciudades, pero hasta que sea completa todavía le quedan unos años en los que TETRA puede estar tranquila, pero tendrá que evolucionar y buscar soluciones si no quiere terminar desapareciendo.

Las primeras pruebas de TETRA con 5G

A finales del año 2019 se produjo la primera prueba de red híbrida TETRA 5G del mundo. Esta prueba se realizó en China concretamente en Guangzhou. La empresa que realizó las pruebas fue Airbus que finalizó con éxito las pruebas de comunicación entre terminales y teléfonos inteligentes 5G de la Red de Radiocomunicación Compartida del Gobierno de Guangzhou y se conectaron por primera vez con la red 5G de China Telecom de Guanzhou

Ahora, los usuarios finales de los organismos gubernamentales pueden experimentar una interoperabilidad total entre las dos redes haciendo uso de la aplicación segura Tactilon Agnet. **Gracias a esta app permite utilizar servicios de voz y datos sin interrupciones conectando** a los usuarios finales de la **red Tetra con los de la red 5G**. Entre los servicios que puede ofrecer encontramos:

- Las llamadas individuales y de grupo.
- Los servicios de mensajería.
- Vídeo y datos compartidos.
- Funciones de geolocalización
- Y pulsar para hablar.

Tactilon Agnet de Airbus, la podemos considerar como una aplicación y una plataforma de colaboración profesional de vanguardia para usuarios con misiones críticas y empresariales. Esta app se instaló en varios dispositivos para el personal del Gobierno de Guangzhou como:

- Teléfonos inteligentes.
- Teléfonos seguros con sistemas de operación dual.
- Cámaras portátiles.
- Teléfonos inteligentes vía satélite.

La Red Tetra compartida del Gobierno de Guangzhou que implementó Airbus fue la primera red híbrida de la región de Asia-Pacífico. Está interconectada con redes 4G de los tres operadores de redes móviles (China Telecom, China Mobile y China Unicom). Por último, con el paso del tiempo y con cada vez más grandes ciudades con cobertura 5G podremos ir viendo más redes de este tipo.

- **P25 (Project 25):**

P25 es la abreviatura de Project 25 y APCO-25, se trata de un estándar de comunicaciones digitales por radio. Esta tecnología es un estándar de TIA (Telecommunications Industry Association) y está apoyada por APCO (Association of Public-Safety Communications Officials-International). Es ampliamente usada en Estados Unidos y Canadá, sería un equivalente al estándar europeo TETRA.

Actualmente se está pasando de la Fase 1 a la Fase 2 del estándar para conseguir un mayor aprovechamiento del espectro radioeléctrico. Además de exigir simulcast en las nuevas concesiones de frecuencias.

Estándar en Norteamérica para radiocomunicaciones de emergencia con alta resistencia a interferencias.

Radios compatibles con el P25, fueron usadas durante el 2012-2017.

- **Integración de geolocalización en redes de emergencia:**
  - La geolocalización permite localizar equipos y personal en tiempo real para mejorar la respuesta ante desastres.
  - Se combinan redes GPS con sistemas de radiofrecuencia para maximizar la eficiencia operativa.

6.4.2.6. REDES DE VOZ SOBRE 5G:

La llegada de las redes **5G** ha permitido mejoras significativas en la transmisión de voz, optimizando la calidad, la latencia y la capacidad de las comunicaciones móviles. Gracias a su arquitectura avanzada, las redes 5G ofrecen mayor eficiencia espectral, soporte para un mayor número de dispositivos conectados y una menor latencia en la comunicación.

Desarrollo de nuevos estándares de transmisión de voz

- **Reducción de la latencia:**
  - 5G permite minimizar la latencia en la transmisión de voz, mejorando la comunicación en tiempo real y reduciendo los retrasos en las llamadas.
  - Esta mejora es crucial para aplicaciones críticas como telemedicina, comunicaciones industriales y videoconferencias de ultra alta definición.

Problemas/ causa	Conexión internet	Códec	Sobrecarga procesos PC	Cascos	Conexión interlocutor
Cortes	☹	☹	☹		☹
Voz inaudible	☹			☹	
Voz robótica	☹		☹		
Voz lejana	☹			☹	
Voz entrecortada	☹	☹	☹		
Crepitaciones	☹				

- **Códecs avanzados para optimizar la calidad de audio:**
  - Se han desarrollado códecs de audio más eficientes, como **EVS (Enhanced Voice Services)**, que proporcionan un audio más claro y con un rango de frecuencia ampliado.
  - Estos códecs permiten una mejor calidad de audio incluso en condiciones de señal débil.

Implementación de VoNR (Voice over New Radio)

- **Evolución de VoLTE:**
  - VoNR (Voice over New Radio) es la evolución de VoLTE y permite la transmisión de voz en redes 5G sin depender de infraestructuras 4G.
  - Esto mejora la continuidad del servicio y optimiza la eficiencia en redes de nueva generación.
- **Beneficios clave de VoNR:**
  - Mayor calidad de voz y video en llamadas gracias a la menor latencia y mayor ancho de banda disponible en 5G.
  - Soporte para comunicaciones de emergencia más confiables, con capacidades de priorización en la red para llamadas críticas.
  - Reducción del consumo de batería en dispositivos móviles, al evitar la conmutación entre redes 4G y 5G.

Uso de inteligencia artificial para mejorar la calidad de voz

- **Optimización de la supresión de ruido:**
  - La inteligencia artificial se emplea en redes 5G para filtrar ruidos ambientales y mejorar la claridad de las llamadas en entornos ruidosos.
  - Los algoritmos de IA analizan patrones de audio y ajustan la calidad de la señal en tiempo real.

- **Ajuste dinámico de la modulación de voz:**
    - Se implementan algoritmos de aprendizaje automático para adaptar la modulación de voz en función de la calidad de la señal y el ancho de banda disponible.
    - Esto permite mejorar la estabilidad de las llamadas y reducir la probabilidad de interrupciones.
- **Análisis predictivo para optimización de redes:**
    - IA permite anticipar posibles fallos en la red y ajustar dinámicamente los recursos de transmisión de voz para maximizar la eficiencia.
    - Se utilizan modelos de predicción para mejorar la asignación de espectro y reducir congestiones en la red.

Integración con tecnologías emergentes

- **Voz en realidad aumentada y virtual (AR/VR):**
    - Las redes 5G, combinadas con VoNR, permiten experiencias inmersivas en realidad aumentada y virtual con comunicación de voz de ultra baja latencia.
    - Esto es clave en aplicaciones de gaming, formación a distancia y asistencia técnica remota.
- **Interoperabilidad con redes satelitales:**
    - La combinación de redes 5G con comunicaciones satelitales permitirá ampliar la cobertura de voz en áreas rurales y remotas.
    - Se están desarrollando estándares para integrar VoNR con redes satelitales LEO (Low Earth Orbit).
- **Conectividad en vehículos autónomos:**
    - La baja latencia de 5G y VoNR es clave para la comunicación en tiempo real entre vehículos autónomos y sistemas de control de tráfico.
    - Se están probando aplicaciones en sistemas de emergencia vehicular que permiten la transmisión de voz con prioridad en la red.

Conclusión

Las técnicas de modulación y demodulación son esenciales para el funcionamiento eficiente de las redes de datos y voz. Gracias a los avances en la tecnología de telecomunicaciones, la calidad de las comunicaciones ha mejorado significativamente, permitiendo la transmisión de información con mayor velocidad, menor latencia y mayor seguridad. La continua evolución de estas tecnologías permitirá nuevas aplicaciones en el futuro, impulsando la conectividad global y la digitalización de la sociedad.

7. INFRAESTRUCTURA DE SISTEMAS DE TELECOMUNICACIONES

7.1. FUNDAMENTOS DE TELECOMUNICACIONES

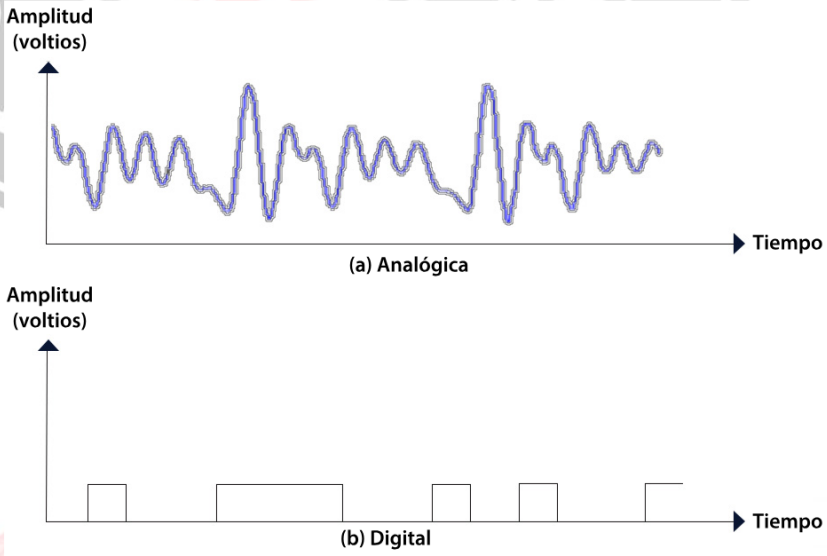
Las telecomunicaciones engloban el conjunto de técnicas y tecnologías que permiten la transmisión y recepción de información a través de diferentes medios. Estos sistemas han evolucionado a lo largo del tiempo, permitiendo la interconexión de dispositivos a nivel global y facilitando el intercambio de datos de manera más rápida y eficiente. Gracias a los avances tecnológicos, hoy en día es posible la comunicación instantánea en prácticamente cualquier parte del mundo.

7.1.1. CONCEPTOS BÁSICOS DE TELECOMUNICACIONES

Las telecomunicaciones abarcan diversos conceptos fundamentales que permiten entender cómo funciona la transmisión de información a través de diferentes medios. Algunos de los conceptos clave incluyen:

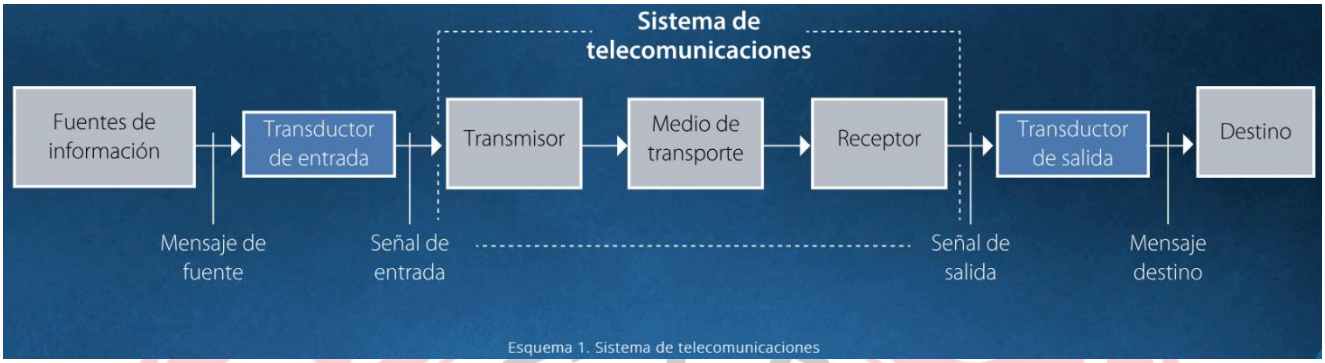
7.1.1.1. EMISOR, MEDIO DE TRANSMISIÓN, RECEPTOR Y UN TRANSFORMADOR DE LA SEÑAL (ENTRE EL EMISOR, EL MEDIO Y EL RECEPTOR).:

El objetivo de un sistema de comunicaciones electrónicas es enviar información a distancia. Este sistema está formado de manera general por los siguientes elementos: **emisor, medio de transmisión, receptor y un transformador de la señal** (**entre el emisor, el medio y el receptor**). Para que la información pueda transmitirse, es necesario auxiliarse de algún tipo de energía portadora, en la cual se codifica la información mediante el proceso llamado modulación. La energía portadora puede ser eléctrica o luminosa, dependiendo del medio de transmisión que se utilice; puede ser fibra óptica, cables de cobre, ondas de radio, entre otros. Las señales que se generan, se procesan, se transmiten y se reciben en el sistema de comunicaciones pueden ser de naturaleza analógica o digital; siempre representan algún tipo de información.



SEÑALES

En el campo de las telecomunicaciones las señales tienen una gran importancia, ya que para instalar un sistema de red o realizar la interconexión de los diferentes dispositivos, es necesario entender cómo funcionan, sus tipos, características y sistemas con los que interactúan. Este tema presenta los conceptos necesarios para entender su función y aplicación en un sistema de comunicaciones, concretamente en las redes de voz y datos para redes de área local (LAN).



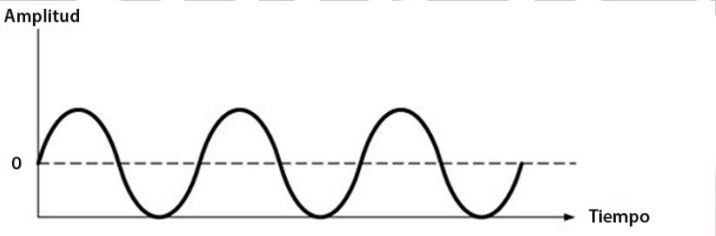
Esquema 1. Sistema de telecomunicaciones

- **Analógicas**

Los sistemas de comunicaciones electrónicas están basados en dispositivos que manejan básicamente dos tipos de señales: analógicas o digitales. En el caso de una señal analógica, ésta varía de forma continua en el tiempo.

Cuando una señal representa alguna magnitud física como temperatura, intensidad luminosa, energía, presión, sonido o campo eléctrico, son señales analógicas que varían constantemente y pueden tomar todos los valores posibles de un intervalo, es decir, que para pasar de un valor a otro, pasa por todos los valores intermedios, por lo que es continua.

Las señales analógicas son percibidas en el ambiente y se transforman en señales eléctricas mediante un transductor, para su tratamiento electrónico



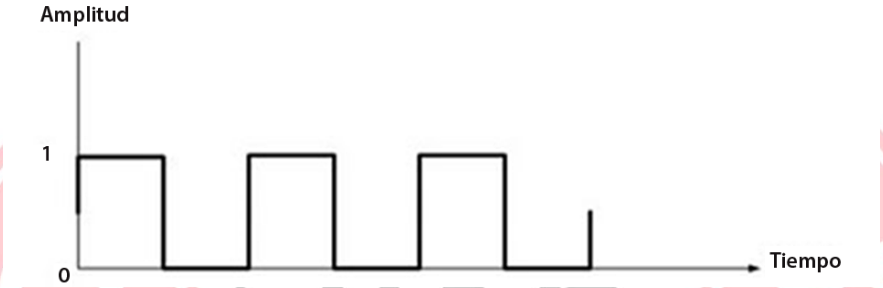
Señales analógicas:

- Son susceptibles al ruido e interferencia electromagnética.
- Presentan grandes atenuaciones en grandes distancias.

- No es posible la regeneración de las señales.
- No conviven con sistemas digitales; hay que instalar equipo adicional para lograr la comunicación con sistemas digitales.

- **Digitales**

Las señales digitales son discretas (valores finitos) en el tiempo y en amplitud; esto significa que la señal sólo puede tomar uno de dos valores (**0** o **1**) en intervalos definidos de tiempo; se pueden considerar ejemplos de señales digitales: un programa de una computadora, el contenido de un CD, entre otros.



Señales digitales:

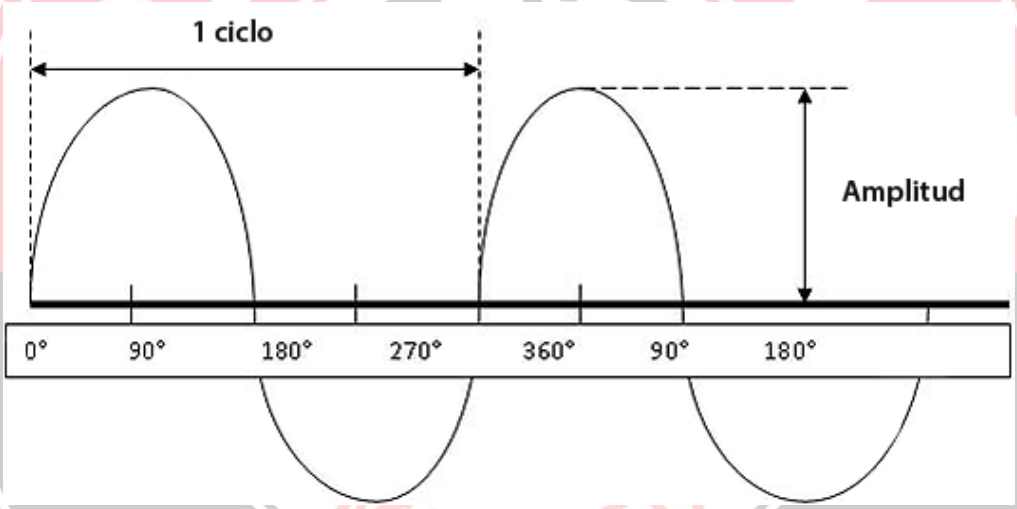
- La ventaja principal de las señales digitales es la inmunidad al ruido electromagnético.
- Convivencia con sistemas digitales (CD-ROM, estéreo, etc.).
- Es posible la regeneración de señales.
- Es posible la detección y corrección de errores.
- El procesamiento digital requiere menos potencia eléctrica, componentes más pequeños y, en ocasiones, es de menor precio.
- Son sensibles a la sincronía entre elementos conectados.

Históricamente los sistemas de comunicaciones funcionaron usando las señales analógicas para transmitir información, como en el caso de la voz que tiene esas características y que dio origen a la Red Telefónica Conmutada (RTC). El desarrollo tecnológico y las computadoras en los sistemas de comunicaciones han ocasionado la migración de sistemas analógicos hacia los de tecnología digital. La tendencia es que, por múltiples razones y con el paso del tiempo, las mismas se conviertan totalmente en redes digitales. Son varias las ventajas de las señales digitales respecto a las analógicas: mayor facilidad de uso e instalación, facilidad de mantenimiento, mayor calidad de servicio (QoS) por las técnicas de regeneración de señales que utiliza, así como su menor

costo. Las redes de área local (LAN) son un ejemplo de la digitalización que permite la transmisión de cualquier tipo de información.

CARACTERÍSTICAS DE LAS SEÑALES

Las señales analógicas y digitales se caracterizan por ser de forma variable y tomar una determinada forma según la información que transmiten. Sus características técnicas pueden representarse como la combinación de varias señales de tipo periódico. Su entendimiento es muy importante, ya que nos permite comprender el funcionamiento de los medios de transmisión, equipos de comunicación, estándares de redes LAN y WAN, etc. Por ejemplo, la amplitud puede aplicarse a la atenuación que pueden sufrir las señales en un medio de trasmisión determinado, cuando no se cumplen las normas y estándares establecidos. La frecuencia a la cantidad necesaria de Hz (ancho de banda) que deberá soportar un medio de transmisión alámbrico o inalámbrico de acuerdo con las aplicaciones que soportará: voz, video, datos, videoconferencia, telepresencia, VoIP, etc.



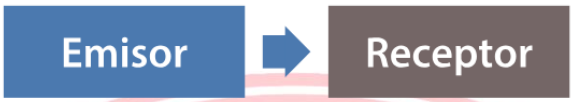
Amplitud (A): Es la distancia entre el punto más alejado de una onda y el punto de equilibrio o medio. La intensidad máxima de la señal o "valor pico" puede ser representada en valores de voltaje o corriente.

MODO DE OPERACIÓN

El modelo general de un sistema de comunicaciones está compuesto por un emisor, un receptor y un medio de transmisión, el cual inicia la comunicación y que, al iniciar la respuesta, puede invertir los roles. La comunicación emisor-receptor puede tener varios modos de operación de las señales, dependiendo de las limitaciones del medio de transmisión de los equipamientos: DCE (Equipo de Comunicación de Datos) y DTE (Equipo Terminal de Datos), y de los procesos del usuario. Un DCE puede ser un conmutador de datos (*switch*), un ruteador o un conmutador de voz, por ejemplo, mientras que un DTE puede ser una computadora o un teléfono, entre otros.

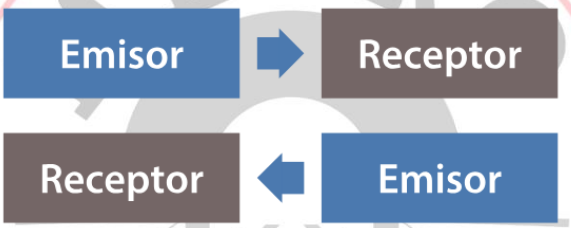
Simplex

En el modo de operación simplex, la comunicación es unidireccional, esto es, mientras un equipo transmite, el otro sólo recibe; en ningún momento el receptor puede tomar el papel de emisor, un ejemplo de este tipo de modo de operación es la TV. En este caso no es el medio de transmisión el que define el tipo de operación, sino el diseño de la aplicación.



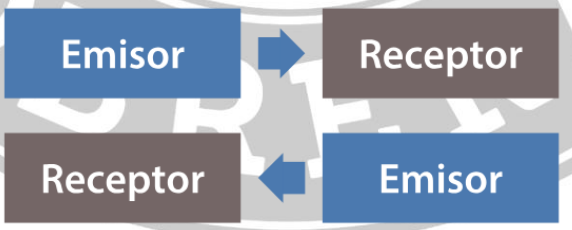
Half duplex

La comunicación half duplex es bidireccional, pero no en forma concurrente; ambos elementos pueden fungir como receptor y emisor, pero nunca de manera simultánea, sino que invierten sus roles. El ejemplo más simple de este tipo de comunicación es el *walkie talkie*.



Full duplex

En el modo full duplex ambos elementos pueden transmitir y recibir de manera simultánea. Ejemplo de este modo lo encontramos en las redes basadas en conmutadores (*switches*) y en equipos de videoconferencia.



MODO DE FLUJO

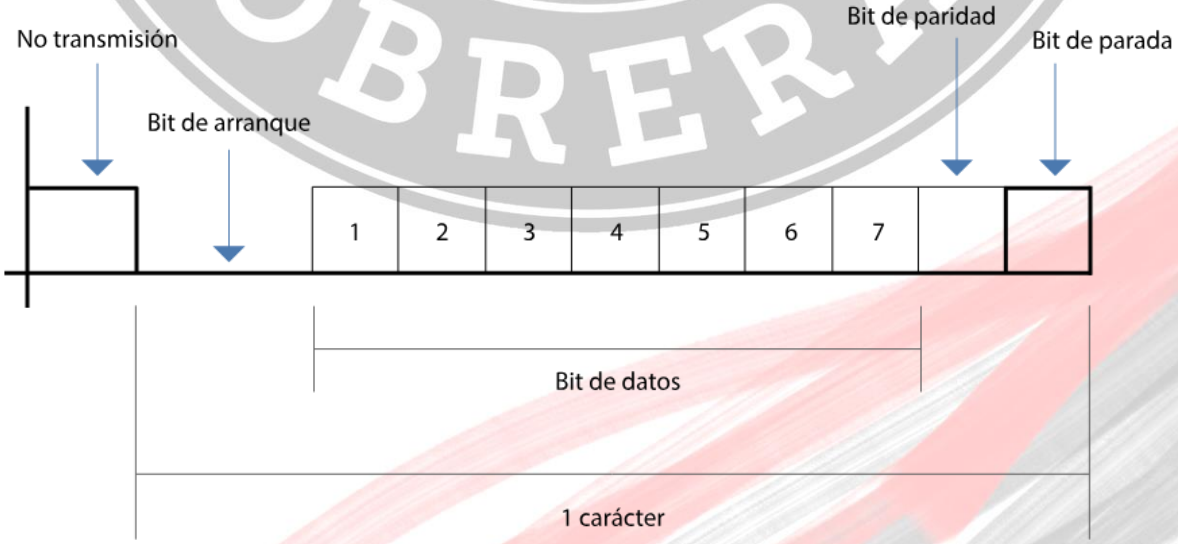
La transmisión de información digital requiere de mecanismos de sincronización para la correcta interpretación de ésta. Si tomamos en cuenta la forma en que se sincronizan el transmisor y el receptor, la transmisión puede ser síncrona y asíncrona (o bien sincrónica y asincrónica).

Síncrona

En esta técnica es necesario sincronizar los relojes de ambos equipos; su ventaja es que se transfiere mayor cantidad de datos por unidad de sincronía. Existen dos tipos: orientada a carácter y orientada a bit.

Asíncrona

En esta técnica no hay necesidad de que emisor y receptor compartan el mismo pulso de reloj; es necesario el uso de bits de inicio y paro, para indicar que el dato está llegando y dar al receptor tiempo suficiente para efectuar operaciones mientras llega el siguiente bit. Tiene un bajo costo de implantación y su desventaja es que tiene un alto desperdicio de la capacidad del canal (*overead*).



7.1.1.2. ANCHO DE BANDA:

El ancho de banda se mide como la cantidad de datos que se pueden transferir entre dos puntos de una red en un tiempo específico. Normalmente, el ancho de banda se mide en bits por segundo (bps) y se expresa como una tasa de bits.

El ancho de banda denota la capacidad de transmisión de una conexión y es un factor importante al determinar la calidad y la velocidad de una red.

Hay varias formas diferentes de medir el ancho de banda. Algunas se utilizan para calcular el flujo de datos en un momento dado, mientras que otras miden el flujo máximo, el flujo típico o lo que se considera un buen flujo.

El ancho de banda también es un concepto clave en muchas otras áreas tecnológicas. Por ejemplo, en el procesamiento de señales se usa para describir la diferencia entre las frecuencias superior e inferior en una transmisión como una señal de radio, y se mide típicamente en hercios (Hz).

Se puede comparar el ancho de banda con el agua que fluye a través de una tubería. El ancho de banda sería la velocidad a la que el agua (los datos) atraviesa la tubería (la conexión) bajo diversas circunstancias. En lugar de bits por segundo, podríamos medirla en litros por minuto. La cantidad de agua que posiblemente pueda fluir a través de la tubería representa el ancho de banda máximo, mientras que la cantidad de agua que fluye en un momento dado a través de la tubería representa el ancho de banda actual.

Originalmente, el ancho de banda se medía en bits por segundo y se expresaba como bps. Sin embargo, hoy en día las redes suelen tener un ancho de banda mucho mayor que el que se puede expresar cómodamente utilizando unidades tan pequeñas. Actualmente, es común ver números mayores que se denotan con prefijos métricos como Mbps (megabits por segundo), Gbps (gigabits por segundo) o Tbps (terabits por segundo).

Unidades de ancho de banda

Unidad de ancho de banda	Abrev.	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1 kbps = 1.000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1.000.000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1.000.000.000 bps = 10^9 bps

Después de terabit existe el petabit, el exabit, el zettabit y el yottabit, y cada uno representa una potencia adicional de 10.

El ancho de banda también se puede expresar en bytes por segundo, lo que generalmente se denota con una B mayúscula. Por ejemplo, 10 megabytes por segundo se expresarían como 10 MB/s o 10 MBps.

Un byte son ocho bits.

De ese modo, 10 MB/s = 80 Mb/s.

Se pueden usar los mismos prefijos tanto con bytes como con bits. Por lo tanto, 1 TB/s es un terabyte por segundo.

7.1.1.3. MODULACIÓN:

- Proceso mediante el cual una señal de información se adapta para ser transmitida a través de un canal específico.
- Existen diferentes tipos de modulación, incluyendo modulación de amplitud (AM), modulación de frecuencia (FM) y modulación digital (PSK, QAM, etc.).

VER 6.2.1. TIPOS DE MODULACIÓN

7.1.1.4. MULTIPLEXACIÓN:

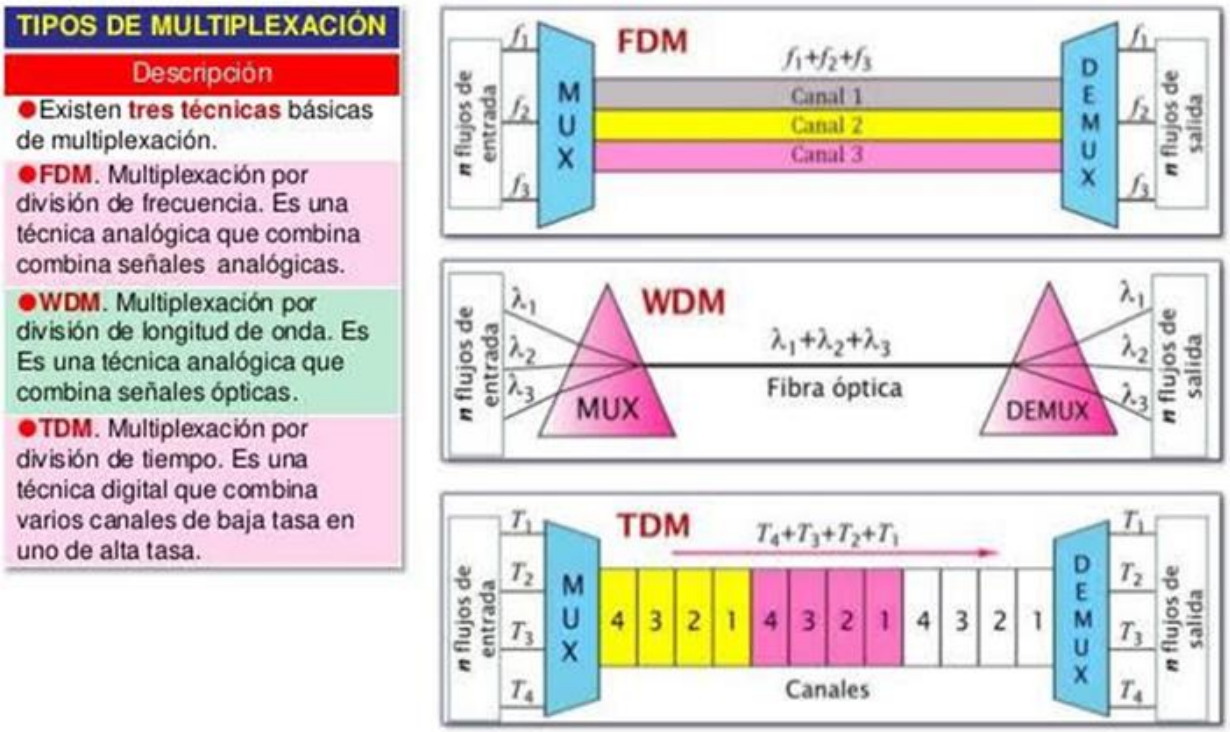
En telecomunicación, la **multiplicación** es la técnica de combinar dos o más señales, y transmitirlas por un solo medio de transmisión. La principal ventaja es que permite varias comunicaciones de forma simultánea, usando un dispositivo llamado multiplicador. El proceso inverso se conoce como demultiplicación. Un concepto muy similar es el de control de acceso al medio.

Existen muchas estrategias de multiplexación según el protocolo de comunicación empleado, que puede combinarlas para alcanzar el uso más eficiente; los más utilizados son:

- la multiplicación por división de tiempo o TDM síncrona (*Time division multiplIxing*);
- la multiplicación estadística o TDM asíncrona o TDM estadística (técnica más avanzada que la anterior);
- la multiplicación por división de frecuencia o FDM (*Frequency-division multiplIxing*) y su equivalente para medios ópticos, por división de longitud de onda o WDM (de *Wavelength*); VER 6.4.1.4 REDES ÓPTICAS Y FIBRA ÓPTICA
- la multiplicación por división en código o CDM (*Code division multiplixing*);

Cuando existe un esquema o protocolo de multiplicación pensado para que múltiples usuarios compartan un medio común, como por ejemplo en telefonía móvil o WiFi, suele denominarse control de acceso al medio o método de acceso múltiple. Como métodos de acceso múltiple destacan:

- el acceso múltiple por división de frecuencia o FDMA;
- el acceso múltiple por división de tiempo o TDMA;
- el acceso múltiple por división de código o CDMA.



Multiplexación en telecomunicaciones

En las telecomunicaciones se usa la multiplexación para dividir las señales en el medio por el que vayan a viajar dentro del espectro radioeléctrico. El término es equivalente al control de acceso al medio.

De esta manera, para transmitir los canales de televisión por aire, vamos a tener un ancho de frecuencia x, el cual habrá que multiplexar para que entren la mayor cantidad posible de canales de TV. Entonces se dividen los canales en un ancho de banda de 6 MHz (en gran parte de Europa y América, mientras que en otros países el ancho de banda es de 8 MHz). En este caso se utiliza una multiplexación por división de frecuencia FDM.

Otro ejemplo es el espectro radioeléctrico usado por el Wi-Fi, que tiene un espaciado de canales de 20/40/80 MHz dependiendo de tecnología.

7.1.1.5. LATENCIA Y VELOCIDAD DE TRANSMISIÓN:

LATENCIA

En la era digital actual, donde las operaciones se miden en milisegundos, un pequeño retraso puede tener un gran impacto. Este retraso, conocido como latencia de red, es un factor crítico en la eficiencia de la transmisión de datos que afecta tanto a la experiencia del usuario como a las operaciones empresariales. Curiosamente, un aumento en la latencia de solo unos pocos milisegundos puede reducir significativamente la productividad y afectar negativamente los resultados financieros de una compañía. Este blog explorará qué es la latencia de red, su importancia en el entorno digital actual, y cómo las empresas pueden implementar estrategias efectivas para mitigar su impacto. Entenderemos cómo un aspecto tan técnico se convierte en esencial para el rendimiento óptimo en un mundo tecnológicamente avanzado.

¿Qué es la Latencia de Red?

La latencia de red se refiere al tiempo de demora que experimentan los datos al ser transmitidos a través de una red. Una latencia elevada significa mayor retardo, afectando negativamente la velocidad de respuesta, mientras que una latencia baja implica una comunicación más rápida y eficiente. Las organizaciones valoran reducir la latencia para optimizar su productividad y la eficiencia operativa. Sectores que requieren computación intensiva, como la dinámica de fluidos, dependen crucialmente de una baja latencia para funcionar efectivamente.

Diferencias entre 4G, 4G+ y 5G

	4G	4G+	5G
Velocidad (Mbps)	200	1200	10000
Latencia (milisegundos)	**100**	**20**	**1-2**

Datos teóricos máximos. En la latencia, cuanto menor sea el dato mejor.

Importancia de la latencia de la conexión a internet

Con la transformación digital, las empresas adoptan masivamente servicios y aplicaciones en la nube. Los dispositivos conectados y el Internet de las Cosas (IoT) acumulan datos críticos para las operaciones en tiempo real. Una alta latencia puede crear cuellos de botella significativos, disminuyendo la efectividad del aumento en la capacidad de red y afectando tanto la experiencia del usuario como su satisfacción.

¿A qué afecta la latencia de red?

Una latencia de red baja es crucial para una variedad de aplicaciones y servicios que dependen de la transmisión rápida y eficiente de datos. Estas son algunas de las áreas más afectadas por la latencia de red:

- ***Aplicaciones de Análisis de Streaming***

Las aplicaciones que requieren análisis de grandes volúmenes de datos en tiempo real, como subastas en tiempo real, plataformas de trading financiero y juegos multijugador en línea, necesitan una red de baja latencia para garantizar transacciones y operaciones fluidas y exactas. Cualquier retardo puede resultar en pérdidas financieras o disminución de la experiencia del usuario.

- ***Gestión de Datos en Tiempo Real***

Las empresas modernas frecuentemente recolectan, procesan y analizan datos de una variedad de fuentes, incluyendo dispositivos IoT, bases de datos transaccionales y aplicaciones en la nube. Utilizan tecnologías avanzadas como la captura de datos de cambio (CDC) para gestionar estos datos en tiempo real. La latencia alta puede complicar estas operaciones, llevando a decisiones basadas en información desactualizada.

- ***Integración mediante API***

Las interfaces de programación de aplicaciones (API) son esenciales para la integración de diferentes sistemas tecnológicos y plataformas de software. Desde servicios financieros hasta operaciones de comercio electrónico y sistemas de reserva, las respuestas de las API tienen que ser rápidas y no obstruir el flujo de procesos críticos. Las APIs facilitan la comunicación entre sistemas distintos, siendo crucial una baja latencia para evitar demoras que afecten operaciones críticas, como la reserva de vuelos.

- ***Operaciones Remotas con Video***

Actividades que involucran control remoto de maquinaria por video, como drones de búsqueda y rescate, requieren redes con baja latencia para prevenir incidentes críticos.

- ***Servicios de VoIP y Conferencias de Video***

La comunicación empresarial a través de VoIP y videoconferencias también requiere latencias bajas para garantizar que las conversaciones sean fluidas y libres de interrupciones o desfases de tiempo, lo cual es crucial para mantener la profesionalidad y efectividad de las comunicaciones comerciales.

¿Qué factores influyen en la Latencia de Red?

La latencia de red puede ser influenciada por múltiples factores:

- **Distancia de Tráfico de Red:** Mayor distancia entre puntos de conexión incrementa la latencia.

- **Número de Saltos de Red:** Múltiples routers intermedios pueden aumentar la latencia.
- **Volumen de Datos:** Un alto volumen de tráfico puede sobrecargar los dispositivos de red, incrementando la latencia.
- **Rendimiento del Servidor:** Servidores lentos pueden ser percibidos como latencia en la red.

¿Cómo medir la latencia de una red?

Se puede monitorear la latencia mediante métricas como el Tiempo hasta el Primer Byte (TTFB) y el Tiempo de Ida y Vuelta (RTT). Estas métricas son herramientas fundamentales para monitorear y mejorar la latencia en redes digitales. Por un lado, el Tiempo hasta el Primer Byte (TTFB) se refiere al tiempo que tarda un navegador web en recibir la primera respuesta desde un servidor después de haber solicitado una página o recurso. Este indicador es crucial para evaluar el rendimiento de los servidores web y la eficiencia de la red en la entrega de contenido.

Por otro lado, el Tiempo de Ida y Vuelta (RTT) es el tiempo total que un paquete de datos tarda en viajar desde el origen hasta el destino y de regreso al origen. Esta métrica proporciona una medida directa de la latencia de red, influyendo en la velocidad y la eficacia de la comunicación entre dispositivos. Un RTT bajo indica una comunicación más rápida y eficiente, mientras que un RTT alto puede señalar congestión de red o distancia física considerable entre los puntos de comunicación.

Optimizar estas métricas implica mejorar la infraestructura de red, reducir la distancia entre servidores y usuarios finales, y optimizar los procesos de entrega de contenido para asegurar una experiencia de usuario fluida y eficiente.

Consejos para mejorar la Latencia de Red

Optimizar la latencia de red es fundamental para mejorar la velocidad y la eficiencia de las comunicaciones digitales. Aquí te ofrecemos algunos consejos prácticos para reducir la latencia y optimizar el rendimiento de tu red:

Conexión por Cable Ethernet: Conectarse mediante cable Ethernet en lugar de WiFi puede reducir significativamente la latencia. Los cables proporcionan una conexión más estable y rápida, ideal para aplicaciones que requieren baja latencia como juegos en línea o transmisión de video en tiempo real.

Mantén tu Sistema Actualizado y Seguro: Asegúrate de que todos los dispositivos estén limpios de malware y actualizados con los últimos parches de seguridad. Las actualizaciones no solo mejoran el rendimiento, sino que también protegen contra vulnerabilidades que podrían ser explotadas por amenazas cibernéticas.

Reduce la Carga de Dispositivos Conectados: Limita el número de dispositivos conectados simultáneamente a tu red WiFi. La sobrecarga de dispositivos puede congestioanr la red inalámbrica y aumentar la latencia.

Actualización de Infraestructura: Moderniza los dispositivos de red utilizando tecnologías más recientes. Equipos obsoletos pueden ser una causa de latencia debido a su menor capacidad de procesamiento y gestión de datos.

Monitoreo de Rendimiento: Utiliza herramientas de monitoreo para identificar y resolver problemas de latencia en tiempo real. Esto te permite detectar cuellos de botella y optimizar la configuración de red para mejorar el rendimiento general.

Agrupación de Puntos de Conexión: Crea subredes para minimizar los saltos de red. Reducir la distancia y el número de nodos entre los dispositivos conectados puede mejorar la latencia al disminuir el tiempo de transmisión de datos.

Reducción de Distancia: Aloja servidores y recursos críticos más cerca de los usuarios finales. Esto reduce el tiempo de viaje de los datos y mejora la respuesta general de la red.

Minimización de Saltos de Red: Reduce la cantidad de saltos de datos a través de la red pública. Evitar rutas indirectas y redundantes puede mejorar la latencia al establecer conexiones más directas y eficientes.

Implementar estos consejos puede ayudarte a optimizar la latencia de red y mejorar la experiencia de usuario, asegurando que tus operaciones digitales sean más rápidas, eficientes y seguras.

La latencia es un aspecto fundamental del rendimiento de la red que afecta significativamente las operaciones comerciales. Una comprensión profunda y una gestión efectiva de la latencia son esenciales para maximizar la eficiencia y satisfacción del usuario en el entorno digital actual. Lynks se compromete a proporcionar soluciones que aborden estas necesidades, asegurando que sus clientes siempre estén un paso adelante en la tecnología de comunicación.

VELOCIDAD DE TRANSMISION

¿Cuál es la diferencia entre velocidad de transmisión de datos y ancho de banda?

A veces, los conceptos de velocidad de transmisión de datos y ancho de banda se utilizan indistintamente. Esto se debe, en gran medida, a las empresas de publicidad y los medios de comunicación, que han convertido un importante término técnico del diseño de circuitos analógicos en una palabra de moda. En la actualidad, la palabra "ancho de banda" se utiliza erróneamente hasta el punto de que, sin querer, ha adquirido un significado algo relacionado con el diseño de convertidores analógico-digitales (ADC).

El ancho de banda tiene una clara connotación que no tiene nada que ver con la velocidad de transmisión de datos. Incluso, a veces se refiere a alguna cualidad de la señal y a su interacción con un receptor.

Dado que la diferencia entre velocidad transmisión de datos y ancho de banda resulta un poco difusa.

Diferencia entre la velocidad de transmisión de datos y el ancho de banda

La velocidad de transmisión de datos es exactamente lo que su nombre indica. Es el número de bits transmitidos a través de un canal o por un componente por unidad de tiempo. La velocidad de transmisión de datos también puede indicarse en baudios (por ejemplo, el número de unidades de señal por segundo). Esto nos permite diferenciar entre los esquemas de señalización binarios y multinivel. Esto es bastante sencillo; para una señal de dos niveles (por ejemplo, los códigos NRZ), la velocidad en baudios es igual a la velocidad en bits. Para las señales de cuatro niveles (por ejemplo, la PAM4), la velocidad en baudios es la mitad de la velocidad en bits, ya que se transmiten dos bits por intervalo unitario (IU).

En cuanto a la definición de ancho de banda, los diseñadores de componentes electrónicos de todo tipo suelen utilizar el término “ancho de banda” para referirse a uno o varios de los siguientes aspectos:

- **Punto de -3 dB.** Se suele utilizar en el diseño de filtros para indicar la frecuencia a la que la función de transferencia del filtro (su magnitud) disminuye en 3 dB.
- **Gama de frecuencias en el que un componente puede recibir/transmitir.** Esto casi siempre se lo he visto hacer a investigadores que trabajan en la integración o el diseño de sistemas, cuando necesitan adaptar un nuevo componente/sistema para recibir/transmitir dentro de un rango de frecuencias específico.
- **Contenido de frecuencias de la señal.** Una señal de banda ancha puede tener su contenido de frecuencias repartido en un amplio rango de frecuencias. El ancho de banda define el tamaño de este espectro.
- **La capacidad de velocidad de transmisión de datos de un canal.** Esta definición de ancho de banda surge del hecho de que la velocidad de transmisión de datos (en realidad, la velocidad en baudios) y el contenido de frecuencia están relacionados, pero normalmente se utiliza para describir los enlaces de fibra o inalámbricos, más que las interconexiones a nivel de la placa.

7.1.2. MEDIOS DE TRANSMISIÓN

Las telecomunicaciones utilizan diversos medios físicos y no físicos para la transmisión de datos. Estos medios pueden dividirse en:

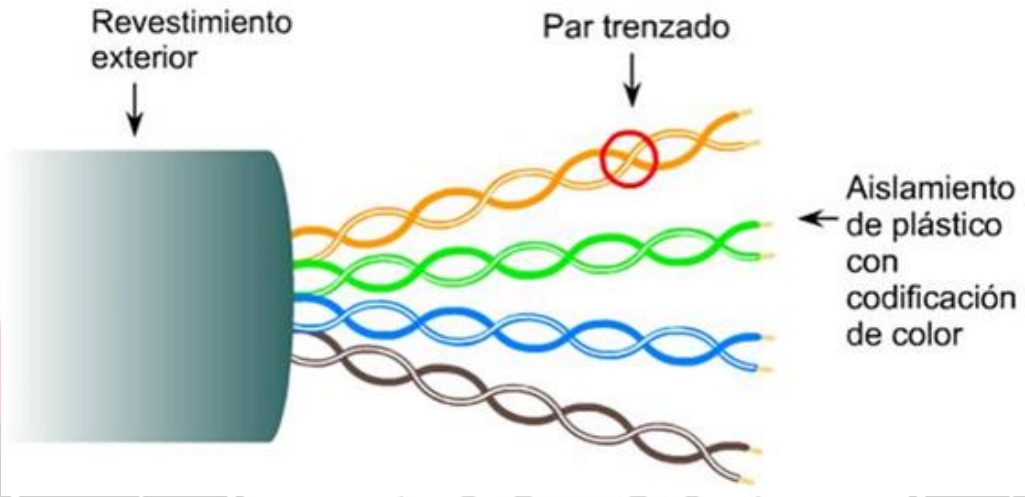
7.1.2.1. MEDIOS CABLEADOS:

VER TAMBIÉN 6.1.4. TIPOS DE CABLES EN TELECOMUNICACIONES

EL PAR TRENZADO

El par trenzado consiste en un par de hilos de cobre conductores cruzados entre sí, con el objetivo de

reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía.



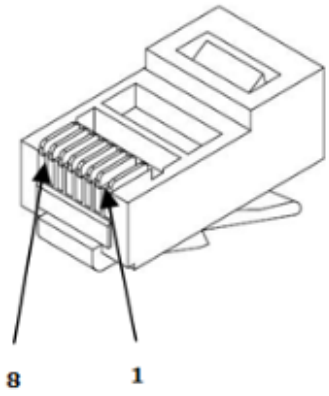
Existen dos tipos de par trenzado:

1) Protegido: Shielded Twisted Pair (STP)
2) No protegido: Unshielded Twisted Pair (UTP)

Las aplicaciones principales en las que se hace uso de cables de par trenzado son:

- **Bucle de abonado:** Es el último tramo de cable existente entre el teléfono de un abonado y la central a la que se encuentra conectado. Este cable suele ser UTP Cat.3 y en la actualidad es uno de los medios más utilizados para transporte de banda ancha, debido a que es una infraestructura que está implantada en el 100% de las ciudades.
- **Redes LAN**: En este caso se emplea UTP Cat.5 o Cat.6 para transmisión de datos. Consiguiendo velocidades de varios centenares de Mbps. Un ejemplo de este uso lo constituyen las redes 10/100/1000BASE-T.

Para conectar el cable UTP a los distintos dispositivos de red se usan unos conectores especiales, denominados RJ-45

RJ-45			
	Nr. de pin	Identif.	Color
	1	Tx+	
	2	Tx –	
	3	Rx+	
	4	PoE –	
	5	PoE –	
	6	Rx –	
	7	PoE +	
	8	PoE +	

Velocidades de transmisión de datos:

- Categoría1 Voz (Cable de teléfono)
- Categoría 2 Datos a 4 Mbps (LocalTalk)
- Categoría 3 Datos a 10 Mbps (Ethernet)
- Categoría 4 Datos a 20 Mbps/16 Mbps Token Ring
- Categoría 5 Datos a 100 Mbps (Fast Ethernet)

EL CABLE COAXIAL

El cable coaxial se compone de un hilo conductor, llamado núcleo, y una malla externa separados por un dieléctrico o aislante

El cable coaxial es quizá el medio de transmisión más versátil, por lo que está siendo cada vez más utilizado en una gran variedad de aplicaciones. Se usa para trasmitir tanto señales analógicas como digitales. El cable coaxial tiene una respuesta en frecuencia superior a la del par trenzado, permitiendo por tanto mayores frecuencias y velocidades de transmisión. Por construcción el cable coaxial es mucho menos susceptible que el par trenzado tanto a interferencias como a diafonía.

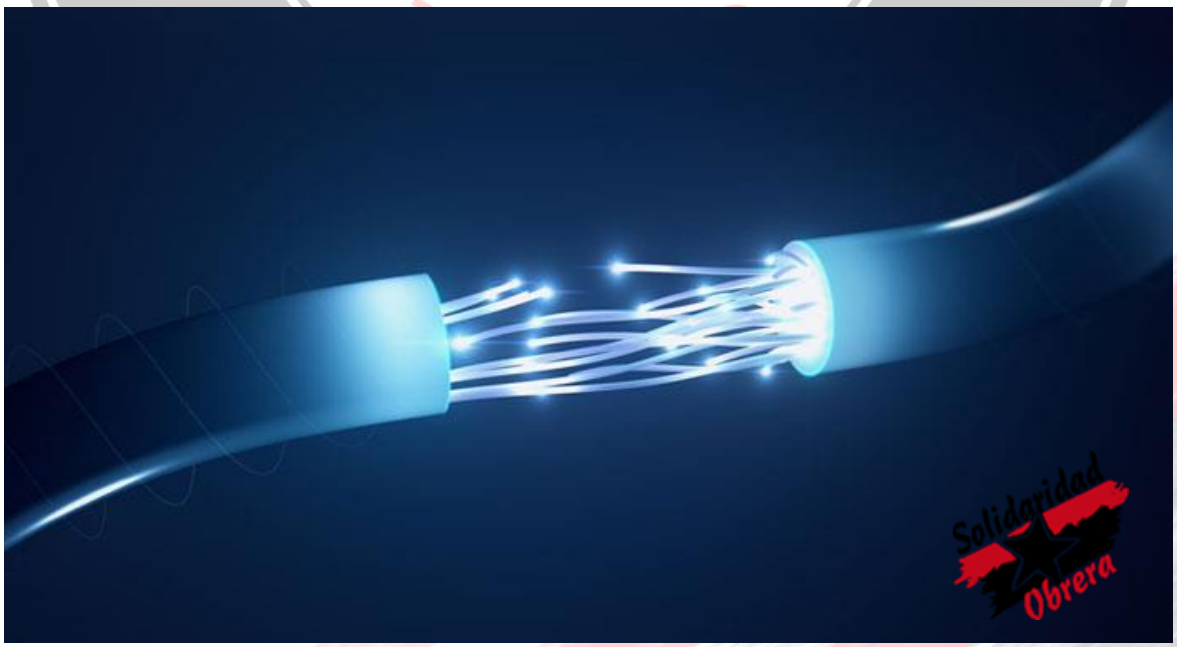
Las aplicaciones más importantes son:

- Distribución de televisión
- Telefonía a larga distancia
- Conexión con periféricos a corta distancia
- Redes de área local

Debido a la necesidad de manejar frecuencias cada vez más altas y a la digitalización de las transmisiones, en años recientes se ha sustituido paulatinamente el uso del cable coaxial por el de fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de esta última es muy superior.

LA FIBRA ÓPTICA

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED.



Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Características

La fibra óptica es una guía de ondas dieléctrica que opera a frecuencias ópticas. Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total.

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

A lo largo de toda la creación y desarrollo de la fibra óptica, algunas de sus características han ido cambiando para mejorarla. Las características más destacables de la fibra óptica en la actualidad son:

- Cobertura más resistente: La cubierta contiene un 25% más material que las cubiertas convencionales.
- Uso dual (interior y exterior): La resistencia al agua y emisiones ultravioleta, la cubierta resistente y el funcionamiento ambiental extendido de la fibra óptica contribuyen a una mayor confiabilidad durante el tiempo de vida de la fibra.
- Mayor protección en lugares húmedos: Se combate la intrusión de la humedad en el interior de la fibra con múltiples capas de protección alrededor de ésta, lo que proporciona a la fibra, una mayor vida útil y confiabilidad en lugares húmedos.
- Empaquetado de alta densidad: Con el máximo número de fibras en el menor diámetro posible se consigue una más rápida y más fácil instalación, donde el cable debe enfrentar dobleces agudos y espacios estrechos. Se ha llegado a conseguir un cable con 72 fibras de construcción súper densa cuyo diámetro es un 50% menor al de los cables convencionales.

Funcionamiento

Los principios básicos de su funcionamiento se justifican aplicando las leyes de la óptica geométrica, principalmente, la ley de la refracción (principio de reflexión interna total) y la ley de Snell.

Su funcionamiento se basa en transmitir por el núcleo de la fibra un haz de luz, tal que este no atraviese el revestimiento, sino que se refleje y se siga propagando. Esto se consigue si el índice de refracción del núcleo es mayor al índice de refracción del revestimiento, y también si el ángulo de incidencia es superior al ángulo limite.

Ventajas

- Una banda de paso muy ancha, lo que permite flujos muy elevados (del orden del Ghz).
- Pequeño tamaño, por tanto, ocupa poco espacio.
- Gran flexibilidad, el radio de curvatura puede ser inferior a 1 cm, lo que facilita la instalación enormemente.
- Gran ligereza, el peso es del orden de algunos gramos por kilómetro, lo que resulta unas nueve veces menos que el de un cable convencional.
- Inmunidad total a las perturbaciones de origen electromagnético, lo que implica una calidad de transmisión muy buena, ya que la señal es inmune a las tormentas, chisporroteo...
- Gran seguridad: la intrusión en una fibra óptica es fácilmente detectable por el debilitamiento de la energía luminosa en recepción, además, no radia nada, lo que es particularmente interesante para aplicaciones que requieren alto nivel de confidencialidad.
- No produce interferencias.
- Insensibilidad a los parásitos, lo que es una propiedad principalmente utilizada en los medios industriales fuertemente perturbados (por ejemplo, en los túneles del metro). Esta propiedad también permite la coexistencia por los mismos conductos de cables ópticos no metálicos con los cables de energía eléctrica.
- Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios. Puede proporcionar comunicaciones hasta los 70 km. antes de que sea necesario regenerar la señal, además, puede extenderse a 150 km. utilizando amplificadores láser.
- Gran resistencia mecánica (resistencia a la tracción, lo que facilita la instalación).
- Resistencia al calor, frío, corrosión.
- Facilidad para localizar los cortes gracias a un proceso basado en la telemetría, lo que permite detectar rápidamente el lugar y posterior reparación de la avería, simplificando la labor de mantenimiento.
- Con un coste menor respecto al cobre.

Desventajas

A pesar de las ventajas antes enumeradas, la fibra óptica presenta una serie de desventajas frente a otros medios de transmisión, siendo las más relevantes las siguientes:

- La alta fragilidad de las fibras.
- Necesidad de usar transmisores y receptores más caros.
- Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable.

- No puede transmitir electricidad para alimentar repetidores intermedios.
- La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica-óptica.
- La fibra óptica convencional no puede transmitir potencias elevadas.
- No existen memorias ópticas.

La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica. La energía debe proveerse por conductores separados.

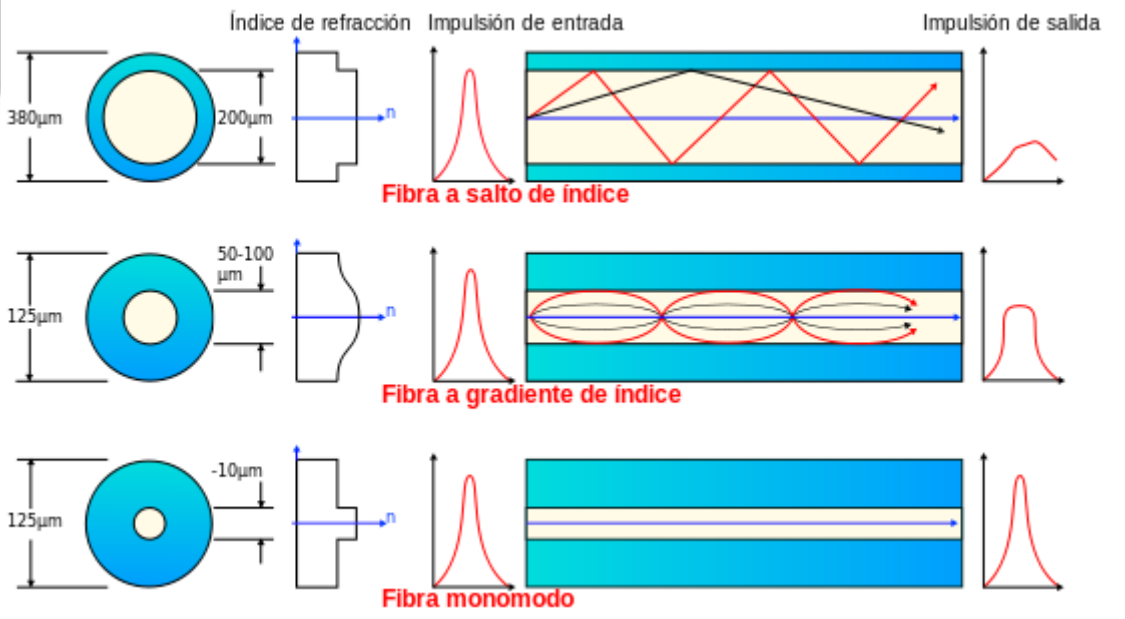
Las moléculas de hidrógeno pueden difundirse en las fibras de silicio y producir cambios en la atenuación.

El agua corroe la superficie del vidrio y resulta ser el mecanismo más importante para el envejecimiento de la fibra óptica.

Incipiente normativa internacional sobre algunos aspectos referentes a los parámetros de los componentes, calidad de la transmisión y pruebas.

Tipos

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.



- Tipos de fibra óptica.

a) Fibra multimodo

Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino.

Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 1 km, es simple de diseñar y económico.

b) Fibra monomodo

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gb/s).

- **Tipos según su diseño**

De acuerdo a su diseño, existen dos tipos de cable de fibra óptica:

a) Cable de estructura holgada

Es un cable empleado tanto para exteriores como para interiores que consta de varios tubos de fibra rodeando un miembro central de refuerzo y provisto de una cubierta protectora. Cada tubo de fibra, de dos a tres milímetros de diámetro, lleva varias fibras ópticas que descansan holgadamente en él. Los tubos pueden ser huecos o estar llenos de un gel hidrófugo que actúa como protector antihumedad impidiendo que el agua entre en la fibra. El tubo holgado aísla la fibra de las fuerzas mecánicas exteriores que se ejerzan sobre el cable.

Su núcleo se complementa con un elemento que le brinda resistencia a la tracción que bien puede ser de varilla flexible metálica o dieléctrica como elemento central o de hilaturas de Aramida o fibra de vidrio situadas periféricamente.

b) Cable de estructura ajustada

Es un cable diseñado para instalaciones en el interior de los edificios, es más flexible y con un radio de

curvatura más pequeña que el que tienen los cables de estructura holgada. Contiene varias fibras con protección secundaria que rodean un miembro central de tracción, todo ello cubierto de una protección exterior. Cada fibra tiene una protección plástica extrusionada directamente sobre ella, hasta alcanzar un diámetro de 900 µm rodeando al recubrimiento de 250 µm de la fibra óptica.

Esta protección plástica además de servir como protección adicional frente al entorno, también provee un soporte físico que serviría para reducir su coste de instalación al permitir reducir las bandejas de empalmes.

Componentes de la fibra óptica

Dentro de los componentes que se usan en la fibra óptica caben destacar los siguientes: los conectores, el tipo de emisor del haz de luz, los conversores de luz, etc.

Transmisor de energía óptica. Lleva un modulador para transformar la señal electrónica entrante a la frecuencia aceptada por la fuente luminosa, la cual convierte la señal electrónica (electrones) en una señal óptica (fotones) que se emite a través de la fibra óptica.

Detector de energía óptica. Normalmente es un fotodiodo que convierte la señal óptica recibida en electrones (es necesario también un amplificador para generar la señal)

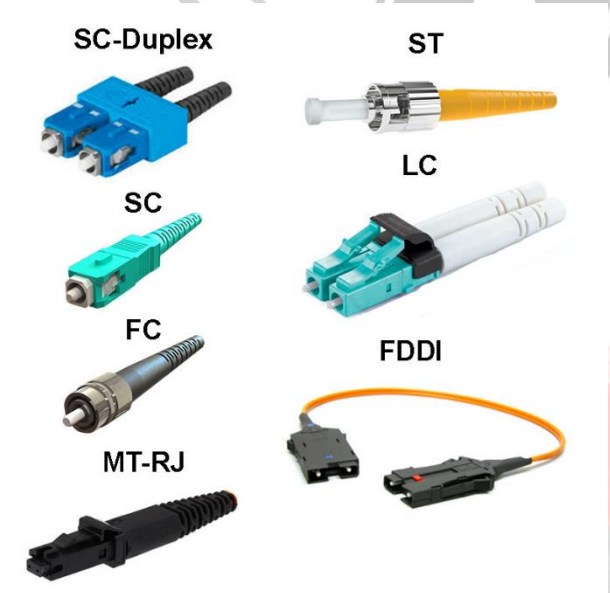
Su componente es el silicio y se conecta a la fuente luminosa y al detector de energía óptica. Dichas conexiones requieren una tecnología compleja.

Tipos de conectores

Estos elementos se encargan de conectar las líneas de fibra a un elemento, ya puede ser un transmisor o

un receptor. Los tipos de conectores disponibles son muy variados, entre los que podemos encontrar se hallan los siguientes:

- FC, que se usa en la transmisión de datos y en las telecomunicaciones.
- FDDI, se usa para redes de fibra óptica.
- LC y MT-Array que se utilizan en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC se usa en redes de edificios y en sistemas de seguridad.



Emisores del haz de luz

Estos dispositivos se encargan de convertir la señal eléctrica en señal luminosa, emitiendo el haz de luz que permite la transmisión de datos, estos emisores pueden ser de dos tipos:

- **LEDs**. Utilizan una corriente de 50 a 100 mA, su velocidad es lenta, solo se puede usar en fibras multimodo, pero su uso es fácil y su tiempo de vida es muy grande, además de ser económicos.
- **Lasers**. Este tipo de emisor usa una corriente de 5 a 40 mA, son muy rápidos, se puede usar con los dos tipos de fibra, monomodo y multimodo, pero por el contrario su uso es difícil, su tiempo de vida es largo pero menor que el de los LEDs y también son mucho más costosos.

Conversores luz-corriente eléctrica

Este tipo de dispositivos convierten las señales luminosas que proceden de la fibra óptica en señales eléctricas. Se limitan a obtener una corriente a partir de la luz modulada incidente, esta corriente es proporcional a la potencia recibida, y por tanto, a la forma de onda de la señal moduladora.

Se fundamenta en el fenómeno opuesto a la recombinación, es decir, en la generación de pares electrón-hueco a partir de los fotones. El tipo más sencillo de detector corresponde a una unión semiconductora PN.

Las condiciones que debe cumplir un fotodetector para su utilización en el campo de las comunicaciones, son las siguientes:

- La corriente inversa (en ausencia de luz) debe ser muy pequeña, para así poder detectar señales ópticas muy débiles (alta sensibilidad).
- Rapidez de respuesta (gran ancho de banda).
- El nivel de ruido generado por el propio dispositivo ha de ser mínimo.
- Hay dos tipos de detectores: los fotodiodos PIN y los de avalancha APD.
    - **Detectores PIN**: Su nombre viene de que se componen de una unión P-N y entre esa unión se intercala una nueva zona de material intrínseco (I), la cual mejora la eficacia del detector. Se utiliza principalmente en sistemas que permiten una fácil discriminación entre posibles niveles de luz y en distancias cortas.
    - **Detectores APD**: Los fotodiodos de avalancha son fotodetectores que muestran, aplicando un alto voltaje en inversa, un efecto interno de ganancia de corriente (aproximadamente 100), debido a la ionización de impacto (efecto avalancha). El mecanismo de estos detectores consiste

en lanzar un electrón a gran velocidad (con la energía suficiente), contra un átomo para que sea capaz de arrancarle otro electrón.

Estos detectores se pueden clasificar en tres tipos:

1. de silicio: presentan un bajo nivel de ruido y un rendimiento de hasta el 90% trabajando en primera ventana. Requieren alta tensión de alimentación (200-300V).
2. de germanio: aptos para trabajar con longitudes de onda comprendidas entre 1000 y 1300 nm y con un rendimiento del 70%.
3. de compuestos de los grupos III y V.

Cables de fibra óptica

Un cable de fibra óptica está compuesto por un grupo de fibras ópticas por el cual se transmiten señales luminosas. Las fibras ópticas comparten su espacio con hiladuras de aramida que le confieren la necesaria resistencia a la tracción.

Los cables de fibra óptica proporcionan una alternativa sobre los coaxiales en la industria de la electrónica y las telecomunicaciones. Así, un cable con 8 fibras ópticas tiene un tamaño bastante más pequeño que los utilizados habitualmente, puede soportar las mismas comunicaciones que 60 cables de 1623 pares de cobre o 4 cables coaxiales de 8 tubos, todo ello con una distancia entre repetidores mucho mayor.

Por otro lado, el peso del cable de fibra óptica es muchísimo menor que el de los coaxiales, ya que una bobina del cable de 8 fibras antes citado puede pesar del orden de 30 kg/km, lo que permite efectuar tendidos de 2 a 4 km de una sola vez, mientras que en el caso de los cables de cobre no son prácticas distancias superiores a 250 - 300 m.

La “fibra óptica” no se suele emplear tal y como se obtiene tras su proceso de creación (tan sólo con el revestimiento primario), sino que hay que dotarla de más elementos de refuerzo que permitan su instalación sin poner en riesgo al vidrio que la conforma. Es un proceso difícil de llevar a cabo, ya que el vidrio es quebradizo y poco dúctil. Además, la sección de la fibra es muy pequeña, por lo que la resistencia que ofrece a romperse es prácticamente nula. Es por tanto necesario protegerla mediante la estructura que denominamos cable.

Las funciones del cable

Las funciones del cable de fibra óptica son varias. Actúa como elemento de protección de la(s) fibra(s) óptica(s) que hay en su interior frente a daños y fracturas que puedan producirse tanto en el momento de su instalación como a lo largo de la vida útil de ésta. Además, proporciona suficiente consistencia mecánica para que pueda manejarse en las mismas condiciones de tracción, compresión, torsión y medioambientales que los cables

de conductores. Para ello incorporan elementos de refuerzo y aislamiento frente al exterior.

Instalación y explotación

Referente a la instalación y explotación del cable, nos encontramos frente a la cuestión esencial de qué tensión es la máxima que debe admitirse durante el tendido para que el cable no se rompa y se garantice una vida media de unos 20 años.

Técnicas de empalme: Los tipos de empalmes pueden ser:

- Empalme mecánico con el cual se pueden provocar pérdidas del orden de 0.5 dB.
- Empalme con pegamentos con el cual se pueden provocar pérdidas del orden de 0.2 dB.
- Empalme por fusión de arco eléctrico con el cual se logran pérdidas del orden de 0.02 dB.

Elementos y diseño del cable de fibra óptica

La estructura de un cable de fibra óptica dependerá en gran medida de la función que deba desempeñar esa fibra. A pesar de esto, todos los cables tienen unos elementos comunes que deben ser considerados y que comprenden: el revestimiento secundario de la fibra o fibras que contiene; los elementos estructurales y de refuerzo; la funda exterior del cable, y las protecciones contra el agua. Existen tres tipos de “revestimiento secundario”:

- **“Revestimiento ceñido”:** Consiste en un material (generalmente plástico duro como el nylon o el poliéster) que forma una corona anular maciza situada en contacto directo con el revestimiento primario. Esto genera un diámetro externo final que oscila entre 0’5 y 1 mm. Esto proporciona a la fibra una protección contra microcurvaturas, con la salvedad del momento de su montaje, que hay que vigilar que no las produzca ella misma.
- **“Revestimiento holgado hueco”:** Proporciona una cavidad sobredimensionada. Se emplea un tubo hueco extruido (construido pasando un metal candente por el plástico) de material duro, pero flexible, con un diámetro variable de 1 a 2 mm. El tubo aísla a la fibra de vibraciones y variaciones mecánicas y de temperatura externas.
- **“Revestimiento holgado con relleno”:** El revestimiento holgado anterior se puede rellenar de un compuesto resistente a la humedad, con el objetivo de impedir el paso del agua a la fibra. Además, ha de ser suave, dermatológicamente inocuo, fácil de extraer, autorregenerativo y estable para un rango de temperaturas que oscila entre los ¬ 55 y los 85 °C Es frecuente el empleo de derivados del petróleo y compuestos de silicona para este cometido.

Elementos estructurales

Los elementos estructurales del cable tienen como misión proporcionar el núcleo alrededor del cual se sustentan las fibras, ya sean trenzadas alrededor de él o dispersándose de forma paralela a él en ranuras practicadas sobre el elemento a tal efecto.

Elementos de refuerzo

Tienen por misión soportar la tracción a la que éste se ve sometido para que ninguna de sus fibras sufra una elongación superior a la permitida. También debe evitar posibles torsiones. Han de ser materiales flexibles y, ya que se emplearán kilómetros de ellos han de tener un coste asequible. Se suelen utilizar materiales como el acero, Kevlar y la fibra de vidrio.

Funda

Por último, todo cable posee una funda, generalmente de plástico cuyo objetivo es proteger el núcleo que contiene el medio de transmisión frente a fenómenos externos a éste como son la temperatura, la humedad, el fuego, los golpes externos, etc. Dependiendo de para qué sea destinada la fibra, la composición de la funda variará. Por ejemplo, si va a ser instalada en canalizaciones de planta exterior, debido al peso y a la tracción bastará con un revestimiento de polietileno extruido. Si el cable va a ser aéreo, donde sólo importa la tracción en el momento de la instalación nos preocupará más que la funda ofrezca resistencia a las heladas y al viento. Si va a ser enterrado, querremos una funda que, aunque sea más pesada, soporte golpes y aplastamientos externos. En el caso de las fibras submarinas la funda será una compleja superposición de varias capas con diversas funciones aislantes.

Pérdida en los cables de Fibra Óptica

A la pérdida de potencia a través del medio se conoce como Atenuación, es expresada en decibelios, con un valor positivo en dB, es causada por distintos motivos, como la disminución en el ancho de banda del sistema, velocidad, eficiencia. La fibra de tipo multimodal, tiene mayor pérdida debido a que la onda luminosa se dispersa originada por las impurezas. Las principales causas de pérdida en el medio son:

- Pérdidas por absorción. Ocurre cuando las impurezas en la fibra absorben la luz, y esta se convierte en energía calorífica; las pérdidas normales van de 1 a 1000 dB/Km.
- Pérdida de Rayleigh. En el momento de la manufactura de la fibra, existe un momento donde no es líquida ni sólida y la tensión aplicada durante el enfriamiento puede provocar microscópicas irregularidades que se quedan permanentemente; cuando los rayos de luz pasan por la fibra, estos se difractan haciendo que la luz vaya en diferentes direcciones.

- Dispersión cromática. Esta dispersión sólo se observa en las fibras tipo unimodal, ocurre cuando los rayos de luz emitidos por la fuente y se propagan sobre el medio, no llegan al extremo opuesto en el mismo tiempo; esto se puede solucionar cambiando el emisor fuente.
- Pérdidas por radiación. Estas pérdidas se presentan cuando la fibra sufre de dobleces, esto puede ocurrir en la instalación y variación en la trayectoria, cuando se presenta discontinuidad en el medio.
- Dispersión modal. Es la diferencia en los tiempos de propagación de los rayos de luz.
- Pérdidas por acoplamiento. Las pérdidas por acoplamiento se dan cuando existen uniones de fibra, se deben a problemas de alineamiento.

7.1.2.2. MEDIOS INALÁMBRICOS:

RADIOFRECUENCIA:

- Se basa en la transmisión de señales electromagnéticas a través del aire en un rango de frecuencias específicas.
- Es utilizada en diversos sistemas como la telefonía móvil, Wi-Fi, Bluetooth y comunicaciones de radio bidireccional.
- La radiofrecuencia se divide en bandas de frecuencia, incluyendo:
  - **Banda VHF (Very High Frequency):** Utilizada en radiodifusión, radioaficionados y comunicaciones marítimas.
  - **Banda UHF (Ultra High Frequency):** Empleada en televisión digital, sistemas de comunicación móvil y redes Wi-Fi.
- La propagación de señales de radiofrecuencia puede verse afectada por fenómenos como la atenuación, el reflejo y la difracción.

¿Cuál es mejor VHF o UHF?

Elegir entre una frecuencia VHF o la frecuencia UHF depende de lo que los usará. VHF es principalmente para uso en exteriores donde está libre de obstrucciones. Las frecuencias de **Viajar VHF aún más si no son interrumpidos por las barreras.**. La única vez que querrá usar VHF es si está afuera en un espacio abierto como un campo. VHF tiene frecuencias más pequeñas que significa que la interferencia con otras radios es común.

UHF, por otro lado, es una mejor señal mejor para la comunicación de larga distancia. UHF es mejor cuando se usa radios para uso en interiores como edificios o alrededor de ciudades. Una ventaja para usar **UHF es que es menos probable que sea interferido por otras radios de dos vías**. La razón por la que UHF es mejor para el uso interno se opone

a VHF, la señal UHF hace un mejor trabajo para alcanzar la madera, el acero y el concreto, por lo tanto, puede llegar a la construcción.

¿Qué significa UHF y VHF?

UHF significa «**Frecuencia ultra alta** «mientras VHF significa» **Muy alta frecuencia**» UHF puede variar desde bandas bajas (378-512 MHz) a banda alta (764-870 MHz), mientras que VHF varía de banda baja (49-108 MHz) a banda alta (169-216 MHz). MHZ significa Megahertz y mide la velocidad de los dispositivos electrónicos.

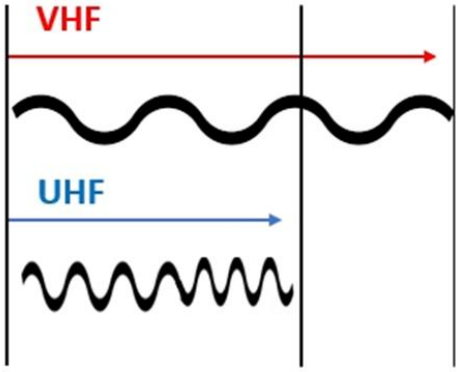


Tabla rango de frecuencia UHF VS VHF

0.003 MHz- 0.03 MHz	Muy baja frecuencia (VLF)
.03 MHz - 0.3 MHz	Baja frecuencia (LF)
0.3 MHz - 3 MHz	Frecuencia media (MF)
3 MHz - 30 MHz	Alta frecuencia (HF)
30 MHz - 300 MHz	Muy alta frecuencia (VHF)
300 MHz - 3.000 MHz	Ultra-High Frecuencia (UHF)
3.000 MHz - 30,000 MHz	Super alta frecuencia (SHF)
30,000 MHz - 300,000 MHz	Frecuencia extra alta (EHF)

¿Quién usa UHF y VHF?

La UHF suele ser utilizada por los funcionarios de seguridad pública como Fuego, Policía y EMS con canales de TV de 77-80. UHF se utiliza para fines comunes como teléfonos, televisores. Los casinos, los funcionarios de seguridad, los almacenes, la construcción, la fabricación y la atención médica también utilizan radios UHF para comunicarse con otros en todo el edificio y a través de los departamentos. **Un funcionario de seguridad pública utiliza frecuencias de MHz entre 849 y 869 y una banda de radio de jamón de 13 cm tiene una MHz de 2300 a 1310.**

VHF se usa comúnmente para la comunicación en Barcos y marine personal. Es un accesorio muy importante que tener a bordo porque puede contactar a los navegantes cercanos si surgen ciertas emergencias. El canal 16 se usa cuando se necesita para hacer una llamada de emergencia y se debe seguir cierto protocolo. Agencias como TSA y CAL FIRE (Departamento de Protección Forestal y Fuego de California) Use VHF para sus comunicaciones de radio de dos vías.

¿Cómo puedo mejorar la fuerza de mi señal en mi radio de dos vías VHF o UHF?

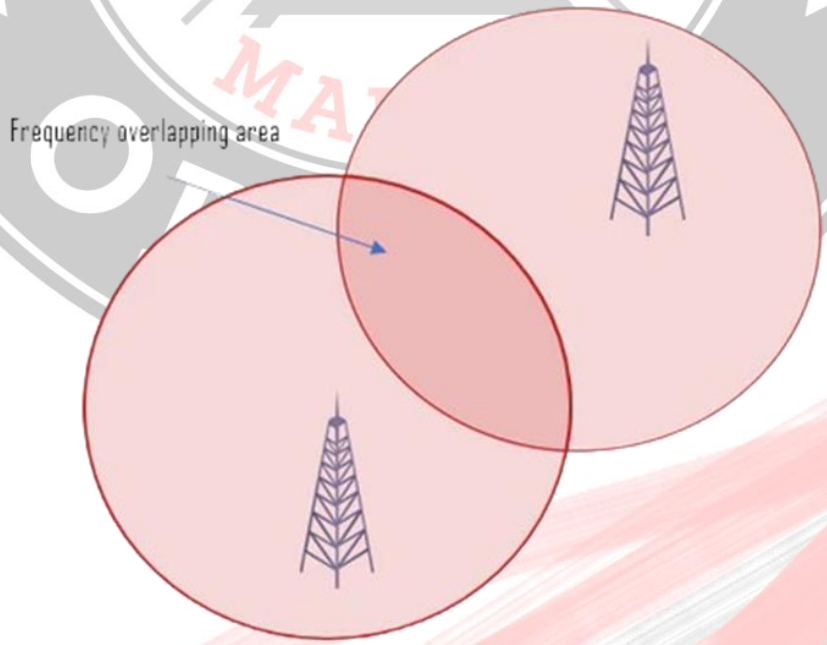
Una forma de mejorar el rango en una radio de dos vías es mejorando la antena. La longitud de su antena determina la longitud de las ondas de radio. Las longitudes de onda de UHF (frecuencia ultra-alta) son cortas para que las antenas para radios de dos vías UHF son **típicamente pequeño y molesto en tamaño.**. VHF requiere un **antena ligeramente más grande** Para mejorar su rango y hasta qué punto viajará. Antenas VHF Puede recibir canales 2 a 13, mientras que las antenas UHF pueden recibir canales 14 a 83.

Dado que VHF a menudo se interfiere con otras frecuencias, las mejores maneras de asegurarse de que no lo interrumpas es localizar de dónde viene la interferencia. En un barco, hay muchos lugares de los que pueden venir el ruido. Escuche el receptor y tenga en cuenta cualquier cambio en el nivel de ruido.

Otra forma de ayudar con las interrupciones es la unión. Esto asegura que el aviso desaparece al suelo en lugar de irradiado. Todos los motores y tales deben ser construidos en el suelo.

Un problema que puede ocurrir con señales es **superposición de frecuencia**. Esto significa que si dos radios están utilizando la misma frecuencia, las ondas de radio se interrumpen entre sí, y las transmisiones se superponen. Lo más probable es que esto suceda cuando estén en el rango del otro o estén en el mismo área de cobertura.

No tendrá ningún problema con un solo transmisor, pero si desea cubrir un área grande con múltiples transmisores, es cuando se vuelve difícil porque no quiere que se interrumpan entre sí.



¿Cuál es la diferencia entre UHF y VHF?

La principal diferencia entre UHF y VHF es rango. **Las radios de dos vías de UHF tienen un rango que es más ancho que VHF**. Esto significa que las frecuencias UHF tienen olas más pequeñas que producen un rango mayor. Es más probable que pasen barreras como rocas y árboles más fáciles.

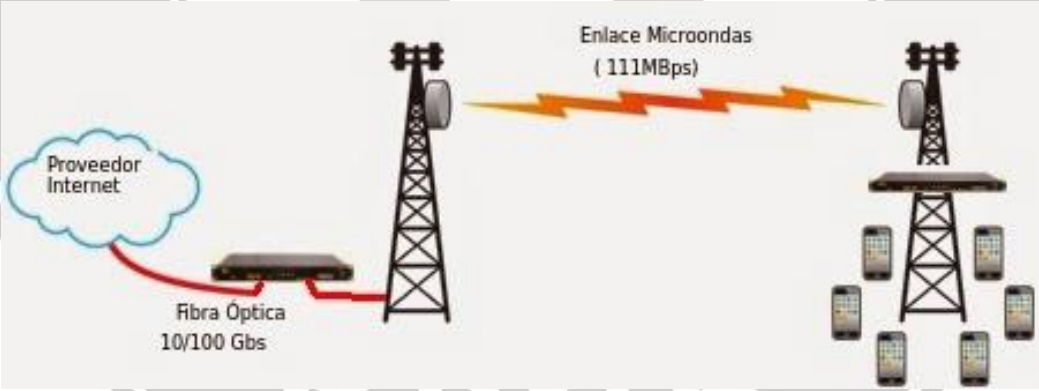
La gama VHF se reduce debido a la degradación de la señal con barreras como árboles o colinas. Juntos ambos alcanzan una buena distancia.

Otra diferencia entre UHF y VHF es su vida útil de la batería. UHF usa mucha batería debido a la frecuencia más alta. La última diferencia entre las dos radios es que UHF viene a un costo más alto que VHF.

MICROONDAS:

Comunicaciones por Microondas: Tecnología, Aplicaciones y Desafíos

Las **comunicaciones por microondas** utilizan ondas electromagnéticas de alta frecuencia para transmitir datos de un punto a otro sin necesidad de cables. Este tipo de comunicación es ampliamente utilizado en **telecomunicaciones, transmisión de datos y enlaces de redes troncales**, debido a su capacidad para transmitir grandes volúmenes de información de manera rápida y eficiente.



Características de las Comunicaciones por Microondas

Las microondas presentan propiedades que las hacen ideales para la transmisión de señales a largas distancias:

- **Alta frecuencia:** Se encuentran en el rango de **300 MHz a 300 GHz**, lo que permite una alta capacidad de transmisión de datos.
- **Direccionalidad:** Requieren antenas parabólicas o de panel direccional para enfocarse en un punto específico, minimizando la dispersión de la señal.
- **Baja latencia:** La propagación de las microondas es casi instantánea, lo que las hace útiles en aplicaciones donde la velocidad es crítica.

- **Sin necesidad de cables:** Reducen los costos de infraestructura en comparación con el despliegue de fibra óptica o cables de cobre.
- **Sensibles a condiciones atmosféricas:** Factores como la lluvia, la humedad y la interferencia de obstáculos pueden afectar su calidad de transmisión.

Aplicaciones de las Comunicaciones por Microondas

Las microondas tienen un papel fundamental en diversos sectores de las telecomunicaciones. Algunas de sus aplicaciones más relevantes incluyen:

Enlaces de Comunicación Satelital

Las microondas son la base de las comunicaciones satelitales, ya que permiten la transmisión de señales entre **estaciones terrestres y satélites en órbita**. Estas señales pueden incluir:

- Transmisión de datos de internet y telefonía.
- Servicios de televisión satelital.
- Comunicaciones en zonas rurales o de difícil acceso.

Los satélites geoestacionarios, que orbitan a unos **36,000 km de la Tierra**, utilizan microondas en bandas como **C, Ku y Ka** para garantizar la conectividad global.

Redes de Telecomunicaciones Terrestres

Las redes de telecomunicaciones usan enlaces de microondas como una alternativa a la fibra óptica o en zonas donde el cableado es inviable. Se utilizan en:

- **Torres de telecomunicaciones:** Transmiten señales de telefonía móvil y datos entre estaciones base.
- **Enlaces troncales de microondas:** Conectan centros de datos y estaciones de telecomunicaciones en áreas remotas.
- **Backhaul de redes móviles:** Soportan la infraestructura de redes 4G y 5G, transmitiendo grandes volúmenes de datos entre antenas y centros de control.

Comunicación en Áreas Rurales y de Difícil Acceso

En regiones donde el despliegue de fibra óptica no es viable, las microondas ofrecen una solución eficiente para conectar comunidades remotas. Ejemplos de su uso incluyen:

- Extensión de cobertura móvil en zonas rurales.
- Enlaces de radio y televisión en regiones alejadas.
- Conectividad de internet en islas o regiones montañosas.

Redes de Emergencia y Seguridad

Las comunicaciones por microondas también son esenciales en situaciones de emergencia y seguridad:

- **Redes de comunicaciones gubernamentales y militares**, asegurando la transmisión de información en tiempo real.
- **Infraestructuras de comunicación para desastres naturales**, como terremotos o huracanes, donde las redes cableadas pueden quedar inoperativas.

Ventajas y Desafíos de las Comunicaciones por Microondas

Ventajas

- **Alta capacidad de transmisión de datos**, ideal para redes de alta velocidad.
- **Menores costos de instalación y mantenimiento** en comparación con redes cableadas.
- **Flexibilidad y rapidez en la implementación**, especialmente en regiones donde el despliegue de fibra óptica es complicado.
- **Posibilidad de conectar zonas remotas**, eliminando la dependencia de infraestructuras físicas.

Desafíos y Limitaciones

- **Interferencia atmosférica:** La lluvia, la humedad y la nieve pueden afectar la señal, especialmente en bandas de alta frecuencia.
- **Líneas de visión directas necesarias:** Los enlaces de microondas requieren que no haya obstáculos entre el transmisor y el receptor.
- **Capacidad limitada en comparación con la fibra óptica**, especialmente en aplicaciones que demandan un ancho de banda muy elevado.
- **Regulaciones y licencias**: El uso de bandas de frecuencia para comunicaciones por microondas está sujeto a regulaciones gubernamentales, lo que puede limitar su disponibilidad en ciertas áreas.

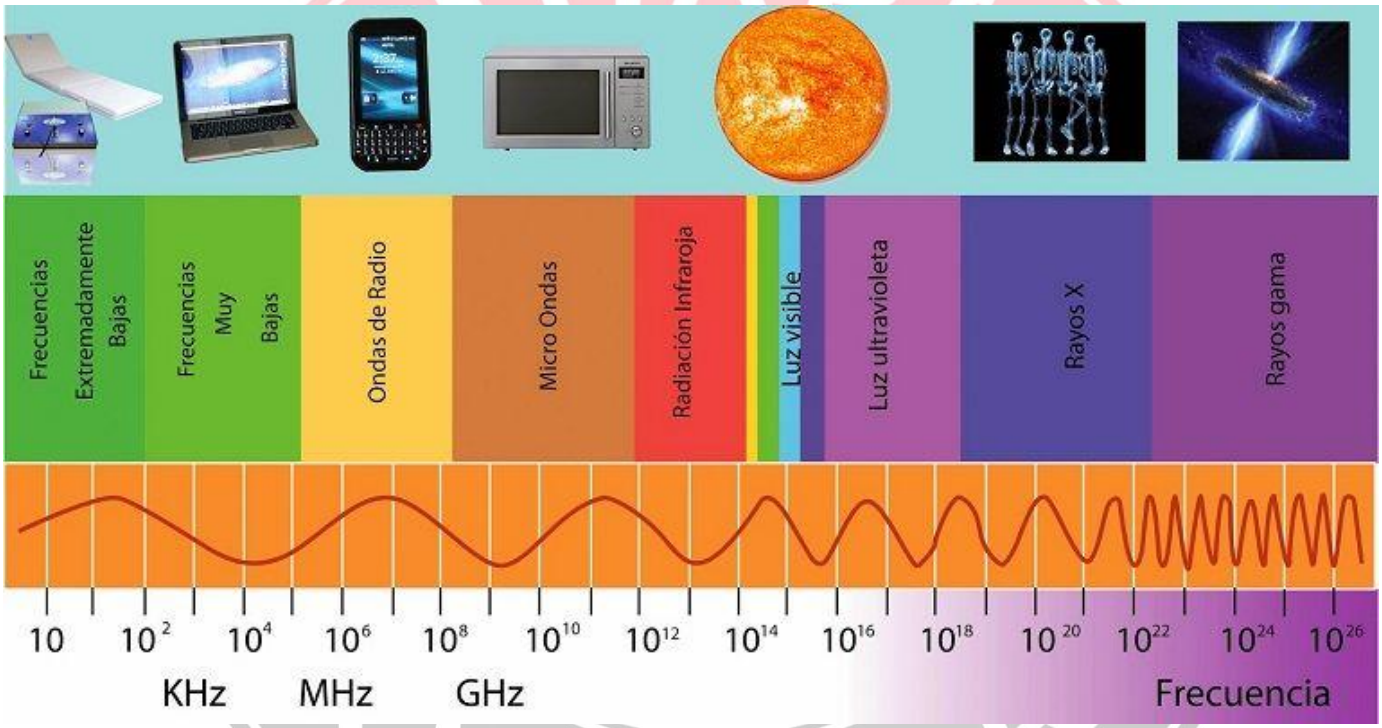
Conclusión

Las **comunicaciones por microondas** son una tecnología fundamental en las telecomunicaciones modernas, permitiendo la transmisión de datos a larga distancia de manera eficiente. A pesar de sus limitaciones, como la interferencia atmosférica y la necesidad de una línea de visión directa, siguen siendo una solución clave en telecomunicaciones satelitales, redes móviles y conectividad en regiones remotas. Con el avance de tecnologías como **las redes 5G y la comunicación satelital de órbita baja (LEO)**, las microondas seguirán desempeñando un papel crucial en la conectividad global.

INFRARROJOS:

Comunicaciones por Infrarrojos: Tecnología, Aplicaciones y Limitaciones

Las **comunicaciones por infrarrojos** utilizan ondas electromagnéticas en la banda del **espectro infrarrojo**, que se encuentra justo por debajo de la luz visible, con longitudes de onda comprendidas entre **700 nm y 1 mm**. Esta tecnología permite la transmisión de datos mediante señales ópticas, aunque su uso está restringido a distancias cortas debido a que las señales infrarrojas **no pueden atravesar obstáculos sólidos y requieren una línea de visión directa** entre el emisor y el receptor.



Características de las Comunicaciones por Infrarrojos

Las ondas infrarrojas poseen propiedades que las hacen útiles en múltiples aplicaciones de transmisión de datos:

- **Alcance limitado:** Se utilizan principalmente en comunicaciones de corto alcance, generalmente **menores a 10 metros**.
- **Seguridad mejorada:** Dado que las señales infrarrojas **no atraviesan paredes ni objetos sólidos**, reducen el riesgo de interceptación, lo que las hace ideales para **transmisiones seguras** en entornos cerrados.

- **Bajo consumo energético:** Su transmisión requiere **poca energía**, lo que las hace adecuadas para dispositivos portátiles y sistemas de bajo consumo.
- **Inmunidad a interferencias electromagnéticas:** No se ven afectadas por las señales de radiofrecuencia ni por los campos electromagnéticos generados por otros dispositivos electrónicos.
- **Necesidad de línea de visión:** La señal debe viajar en un camino sin obstrucciones entre el transmisor y el receptor, lo que limita su flexibilidad en entornos con obstáculos.

Aplicaciones de las Comunicaciones por Infrarrojos

Las comunicaciones infrarrojas se utilizan en diversos dispositivos y sistemas donde se requiere una conexión inalámbrica segura y eficiente.

Mandos a Distancia

El uso más común de las comunicaciones por infrarrojos se encuentra en **mandos a distancia** de:

- Televisores
- Equipos de sonido
- Aire acondicionado
- Proyectores
- Otros dispositivos electrónicos

Estos controles remotos emplean pulsos de luz infrarroja modulada para enviar señales codificadas a un receptor, permitiendo el control de funciones como encendido, volumen o cambio de canal.

Comunicaciones entre Dispositivos Electrónicos

Antes de la popularización de tecnologías como el Bluetooth o el Wi-Fi, los **infrarrojos** fueron ampliamente utilizados para la transferencia de datos entre dispositivos. Ejemplos incluyen:

- **Teléfonos móviles antiguos** con tecnología IrDA (Infrared Data Association), que permitían intercambiar archivos sin cables.
- **Computadoras portátiles y PDAs**, que usaban infrarrojos para sincronización de datos.
- **Impresoras y periféricos**, que en algunos modelos admitían conexiones por infrarrojos sin necesidad de cables.

Sistemas de Seguridad y Sensores de Movimiento

Las comunicaciones infrarrojas juegan un papel clave en los sistemas de seguridad debido a su capacidad de detectar objetos y movimientos. Se utilizan en:

- **Sensores de movimiento en alarmas de seguridad**, donde un emisor infrarrojo detecta cambios en la radiación térmica del entorno.
- **Barreras infrarrojas en accesos restringidos**, como las usadas en aeropuertos o bancos para detectar intrusos.
- **Cámaras y sistemas de visión nocturna**, que aprovechan la capacidad del infrarrojo para detectar calor y generar imágenes en condiciones de baja iluminación.

Comunicación en Dispositivos Biomédicos

Algunos dispositivos médicos y de monitoreo utilizan **infrarrojos** para la transmisión de datos, ya que esta tecnología permite una comunicación rápida sin interferencias externas. Ejemplos incluyen:

- **Oxímetros de pulso**, que miden la saturación de oxígeno en la sangre a través de luz infrarroja.
- **Monitores de frecuencia cardíaca** que utilizan sensores infrarrojos para medir el flujo sanguíneo en la piel.

Ventajas y Desafíos de las Comunicaciones por Infrarrojos

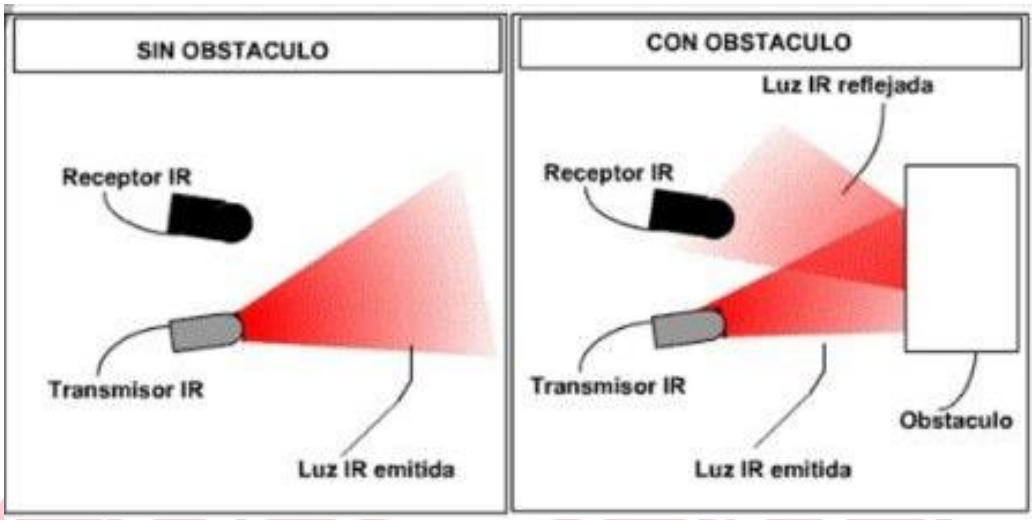
Ventajas

- **Mayor seguridad:** Como la señal no atraviesa paredes, es difícil de interceptar, reduciendo los riesgos de ataques de terceros.
- **Bajo consumo energético:** Se requiere poca potencia para la transmisión, lo que permite su uso en dispositivos portátiles y sistemas autónomos.
- **Sin interferencias electromagnéticas:** No se ve afectada por otras señales inalámbricas, como las de Wi-Fi o Bluetooth, lo que la hace ideal para entornos con múltiples dispositivos electrónicos.

Desafíos y Limitaciones

- **Alcance corto:** La distancia de transmisión es limitada, generalmente **menor a 10 metros**.

- **Requiere línea de visión directa:** Cualquier obstáculo entre el emisor y el receptor **bloquea completamente la comunicación**.



- **Menor velocidad de transmisión en comparación con otras tecnologías inalámbricas:** Aunque los infrarrojos fueron utilizados en la transferencia de datos en el pasado, **han sido reemplazados por Bluetooth y Wi-Fi**, que ofrecen mayores velocidades y mayor flexibilidad.
- **Sensibilidad a la luz ambiental:** La luz solar intensa o fuentes de iluminación artificial pueden **interferir con la señal infrarroja**, afectando su fiabilidad en ciertos entornos.

Conclusión

Las **comunicaciones por infrarrojos** siguen siendo una tecnología relevante en aplicaciones donde se requiere una transmisión segura, de corto alcance y de bajo consumo energético. Aunque su uso ha disminuido en favor de tecnologías más avanzadas como Wi-Fi y Bluetooth, sigue siendo esencial en **mandos a distancia, sistemas de seguridad, sensores de movimiento y dispositivos biomédicos**. A pesar de sus limitaciones, como la necesidad de una línea de visión directa y su corto alcance, **los infrarrojos siguen siendo una opción confiable y eficiente en numerosos sectores tecnológicos**.

SATÉLITE:

Comunicaciones por Satélite: Tecnología, Aplicaciones y Desafíos

Las **comunicaciones por satélite** permiten la transmisión de datos a nivel global, proporcionando conectividad en áreas donde la infraestructura terrestre de telecomunicaciones es limitada o inexistente. Esta tecnología es clave en **televisión,**

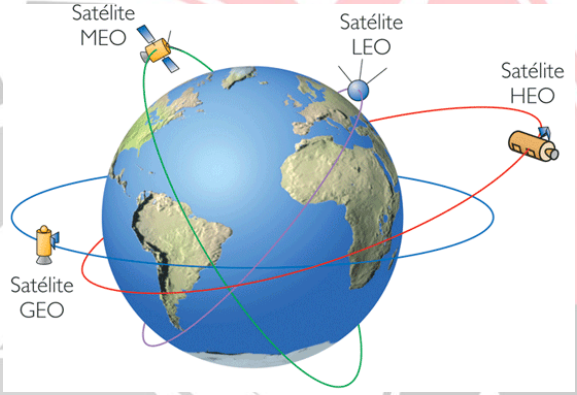
telefonía, internet, navegación y comunicaciones de emergencia, desempeñando un papel esencial en la interconexión global.

Principios de la Comunicación por Satélite

Un **sistema de comunicación satelital** consiste en un satélite en órbita que recibe, amplifica y retransmite señales hacia estaciones terrestres o terminales de usuario. La señal viaja desde una **estación emisora** hasta el satélite, que la redirige hacia una **estación receptora** en otro punto del planeta.

Los satélites de comunicación operan en **diferentes bandas de frecuencia** dentro del espectro electromagnético, como las bandas **C, Ku, Ka y L**, cada una con características específicas en cuanto a capacidad y cobertura.

Tipos de Satélites según su Órbita



Los satélites de comunicación pueden clasificarse según la altitud de su órbita, lo que influye en su cobertura, latencia y aplicaciones.

Satélites Geoestacionarios (GEO)

- **Altitud:** ~35,786 km sobre el ecuador.
- **Características:**
  - Permanecen fijos en una posición relativa respecto a la Tierra.
  - Cubren grandes áreas, proporcionando conectividad continua.
  - Tienen **alta latencia** (~500 ms) debido a la gran distancia.
- **Aplicaciones:**
  - **Televisión satelital:** Empresas como DirecTV y Dish Network utilizan satélites GEO para la transmisión de señales de TV.
  - **Telefonía satelital:** Permiten llamadas en zonas remotas sin infraestructura terrestre.
  - **Comunicaciones gubernamentales y militares:** Se utilizan en redes de defensa y seguridad nacional.
  - **Meteorología:** Satélites como el GOES (Geostationary Operational Environmental Satellite) monitorizan el clima.

Satélites de Órbita Media (MEO)

- **Altitud:** Entre 2,000 km y 20,000 km.
- **Características:**
  - Tienen menor latencia (~100 ms) en comparación con los GEO.
  - Requieren menos satélites para cubrir grandes áreas en comparación con los LEO.
- **Aplicaciones:**
  - **Sistemas de posicionamiento global (GPS, GLONASS, Galileo, BeiDou).**
  - **Navegación y rastreo marítimo y aéreo.**

Satélites de Órbita Baja (LEO)

- **Altitud:** Entre 300 km y 2,000 km.
- **Características:**
  - **Baja latencia (~20-40 ms)**, comparable con redes terrestres.
  - Mayor velocidad y capacidad para la transmisión de datos.
  - Requieren **constelaciones de múltiples satélites** para cobertura continua, ya que orbitan rápidamente la Tierra.
- **Aplicaciones:**
  - **Internet satelital:** Empresas como SpaceX (Starlink), OneWeb y Amazon (Project Kuiper) están desplegando redes LEO para ofrecer internet global de alta velocidad.
  - **Monitoreo de la Tierra y observación remota:** Se utilizan en vigilancia ambiental y gestión de desastres.
  - **Comunicaciones militares y gubernamentales.**

Aplicaciones de la Tecnología Satelital

Comunicaciones de Emergencia y Desastres Naturales

En eventos como **terremotos, huracanes o incendios forestales**, las redes terrestres pueden colapsar. Los sistemas satelitales garantizan la comunicación en estas situaciones críticas:

- Proveen acceso a telefonía y datos en zonas devastadas.
- Son utilizados por organismos de rescate y fuerzas de seguridad.

- Permiten la coordinación de ayuda humanitaria en tiempo real.

Exploración Espacial y Ciencia

Las misiones espaciales dependen de los satélites para la transmisión de datos científicos:

- **Exploración planetaria:** Satélites como el Mars Reconnaissance Orbiter envían imágenes y datos desde Marte.
- **Observación astronómica:** Telescopios espaciales como el Hubble y el James Webb transmiten información sobre el universo.
- **Monitoreo ambiental:** Satélites como el Copernicus Sentinel rastrean el cambio climático y la deforestación.

Redes de Comunicación Global

Las redes de satélites han revolucionado la conectividad global:

- **Internet satelital:** Starlink y OneWeb ofrecen banda ancha en zonas rurales y en países en desarrollo.
- **Telefonía satelital:** Empresas como Iridium y Thuraya permiten llamadas desde cualquier parte del mundo.
- **Transmisión de datos en aviación y navegación marítima.**

Ventajas y Desafíos de la Comunicación Satelital

Ventajas

- **Cobertura Global:** Llega a zonas rurales, montañosas, desiertos y océanos.
- **Resiliencia ante desastres:** No depende de infraestructuras terrestres vulnerables a cortes.
- **Conectividad en movilidad:** Ideal para aviones, barcos y vehículos en zonas remotas.
- **Alta capacidad de transmisión:** Puede soportar tráfico de voz, video y datos de alta velocidad.

Desafíos y Limitaciones

- **Latencia en satélites GEO:** La alta altitud provoca retardos en la comunicación, afectando aplicaciones en tiempo real como videollamadas y juegos en línea.
- **Costos elevados:** El lanzamiento y mantenimiento de satélites es costoso. Empresas como SpaceX están reduciendo costos con cohetes reutilizables.
- **Interferencia electromagnética:** La señal satelital puede verse afectada por tormentas solares o interferencia terrestre.

- **Espacio orbital congestionado:** Con el aumento de satélites en órbita, la gestión del tráfico espacial y la mitigación de basura espacial se han convertido en desafíos críticos.

Futuro de las Comunicaciones por Satélite

Las comunicaciones satelitales están evolucionando rápidamente con nuevas tecnologías:

- **Redes de satélites LEO en crecimiento:** Starlink ya tiene más de **5,000 satélites en órbita** y sigue expandiéndose.
- **Integración con 5G:** Los satélites se están combinando con redes terrestres para mejorar la conectividad global.
- **Desarrollo de nanosatélites:** Empresas están explorando el uso de pequeños satélites con menor costo y mayor eficiencia.
- **Lanzamiento de estaciones espaciales privadas:** La NASA y empresas como Blue Origin y Axiom Space planean desarrollar nuevas infraestructuras en órbita para futuras misiones y comunicaciones avanzadas.

Conclusión

Las **comunicaciones por satélite** son fundamentales para la conectividad global, permitiendo la transmisión de datos en regiones inaccesibles para redes terrestres. Desde **televisión e internet hasta navegación GPS y comunicaciones de emergencia**, su impacto es significativo. Aunque enfrenta desafíos como **altos costos, latencia en los GEO y congestión orbital**, la innovación en **satélites LEO y tecnologías emergentes** promete mejorar la eficiencia y accesibilidad de estas redes en los próximos años.

7.2. NORMATIVA Y REGULACIÓN EN TELECOMUNICACIONES

El sector de las telecomunicaciones es uno de los más regulados a nivel mundial, ya que juega un papel esencial en la **conectividad, el desarrollo económico y la seguridad de las comunicaciones**. Las normativas y regulaciones en telecomunicaciones buscan garantizar:

- **Uso eficiente del espectro radioeléctrico.**
- **Seguridad y protección de los datos de los usuarios.**
- **Calidad y accesibilidad de los servicios de telecomunicaciones.**
- **Promoción de la competencia y prevención de monopolios.**
- **Neutralidad de la red para asegurar un acceso equitativo a la información.**

La regulación de las telecomunicaciones involucra tanto **organismos internacionales** como **entidades gubernamentales nacionales**, que establecen políticas y supervisan el cumplimiento de normativas dentro de sus jurisdicciones.

8. INFRAESTRUCTURA DE REDES

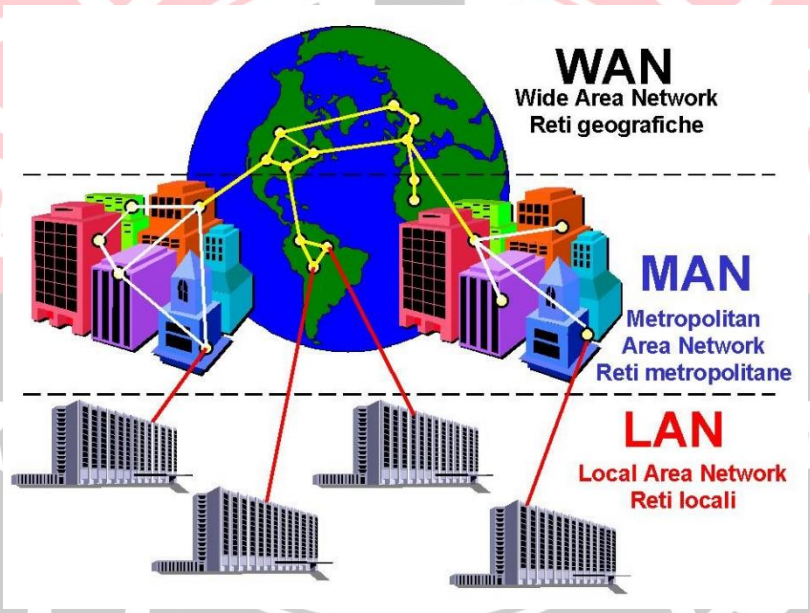
CONCEPTOS BÁSICOS DE REDES

Las redes de información se pueden clasificar según su extensión y su topología. Una red puede empezar siendo pequeña para crecer junto con la organización o institución. A continuación, se presenta los distintos tipos de redes disponibles:

8.1. TIPOS DE REDES

POR EXTENSIÓN

De acuerdo con la distribución geográfica:



RED DE ÁREA LOCALES (LAN)

Una LAN es un segmento de red que tiene conectadas estaciones de trabajo y servidores o un conjunto de segmentos de red interconectados, generalmente dentro de la misma zona. Por ejemplo, un edificio.

RED DE ÁREA METROPOLITANAS (MAN)

Una red MAN es una red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

RED DE ÁREA EXTENSA (WAN Y REDES GLOBALES)

Las WAN y redes globales se extienden sobrepasando las fronteras de las ciudades, pueblos o naciones. Los enlaces se realizan con instalaciones de telecomunicaciones públicas y privadas, además por microondas y satélites.

VER 6.4.1. REDES DE DATOS

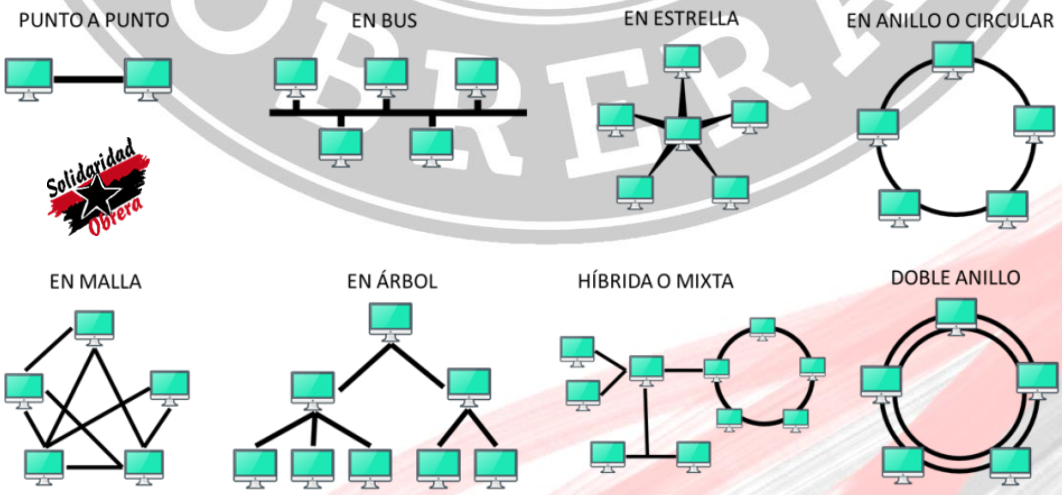
8.2. TOPOLOGÍA DE REDES

¿Qué es una Topología de Red?

La topología de red se define como una familia de comunicación usada por los computadores que conforman una red para intercambiar datos. En otras palabras, la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos refiramos.

Tipos de topologías

1. **Punto a punto.**
2. **En bus.**
3. **En estrella.**
4. **En anillo o circular.**
5. **En malla.**
6. **En árbol**
7. **Topología híbrida**



1. Punto a punto

La topología más simple es un enlace permanente entre dos puntos finales (también conocida como point-to-point, o abreviadamente, PtP). La topología punto a punto conmutado es el modelo básico de la telefonía convencional. El valor de una red permanente de punto a punto la comunicación sin obstáculos entre los dos puntos finales. El valor de una conexión punto-a-punto a demanda es proporcional al número de pares posibles de abonados y se ha expresado como la ley de Metcalfe.

2. Topología en Bus

Topología de 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 computadoras 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. En una topología de bus, cada computadora está conectada a un segmento común de cable de red. El segmento de red se coloca como un bus lineal, es decir un cable largo que va de un extremo a otro de la red, y al cual se conecta cada nodo de ésta. El cable puede ir por el piso, las paredes, el techo o por varios lugares, siempre y cuando sea un segmento continuo.

3. Topología en estrella

Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en la topología estrella este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto. El tipo de concentrador hub se utiliza en esta topología, aunque ya es muy obsoleto; se suele usar comúnmente un switch.

La desventaja radica en la carga que recae sobre el nodo central. La cantidad de tráfico que deberá soportar es grande y aumentará conforme vayamos agregando más nodos periféricos, lo que la hace poco recomendable para redes de gran tamaño. Además, un fallo en el nodo central puede dejar inoperante a toda la red. Esto último conlleva también una mayor vulnerabilidad de la red, en su conjunto, ante ataques.

4. Topología en Anillo

Si el nodo central es pasivo, el nodo origen debe ser capaz de tolerar un eco de su transmisión. Una red, en estrella activa, tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Una red en anillo es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación. En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones. En un anillo doble (Token Ring), dos anillos permiten que los datos se envíen en ambas direcciones (Token passing). Esta configuración crea redundancia (tolerancia a fallos). Evita las colisiones.

5. Topología en árbol

(También conocida como topología jerárquica) puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales (por ejemplo hojas) que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

Como en las redes en estrella convencionales, los nodos individuales pueden quedar aislados de la red por un fallo puntual en la ruta de conexión del nodo. Si falla un enlace que conecta con un nodo hoja, ese nodo hoja queda aislado; si falla un enlace con un nodo que no sea hoja, la sección entera queda aislada del resto.

Para aliviar la cantidad de tráfico de red que se necesita para retransmitir en su totalidad, a todos los nodos, se desarrollaron nodos centrales más avanzados que permiten mantener un listado de las identidades de los diferentes sistemas conectados a la red. Éstos switches de red “aprenderían” cómo es la estructura de la red transmitiendo paquetes de datos a todos los nodos y luego observando de dónde vienen los paquetes de respuesta también es utilizada como un enchufe u artefacto.

6. Topología en Malla

La topología de red mallada es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores. Las redes de malla son auto ruteables. La red puede funcionar, incluso cuando un nodo desaparece o la conexión

falla, ya que el resto de los nodos evitan el paso por ese punto. En consecuencia, la red malla, se transforma en una red muy confiable.

7. Topología Hibrida o Mixta

Topología híbrida, las redes pueden utilizar diversas tipologías para conectarse, como por ejemplo en estrella. La topología híbrida 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. Ejemplos de topologías híbridas serían: 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 híbridas 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.

8.3. COMPONENTES DE UNA RED

Una red de computadoras consta de "hardware" y "software". En el "hardware" se incluyen las tarjetas de interfaz de red y los cables que las unen y en el "software" se encuentran los sistemas operativos del servidor, los protocolos de comunicación y los controladores de tarjetas de interfaz de la red.

Para seleccionar el sistema operativo hay que saber la manera en que la red está organizada. Las redes se pueden organizar en: cliente-servidor, servidor de archivos y computación par a par. El "software" puede incorporar varias funciones de seguridad, proporciona los protocolos de comunicación y el manejo de la tarjeta de interfaz de la red. Entre ellos podemos mencionar Microsoft Windows para trabajo en grupos, Microsoft Windows NT, Novell NetWare y Artisoft LANtastic.

El medio físico es el medio utilizado para conectar los equipos informáticos que constituyen la red. Existen dos tipos de medios:

- **Medio guiado**
- **Medio no guiado**

8.3.1. MEDIO GUIADO

En él se incluye el cable de metal (cobre, aluminio, etc.) y cable de fibra óptica. El cable suele instalarse dentro de los edificios o conducciones subterráneas. Entre los cables de metal se incluye el cable de par trenzado y el cable coaxial. También hay disponible cable de fibra óptica con uno o varios filamentos de fibras de plástico o cristal.

VER TAMBIÉN: 6.1.4. TIPOS DE CABLES EN TELECOMUNICACIONES Y 9.1.3. MEDIOS DE TRANSMISIÓN

8.3.1.1. CABLES

Las personas que tienen que instalar los cables para las redes tienen que tomar decisiones importantes, tendrán que evaluar detenidamente las necesidades actuales y futuras y los requisitos de las aplicaciones multimedio de alto ancho de banda, videoconferencia e imágenes. Aunque muchas instituciones no pueden pagar lo que puede que necesiten en el futuro, la instalación de cable de tipo bajo limitará su crecimiento futuro. El cable y el equipo del cable deben cumplir con:

- los requisitos de transmisiones actuales y futuros
- las características eléctricas
- la topología

CABLES DE COBRE

Es una tecnología relativamente barata, bien conocida y fácil de instalar. Es el cable que suele elegirse en la mayoría de las instalaciones de redes a pesar de sus características eléctricas que producen ciertas limitaciones en la transmisión.

Limitaciones:

- es resistente al flujo de electrones, lo que limita la distancia de transmisión
- radia señales que pueden detectarse y le afecta la radiación externa que puede distorsionar las señales.

Los datos binarios se transmiten por el cable de cobre mediante la aplicación de un voltaje en un extremo y su recepción en el otro. Existen tres tipos principales de cables de cobre que se utilizan para transmitir señales digitales.

CABLE PLANO

El cable de cobre plano consta de conductores de cobre rodeados por un aislante. Se utiliza para conectar diversos dispositivos periféricos a distancias cortas y a bajas velocidades binarias. Los cables serial con los que se conectan los modem o las impresoras son de este tipo. El cable plano se ve afectado por diafonía en distancias largas, por lo que no sirve para las redes.

PAR TRENZADO

El cable de par trenzado consta de conductores de núcleo de cobre rodeados por un aislante. Se trenzan dos conductores juntos para formar un par y dicho par forma un circuito por el que se pueden transmitir datos. Un cable es un haz que consta de uno o más pares trenzados rodeados por un aislante. El par trenzado no apantallado(UTP, Unshielded Twisted-Pair) es habitual en la red telefónica. El par trenzado apantallado (STP, Shielded Twisted-Pair) proporciona protección contra las interferencias. Este tipo de cable se utiliza en Ethernet, red en anillo con paso de testigo y otras topologías de red.

En este tipo de cable se definen las siguientes categorías:

Categoría 1: Es el cable telefónico de par trenzado no apantallado tradicional por el que se puede transmitir voz, pero no datos. La mayoría del cable telefónico instalado antes de 1983 es de esta categoría.

Categoría 2: Es el cable de par trenzado no apantallado certificado para la transmisión de datos hasta 4 Mbps y similar al tipo 3 del sistema de cableado de IBM. Este cable tiene cuatro pares trenzados.

Categoría 3: Admite velocidad de transmisión de 10 Mbps y es necesario para las topologías de red en anillo con paso de testigo (4 Mbps) y Ethernet 10 Base a 10 Mbps. El cable tiene cuatro pares y tres trenzas por cada pie.

Categoría 4: Está certificado para velocidades de transmisión de 16 Mbps y es la calidad inferior aceptable para topologías de red en anillo con paso de testigo a 16 Mbps. El cable tiene cuatro pares.

Categoría 5: Es cable de cobre de par trenzado a cuatro hilos de 100 ohm, que puede transmitir datos hasta 100 Mbps para admitir las tecnologías más recientes como Fast Ethernet y ATM. El cable tiene una baja capacidad y presenta una baja diafonía.

CABLE COAXIAL

El cable coaxial consta de un núcleo de cobre sólido rodeado por un aislante . Con el cable coaxial puede conseguirse mayores distancias que con el par trenzado. Es el medio más tradicional para las redes Ethernet y Arcnet, hoy en día son habituales los cables de par trenzado y de fibra óptica.

CABLES DE FIBRA OPTICA

Transmiten señales luminosas por un núcleo de dióxido de silicio, tan puro que una ventana de cinco kilómetros de gruesa construida con este material no distorsionaría la vista . Las transmisiones fotónicas no producen emisiones fuera del cable y no se ven afectadas por la radiación externa.

Se recomienda el cable de fibra cuando la seguridad es clave. Las señales de las computadoras se transmiten por el cable de fibra óptica convirtiendo los 1 y los 0 electrónicos en pulsos de luz. Un diodo emisor de luz en un extremo emite pulsos de luz por un cable que recogen en el otro extremo con un sencillo fotodetector y se vuelven a convertir en señales eléctricas. Como las señales prácticamente no encuentran resistencia y no hay emisiones, las tasas de transmisión por cable de fibra sólo están limitadas por la pureza del núcleo de cristal, la calidad de los equipos y la velocidad de la luz.

Sus principales características son:

Una baja atenuación por Km cuando se transmite por las llamadas ventanas de transmisión, que están ubicadas en torno a los valores siguientes de longitud de onda: 0.8 mm, 1.3 mm y 1.55 mm. Esta última ventana es la que presenta menor atenuación.

Total inmunidad al ruido y a las interferencias electromagnéticas, lo que constituye un medio especiálmente útil en ambientes con alto ruido.

Uso de potencias del orden de los mW, en comparación con otros medios de comunicaciones que requieren potencias mayores.

Su pequeño tamaño y poco peso, hacen de ellas medios de comunicaciones fáciles de instalar, especialmente cuando se trata de completar sistemas sobre ductos preexistentes, sobrecargados por otro tipo de medios que no es posible eliminar.

Teniendo en cuenta el modo de propagación, las fibras ópticas se clasifican en:

- **MONOMODO**

Las dimensiones del núcleo son comparables a la longitud de onda de luz, por lo cual hay un solo modo de propagación y no existe dispersión.

- **MULTIMODO**

Contiene varios modos de propagación y ocurre en consecuencia al efecto de dispersión.

A su vez estas últimas se subdividen en:

- **Índice escalón:** Tiene dispersión, reducido ancho de banda y son de bajo costo, dado que resultan tecnológicamente sencillas de producir.

- **Índice gradual:** Más costosas, pero de gran ancho de banda. Se puede disminuir la dispersión haciendo variar lentamente el índice de refracción entre el núcleo y el recubrimiento.

8.3.1.2. MEDIO NO GUIADO

El representa la técnica que se utiliza para transmitir señales por el aire y el espacio desde el transmisor al receptor, tales como infrarrojos y microondas. Con este medio se pueden cubrir distancias más grandes.

VER TAMBIÉN: 7.1.2.2. MEDIOS INALÁMBRICOS:

Los medios más comunes en la actualidad son:

SATÉLITE

Los satélites de comunicaciones orbitando sobre un punto fijo de la tierra recibe las señales de radio de un amplificador en tierra y las transmite a su destino. La señal de entrada del satélite es recibida por una antena parabólica y se distribuye localmente mediante cables. Este medio se utiliza cuando la comunicación cubre millones de kilómetros.

VER TAMBIÉN: 6.4.1.3. SISTEMAS DE COMUNICACIÓN POR SATÉLITE

MICROONDAS

Las señales de microondas deben viajar sin obstrucciones, por esto las torres de retransmisión son instaladas en cimas de colinas y montes para enviar las señales sobre terrenos disparejos. También las torres de microondas son instaladas en techos elevados para enlazar oficinas que no están muy distantes.

RADIO

Las ondas de radio pueden ser utilizadas como medio de comunicación estas permiten transmitir en distintas frecuencias. También pueden ser utilizadas en una escala geográfica más amplia.

8.4. PROTOCOLOS

Los protocolos de comunicación establecen las reglas para el intercambio de datos dentro de una red. Algunos de los más importantes incluyen:

8.4.1. MODELO OSI

El modelo OSI (Open Systems Interconnection) divide la comunicación en siete capas:

1. **Capa física:** Define los medios físicos de transmisión.

2. **Capa de enlace de datos:** Controla el acceso al medio y la detección de errores.
3. **Capa de red**: Se encarga del direccionamiento y enrutamiento de datos.
4. **Capa de transporte:** Garantiza una comunicación fiable entre dispositivos.
5. **Capa de sesión:** Administra la comunicación entre aplicaciones.
6. **Capa de presentación:** Traduce datos entre diferentes formatos.
7. **Capa de aplicación:** Proporciona servicios a los usuarios (HTTP, FTP, etc.).

8.4.2. PROTOCOLOS MÁS UTILIZADOS

- **Ethernet (IEEE 802.3):** Estándar para redes cableadas.
- **Wi-Fi (IEEE 802.11):** Redes inalámbricas para transmisión de datos.
- **TCP/IP:** Protocolo base de Internet.
- **HTTP/HTTPS:** Protocolo de comunicación para navegación web.
- **DNS:** Sistema de nombres de dominio.
- **DHCP:** Asigna direcciones IP automáticamente.
- **SNMP:** Protocolo para la administración y monitoreo de redes.
- **ICMP:** Usado para diagnósticos y detección de errores en redes.
- **SMTP, IMAP y POP3:** Protocolos para la gestión del correo electrónico.

8.5. EQUIPOS DE RED

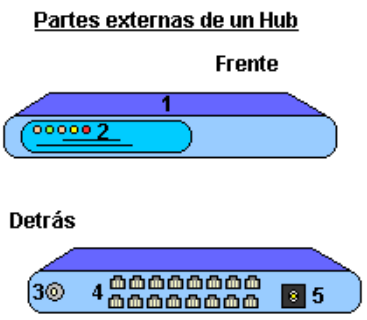
8.5.1. NIC/MAU (TARJETA DE RED)

“Network Interface Card” (Tarjeta de interfaz de red) o “Medium Access Unit” (Medio de unidad de acces). Cada computadora necesita el “hardware” para transmitir y recibir información. Es el dispositivo que conecta la computadora u otro equipo de red con el medio físico. La NIC es un tipo de tarjeta de expansión de la computadora y proporciona un puerto en la parte trasera de la PC al cual se conecta el cable de la red. Hoy en día cada vez son más los equipos que disponen de interfaz de red, principalmente Ethernet,

incorporadas. A veces, es necesario, además de la tarjeta de red, un transceptor. Este es un dispositivo que se conecta al medio físico y a la tarjeta, bien porque no sea posible la conexión directa (10base 5) o porque el medio sea distinto del que utiliza la tarjeta.

8.5.2. HUBS (CONCENTRADORES)

Son equipos que permiten estructurar el cableado de las redes. La variedad de tipos y características de estos equipos es muy grande. En un principio eran solo concentradores de cableado, pero cada vez disponen de mayor número de capacidad de la red, gestión remota, etc. La tendencia es a incorporar más funciones en el concentrador. Existen concentradores para todo tipo de medios físicos.



8.5.3. REPETIDORES

Son equipos que actúan a nivel físico. Prolongan la longitud de la red uniendo dos segmentos y amplificando la señal, pero junto con ella amplifican también el ruido. La red sigue siendo una sola, con lo cual, siguen siendo válidas las limitaciones en cuanto al número de estaciones que pueden compartir el medio.

8.5.4. "BRIDGES" (PUENTES)

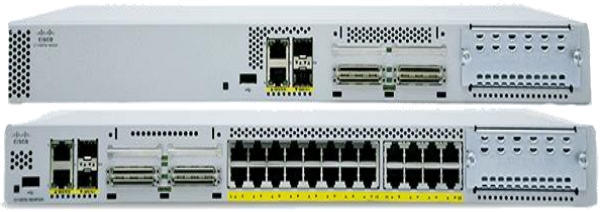
Son equipos que unen dos redes actuando sobre los protocolos de bajo nivel, en el nivel de control de acceso al medio. Solo el tráfico de una red que va dirigido a la otra atraviesa el dispositivo. Esto permite a los administradores dividir las redes en segmentos lógicos, descargando de tráfico las interconexiones. Los bridges producen las señales, con lo cual no se transmite ruido a través de ellos.

8.5.5. "ROUTERS" (ENCAMINADORES)

Son equipos de interconexión de redes que actúan a nivel de los protocolos de red. Permite utilizar varios sistemas de interconexión mejorando el rendimiento de la transmisión entre redes. Su funcionamiento es más lento que los bridges pero su capacidad es mayor. Permiten, incluso, enlazar dos redes basadas en un protocolo, por medio de otra que utilice un protocolo diferente.

8.5.6. "GATEWAYS"

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. La traducción de las unidades de información reduce mucho la velocidad de transmisión a través de estos equipos.



8.5.7. SERVIDORES DE TERMINALES E IMPRESORAS

Son equipos que permiten la conexión a la red de equipos periféricos tanto para la entrada como para la salida de datos. Estos dispositivos se ofrecen en la red como recursos compartidos. Así un terminal conectado a uno de estos dispositivos puede establecer sesiones contra varios ordenadores multiusuario disponibles en la red. Igualmente, cualquier sistema de la red puede imprimir en las impresoras conectadas a un servidor

8.5.8. MODEMS

Son equipos que permiten a las computadoras comunicarse entre sí a través de líneas telefónicas; modulación y demodulación de señales electrónicas que pueden ser procesadas por computadoras. Los módems pueden ser externos (un dispositivo de comunicación) o interno (dispositivo de comunicación interno o tarjeta de circuitos que se inserta en una de las ranuras de expansión de la computadora).

8.5.8.1. CERTIFICACIÓN DE REDES

La certificación de redes es un proceso fundamental en la instalación y mantenimiento de infraestructuras de cableado estructurado, garantizando que cumplan con los estándares internacionales de calidad y desempeño. Este proceso se realiza mediante diversas pruebas que verifican la integridad, eficiencia y seguridad del cableado, asegurando que las redes de datos funcionen de manera óptima y sin interferencias. La certificación es especialmente crítica en entornos empresariales, industriales y de telecomunicaciones, donde el rendimiento de la red es esencial para las operaciones diarias.

A continuación, se detallan las principales pruebas utilizadas en la certificación de redes:

8.5.8.2. Verificación de Continuidad

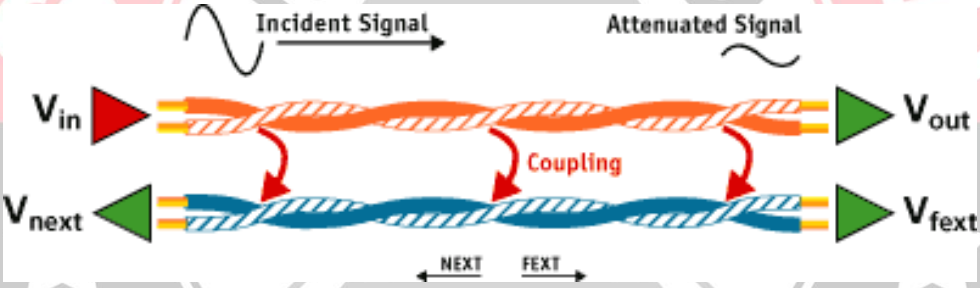
Esta prueba asegura que los cables estén correctamente conectados de extremo a extremo, sin cortes ni conexiones defectuosas. Se verifica que los pares de cables estén correctamente alineados según los estándares TIA/EIA-568A o TIA/EIA-568B. La verificación de continuidad también detecta errores comunes como inversiones de pares, pares abiertos o cortocircuitos.

8.5.8.3. Pruebas de Atenuación y Diafonía

La atenuación se refiere a la pérdida de señal a medida que viaja por el cable, lo que puede afectar la calidad de la transmisión de datos. Esta prueba evalúa si la atenuación se encuentra dentro de los límites establecidos por los estándares, asegurando una transmisión confiable.

La diafonía (NEXT y FEXT) mide la interferencia entre los pares de cables dentro del mismo cableado. Existen dos tipos de diafonía:

- **NEXT (Near-End Crosstalk):** Evalúa la interferencia entre pares en el extremo cercano del cable.
- **FEXT (Far-End Crosstalk):** Mide la interferencia en el extremo lejano del cable.



Un alto nivel de diafonía puede provocar errores en la transmisión de datos, por lo que su medición es crucial en la certificación de redes.

8.5.8.4. Certificación con Fluke Tester

El uso de herramientas profesionales como el **Fluke Tester** es esencial para validar redes de alta velocidad, como las implementaciones de **Cat 5e, Cat 6, Cat 6A, Cat 7 y fibra óptica**. Estos dispositivos permiten realizar pruebas exhaustivas que incluyen:

- Resistencia y continuidad del cableado.
- Medición de atenuación y diafonía.
- Verificación de velocidad de transmisión y ancho de banda.
- Identificación de fallos en conectores y empalmes.
- Generación de informes de certificación con resultados detallados.

La certificación con Fluke Tester es un estándar en la industria y se utiliza para validar redes según normativas como ANSI/TIA-568 y ISO/IEC 11801.

8.5.8.5. Mediciones de Pérdida Óptica en Fibra

En redes de **fibra óptica**, se realizan pruebas de pérdida óptica para evaluar la eficiencia de la transmisión de luz a través del medio de fibra. Entre las pruebas más comunes se encuentran:

- **Pérdida por inserción (IL - Insertion Loss):** Mide la cantidad de señal que se pierde al pasar a través de una conexión o empalme.
- **Pérdida por retorno (RL - Return Loss):** Evalúa la cantidad de señal reflejada de regreso hacia la fuente, lo cual puede afectar la calidad de la transmisión.
- **OTDR (Optical Time-Domain Reflectometer):** Un analizador que permite identificar empalmes, conectores defectuosos o pérdidas anormales a lo largo de un enlace de fibra óptica.

8.5.8.6. Pruebas de Interferencia Electromagnética (EMI)

En entornos donde hay equipos eléctricos y electrónicos operando, la interferencia electromagnética puede afectar el rendimiento del cableado. Estas pruebas verifican la resistencia del cableado ante fuentes de interferencia como:

- Motores eléctricos.
- Transformadores y fuentes de alimentación.
- Equipos de radiofrecuencia y comunicaciones inalámbricas.

Los cables deben contar con protección adecuada, como blindaje o puesta a tierra, para evitar interferencias y garantizar la estabilidad de la transmisión de datos.

Conclusiones

La certificación de redes es un paso esencial en la implementación de infraestructuras de comunicación, ya que garantiza la calidad, seguridad y rendimiento del cableado estructurado y de la fibra óptica. Mediante la aplicación de pruebas especializadas, es posible identificar problemas, corregir defectos y asegurar el cumplimiento de los estándares internacionales. Contar con una red certificada no solo mejora la fiabilidad de la transmisión de datos, sino que también reduce costos de mantenimiento y fallos en el sistema a largo plazo.

9. SISTEMAS INFORMÁTICOS Y REDES LOCALES

9.1. ARQUITECTURA Y COMPONENTES DE UN SISTEMA INFORMÁTICO

Un sistema informático es un conjunto integrado de recursos de hardware y software diseñados para almacenar, procesar, transmitir y presentar información. Su arquitectura define cómo interactúan estos elementos y cómo se organiza el sistema para cumplir con las funciones requeridas.

9.1.1. HARDWARE

El **hardware** incluye todos los componentes físicos del sistema informático. Estos pueden clasificarse en varios grupos funcionales:

- **Unidad Central de Procesamiento (CPU)**: Considerado el "cerebro" del sistema. Es el encargado de interpretar y ejecutar instrucciones. Está compuesto por:
  - Unidad de control: coordina el funcionamiento del sistema.
  - Unidad aritmético-lógica (ALU): realiza operaciones matemáticas y lógicas.
  - Registros: almacenan temporalmente datos y direcciones.
- **Memoria principal (RAM)**: Memoria de acceso aleatorio que guarda datos e instrucciones de forma temporal mientras el sistema está en funcionamiento. Su velocidad de acceso es mucho mayor que la del almacenamiento permanente.
- **Memorias secundarias (HDD, SSD)**: Se encargan del almacenamiento permanente de datos. El SSD (unidad de estado sólido) ofrece mayor velocidad y fiabilidad que un disco duro mecánico (HDD).

- **Placa base (motherboard)**: Circuito principal donde se conectan todos los componentes. Incluye el chipset, buses de datos, zócalos para CPU, slots para RAM, conectores de expansión, etc.
- **Tarjetas de expansión**: Añaden funcionalidades adicionales, como:
  - Tarjetas gráficas (GPU) para procesamiento gráfico.
  - Tarjetas de red (NIC) para conexión a redes LAN o WAN.
  - Tarjetas de sonido o controladoras adicionales.
- **Periféricos**:
  - Entrada: teclado, ratón, escáner, cámara.
  - Salida: monitor, impresora, altavoces.
  - Entrada/Salida: pantallas táctiles, memorias USB.

📌 Referencia ampliada: Ver sección 6.1.1. "Componentes principales de un sistema microinformático".

9.1.2. SOFTWARE

El **software** es el conjunto de programas que permiten utilizar el hardware para realizar tareas. Se clasifica principalmente en:

- **Sistema operativo (SO)**: Es el intermediario entre el usuario y el hardware. Gestiona recursos como la memoria, CPU y dispositivos. Ejemplos: Windows 11, Ubuntu Linux, macOS Ventura.
- **Software de aplicación**: Programas diseñados para realizar tareas específicas. Ejemplos:
  - Ofimática: Microsoft Word, Excel, LibreOffice.
  - Diseño: AutoCAD, Photoshop.
  - Navegación web: Google Chrome, Firefox.
- **Controladores (drivers)**: Software que permite al sistema operativo comunicarse correctamente con los dispositivos de hardware, como impresoras, tarjetas gráficas o de red.

9.1.3. REDES Y CONECTIVIDAD

La conectividad y las redes son elementos fundamentales en cualquier sistema informático moderno. Permiten la comunicación entre dispositivos, el acceso a recursos compartidos y la conexión a servicios externos, como Internet. Una red informática es

un conjunto de dispositivos interconectados que comparten datos, recursos y servicios. Las redes pueden clasificarse según su tamaño, estructura, tecnología de transmisión y propósito.

¿Por qué son necesarias las redes?

- **Intercambio de información** entre usuarios, dispositivos o sistemas.
- **Compartición de recursos**, como impresoras, archivos, almacenamiento o bases de datos.
- **Acceso a Internet** para navegación, correo, servicios en la nube, etc.
- **Trabajo colaborativo** en entornos empresariales, educativos o industriales.

1. Redes según su alcance y cobertura

- **PAN (Personal Area Network)**: Redes personales de corto alcance (hasta 10 metros). Ejemplo: conexión entre un smartphone y unos auriculares Bluetooth.
- **LAN (Local Area Network)**: Redes que cubren áreas pequeñas como oficinas, casas o escuelas. Permiten alta velocidad de transmisión y fácil control.
- **WLAN (Wireless LAN)**: Variante inalámbrica de las LAN. Utiliza tecnologías como Wi-Fi y permite movilidad dentro del área de cobertura.
- **MAN (Metropolitan Area Network)**: Redes que abarcan una ciudad o un campus universitario. Suelen conectar varias LAN mediante fibra óptica.
- **WAN (Wide Area Network)**: Redes de gran extensión, como Internet, que conectan dispositivos a nivel nacional o internacional.

2. Dispositivos de red fundamentales

2.1. Tarjetas de red (NIC - Network Interface Card)

- Componente que permite a un equipo conectarse a una red, mediante cable (Ethernet) o de forma inalámbrica (Wi-Fi).
- Cada tarjeta posee una dirección MAC (Media Access Control), única en el mundo, que identifica al dispositivo dentro de la red.
- Hoy día, muchas placas base incluyen interfaces de red integradas tanto para cable como para Wi-Fi.

2.2. Routers

- Encargados de interconectar redes diferentes (por ejemplo, una red local con Internet).
- Actúan como puerta de enlace (gateway) y asignan direcciones IP a los dispositivos de la red (normalmente mediante DHCP).
- Algunos routers domésticos también incluyen funciones de cortafuegos (firewall), switch y punto de acceso Wi-Fi.

2.3. Switches

- Dispositivos que conectan varios equipos dentro de la misma red local.

- Operan en la **capa 2 del modelo OSI** (nivel de enlace) y gestionan los paquetes de datos basándose en las direcciones MAC.
- A diferencia de los hubs, los switches reducen el tráfico al enviar datos solo al dispositivo destinatario correcto.

2.4. Puntos de acceso (Access Point)

- Permiten conectar dispositivos inalámbricos a una red cableada.
- Ampliamente utilizados en entornos donde se requiere movilidad o donde el cableado es difícil.
- Pueden funcionar como repetidores, extensores de red o nodos independientes.

2.5. Modems

- Dispositivo que convierte la señal digital de un ordenador en una señal analógica que puede transmitirse a través de líneas telefónicas (en tecnologías antiguas) o de fibra/cable en sistemas actuales.
- Hoy en día muchos routers incluyen funciones de módem (router-módem).

3. Medios de transmisión

Los datos en una red pueden transmitirse de dos formas principales

3.1. Medios guiados (cableados)

- **Par trenzado (UTP/STP)**:
  - Utilizado en redes Ethernet.
  - Categorías: Cat 5e (1000 Mbps), Cat 6 (hasta 10 Gbps), Cat 7 (mayor apantallamiento y velocidad).
- **Cable coaxial**:
  - Menos común hoy día en redes locales, pero se utilizó ampliamente en redes antiguas y sistemas de televisión por cable.
- **Fibra óptica**:
  - Medio de transmisión más rápido y seguro.
  - Utiliza pulsos de luz para transmitir datos.
  - Mayor capacidad, menor latencia y mayor alcance que el cableado de cobre.
  - Coste más elevado y más difícil de instalar.

3.2. Medios no guiados (inalámbricos)

- **Wi-Fi (IEEE 802.11)**:
  - Estándar más común en redes inalámbricas.
  - Versiones actuales: 802.11ac (Wi-Fi 5), 802.11ax (Wi-Fi 6), 802.11be (Wi-Fi 7).
  - Opera en bandas de 2.4 GHz y 5 GHz, y ahora también en 6 GHz (Wi-Fi 6E).

- **Bluetooth**:
  - Usado en PAN para conectar dispositivos cercanos (auriculares, móviles, periféricos).
- **LTE/5G**:
  - Redes móviles que también permiten la conexión de dispositivos informáticos a través de redes WAN móviles.

4. Protocolos de comunicación

Los protocolos son normas que rigen cómo los dispositivos se comunican entre sí. Algunos de los más importantes son:

- **TCP/IP (Transmission Control Protocol / Internet Protocol)**:
  - Base de Internet.
  - Divide los datos en paquetes, los envía y reensambla en destino.
- **DHCP (Dynamic Host Configuration Protocol)**:
  - Asigna automáticamente direcciones IP y otros parámetros de red a los dispositivos.
- **DNS (Domain Name System)**:
  - Traduce nombres de dominio (como www.google.com) a direcciones IP comprensibles por las máquinas.
- **HTTP/HTTPS**:
  - Protocolo para la transferencia de páginas web.
  - HTTPS incluye cifrado SSL/TLS para comunicaciones seguras.
- **FTP (File Transfer Protocol)**:
  - Para transferir archivos entre clientes y servidores.
- **ICMP (Internet Control Message Protocol)**:
  - Protocolo utilizado por herramientas como ping para diagnosticar conectividad.

5. Topologías de red

La forma en que se organizan físicamente los dispositivos en una red se llama topología. Algunas comunes:

- **En estrella**: Cada dispositivo se conecta a un nodo central (switch o router). Muy común en LAN.
- **En bus**: Todos los dispositivos comparten un único canal de comunicación (antiguo).
- **En anillo**: Los dispositivos forman un círculo cerrado. No habitual en redes modernas.
- **Malla**: Todos los dispositivos están interconectados. Alta redundancia y fiabilidad (típica en redes críticas o de alta disponibilidad).
- **Híbrida**: Combinación de las anteriores.

6. Direccionamiento IP

Cada dispositivo de una red necesita una dirección única para poder comunicarse.

- **IPv4**:
  - Formato de 32 bits, escrito como cuatro números separados por puntos (ej. 192.168.1.1).
  - Ejemplo de IP privada: 192.168.0.0/16.
- **IPv6**:
  - Formato de 128 bits, desarrollado para reemplazar al IPv4 por agotamiento de direcciones.
  - Ejemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- **Direcciones estáticas y dinámicas**:
  - **Estáticas**: asignadas manualmente.
  - **Dinámicas**: asignadas por el servidor DHCP.

7. Ejemplos de redes en entornos reales

- **Entorno doméstico**: Router que proporciona Wi-Fi, con ordenadores, móviles, smart TVs y consolas conectadas. IPs privadas asignadas por DHCP. Acceso a Internet mediante NAT (traducción de direcciones).
- **Empresa mediana**: LAN cableada con switches y puntos de acceso Wi-Fi. Segmentación en VLANs por departamentos. Servidor central con políticas de seguridad, impresoras compartidas y firewall de red.
- **Entorno industrial o ferroviario**: Redes cableadas con switches industriales, protocolos redundantes (como PRP, HSR), PLCs conectados, redes SCADA. Se prioriza la latencia baja, la fiabilidad y la seguridad física y lógica.

9.2. INSTALACIÓN Y CONFIGURACIÓN DE REDES LOCALES

Una **red local (LAN – Local Area Network)** es una infraestructura de comunicación que conecta múltiples dispositivos (ordenadores, impresoras, servidores, etc.) dentro de una ubicación geográfica limitada: un hogar, una oficina, un aula o un taller industrial. La instalación y configuración adecuada de una red LAN permite compartir recursos, aumentar la productividad y mejorar la seguridad de los sistemas.

9.2.1. TIPOS DE REDES LOCALES

Las redes LAN pueden clasificarse según el tipo de medio físico utilizado y la forma en que se interconectan los dispositivos:

Redes cableadas (Ethernet)

- Utilizan cables de par trenzado (UTP/STP) o fibra óptica para la conexión de los dispositivos.
- Estándares como **IEEE 802.3** permiten velocidades de transmisión desde **10 Mbps hasta 100 Gbps**.
- Las categorías de cable más usadas:
  - **Cat 5e**: hasta 1 Gbps.
  - **Cat 6/6a**: hasta 10 Gbps, mejor apantallamiento.
  - **Cat 7/8**: para redes de alto rendimiento.
- **Ventajas**:
  - Mayor velocidad y estabilidad.
  - Menor latencia.
  - Mayor seguridad ante interferencias o ataques inalámbricos.
- **Inconvenientes**:
  - Menor flexibilidad de movimiento.
  - Instalación más compleja y costosa (cableado estructurado).

Aplicación práctica: Ideal para oficinas, aulas informáticas, laboratorios técnicos o centros de datos.

Redes inalámbricas (Wi-Fi)

- Utilizan señales de radiofrecuencia para conectar dispositivos sin cables.
- Basadas en el estándar **IEEE 802.11**.
- Versiones:
  - **Wi-Fi 4 (802.11n)**: hasta 600 Mbps.
  - **Wi-Fi 5 (802.11ac)**: hasta 3,5 Gbps (5 GHz).
  - **Wi-Fi 6/6E (802.11ax)**: mejora la eficiencia, la velocidad y la capacidad de dispositivos conectados.
- **Ventajas**:
  - Gran flexibilidad y movilidad.
  - Instalación más rápida.
- **Inconvenientes**:
  - Menor seguridad si no está bien configurada.
  - Interferencias por obstáculos o por otras redes.
  - Cobertura limitada.

Aplicación práctica: Oficinas abiertas, hogares, entornos educativos con portátiles o tablets.

Redes híbridas

- Combinan tramos cableados (para servidores, impresoras de red, PCs fijos) con conectividad Wi-Fi para dispositivos móviles.
- Permiten aprovechar las ventajas de ambos tipos: **rendimiento + flexibilidad**.
- Muy utilizadas en pequeñas y medianas empresas, así como en entornos domésticos avanzados.

Aplicación práctica: Entornos mixtos con usuarios fijos y móviles, aulas técnicas o edificios de oficinas.

9.2.2. ELEMENTOS DE UNA RED LOCAL

Una red local se compone de diversos **dispositivos activos y pasivos** que permiten la conexión, el control y la gestión del tráfico de datos:

Puntos de acceso (Access Points – APs)

- Dispositivos que generan señal Wi-Fi.
- Se conectan a la red cableada para ofrecer conectividad inalámbrica.
- En redes empresariales, pueden gestionarse centralizadamente mediante **controladores Wi-Fi**.

Ejemplo: En una escuela técnica, varios APs distribuidos por los pasillos garantizan buena cobertura a portátiles en todas las aulas.

Switches (conmutadores)

- Permiten conectar múltiples dispositivos por cable.
- Operan en **capa 2** del modelo OSI (nivel de enlace).
- Pueden ser:
  - **No gestionables**: plug & play, sin configuración.
  - **Gestionables**: permiten configurar VLANs, QoS, SNMP, etc.
- Reemplazan a los antiguos **hubs**, que enviaban todos los datos a todos los puertos (ineficientes y obsoletos).

Routers

- Dispositivos que **encaminan el tráfico** entre redes diferentes (por ejemplo, entre una LAN y una WAN o Internet).
- Funciones comunes:
  - Servidor DHCP.
  - Firewall básico.
  - Traducción NAT/PAT.
  - Punto de acceso Wi-Fi integrado.
- En entornos profesionales, se usan routers dedicados con políticas de seguridad avanzadas.

Servidores de red

- Equipos que proporcionan servicios a los clientes de la red:
  - Archivos (servidor de ficheros).
  - Aplicaciones (servidor de software o de bases de datos).

- Impresión (servidor de impresión).
- Autenticación (servidor LDAP o Active Directory).

- Pueden ser físicos o virtualizados, y estar alojados en local o en la nube.

9.2.3. CONFIGURACIÓN DE UNA RED LOCAL

1. Diseño de la red

El primer paso es la **planificación**, que incluye:

- Determinar la **topología** más adecuada:
  - Estrella (la más común en LAN).
  - Bus o anillo (obsoletas).
  - Malla (alta redundancia, uso industrial o crítico).
- Analizar el **número de dispositivos** conectados (ordenadores, impresoras, móviles...).
- Planificar los **puntos de acceso Wi-Fi** si es red híbrida.
- Estimar necesidades de **ancho de banda**, segmentación o crecimiento futuro.

Consejo técnico: Siempre prever un 20–30 % más de capacidad para evitar saturación futura.

2. Asignación de direcciones IP

Cada dispositivo necesita una **IP única** dentro de la red. Dos métodos:

- **Estática**:
  - Manualmente configurada.
  - Ideal para dispositivos críticos (servidores, impresoras, switches).
  - Requiere buena planificación de direcciones para evitar conflictos.
- **Dinámica (DHCP)**:
  - Asignación automática por un **servidor DHCP** (normalmente el router).
  - Ideal para dispositivos móviles o equipos de usuarios.
  - Puede complementarse con **reservas DHCP** (asignación fija para dispositivos específicos).

3. Configuración de dispositivos de red

- **Router/AP**:
  - Acceder mediante navegador a la IP de gestión (normalmente 192.168.1.1).
  - Cambiar SSID, activar seguridad WPA2/WPA3.
  - Configurar canales Wi-Fi para evitar interferencias.
  - Definir IPs estáticas o rango DHCP.

- Activar firewall o filtrado por MAC, si es necesario.

- **Switch gestionable**:
  - Configuración de VLANs para segmentar el tráfico.
  - QoS para priorizar ciertos servicios (VoIP, streaming).
  - Supervisión SNMP para mantenimiento remoto.

Ejemplo práctico: En una FP de mantenimiento ferroviario, se segmenta la red en VLANs: una para simuladores de trenes, otra para la administración, otra para el aula.

4. Pruebas de conectividad

Las pruebas de conectividad son fundamentales en el diagnóstico y resolución de problemas de red. Permiten verificar si un dispositivo está accesible, conocer la configuración de red actual, analizar la ruta de los datos a través de la red, examinar el estado de los puertos y obtener información sobre los nombres de dominio. A continuación, se detallan las herramientas más comunes utilizadas para estas pruebas:

4.1. Ping

Ping (Packet Internet Groper) es una herramienta básica de diagnóstico utilizada para comprobar la **conectividad entre dos dispositivos** de red. Su funcionamiento se basa en el envío de paquetes ICMP (Internet Control Message Protocol) al host de destino y espera una respuesta.

```
Pinging google.com [142.251.133.78] with 32 bytes of data:
Reply from 142.251.133.78: bytes=32 time=10ms TTL=116
Reply from 142.251.133.78: bytes=32 time=9ms TTL=116
Reply from 142.251.133.78: bytes=32 time=9ms TTL=116
Reply from 142.251.133.78: bytes=32 time=8ms TTL=116

Ping statistics for 142.251.133.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 10ms, Average = 9ms
```

- **Uso básico**:
  `ping 192.168.1.1`
  Comprueba si el host con IP 192.168.1.1 responde.
- **Lo que muestra**:
  - Tiempo de respuesta (latencia) en milisegundos.
  - Número de paquetes enviados, recibidos y perdidos.
  - Dirección IP del host.

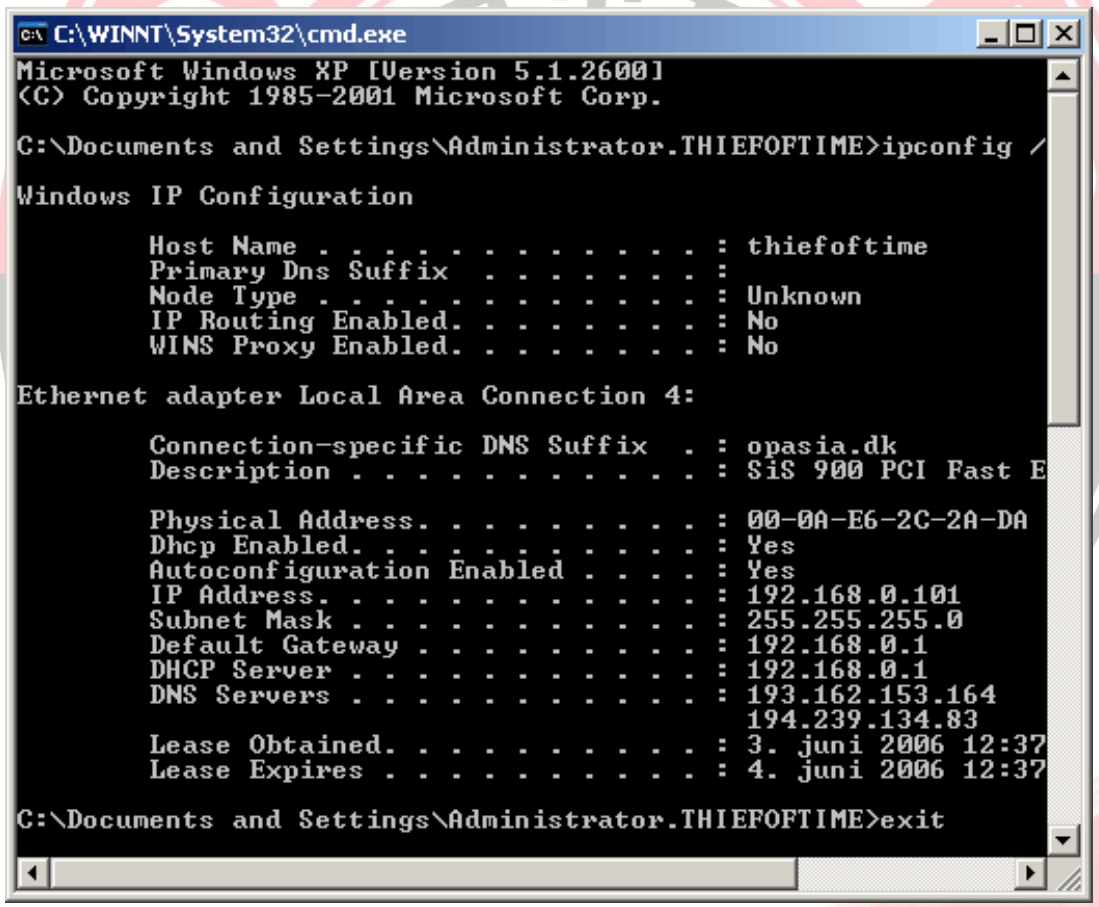
- TTL (Time to Live): número de saltos máximos que puede realizar un paquete.

- **Aplicaciones**:
  - Comprobar si un equipo está encendido y accesible.
  - Detectar pérdida de paquetes o retardo excesivo.
  - Verificar si un servidor remoto está respondiendo.
- **Limitaciones**:
  - Puede estar bloqueado por firewalls o configuraciones de red.
  - No mide el rendimiento real del servicio, solo si responde.

4.2. Ipconfig / Ifconfig

Estas utilidades permiten visualizar y configurar los parámetros de red del sistema operativo.

- **ipconfig (Windows)**:



  - Muestra la configuración IP actual de las interfaces de red.
  - Comando: `ipconfig`
  - Opciones útiles:
    - `ipconfig /all`: información completa, incluyendo direcciones MAC, servidores DNS, DHCP, etc.

- `ipconfig /release` y `ipconfig /renew`: liberan y renuevan la dirección IP mediante DHCP.
- `ipconfig /flushdns`: borra la caché de resolución de DNS.

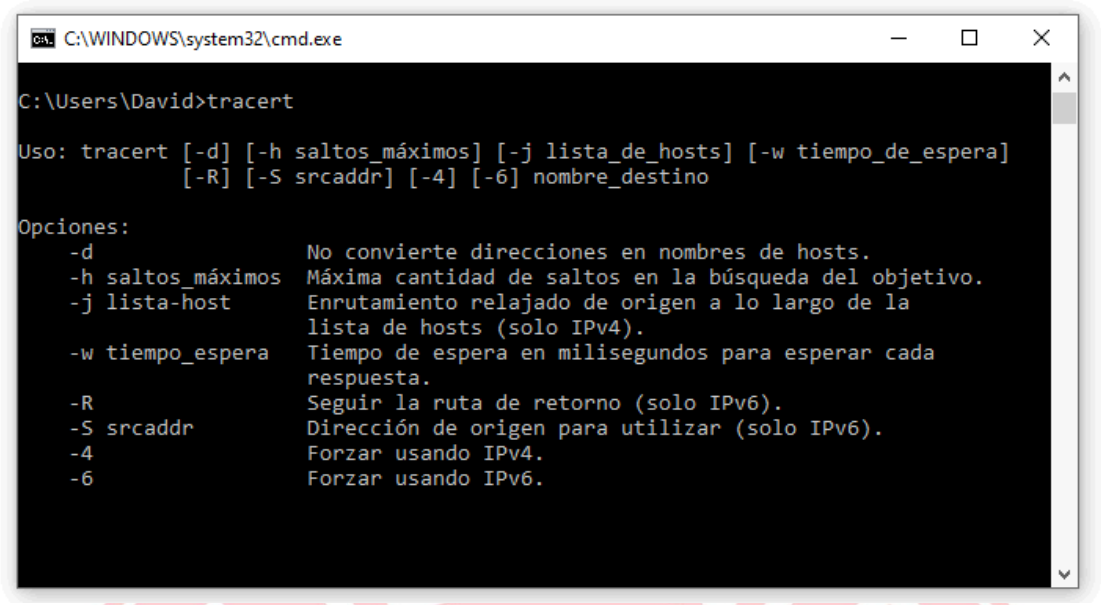
- **ifconfig (Linux/Unix/macOS)**:
  - Similar a ipconfig, muestra y configura interfaces de red.
  - Comando básico: `ifconfig`
  - Se puede usar para activar/desactivar interfaces (`ifconfig eth0 up/down`), asignar IPs, etc.

```
[Tue 25/02/18 10:47 WIB][pts/0][x86_64/linux-gnu/6.13.2-1-default][5.9]
<root@aventurine-topaz:/home/vulcansphere>
zsh/3 831 # ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4029  bytes 461639 (450.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4029  bytes 461639 (450.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ppp0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1400
        inet 172.31.255.5  netmask 255.255.255.255  destination 172.31.255.1
        inet6 2a0a:280:2a26:2120:1473:f066:e1b9:bbbc  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::991f:6497:9eae:bca8  prefixlen 128  scopeid 0x20<link>
        inet6 2a0a:280:2a26:2120:991f:6497:9eae:bca8  prefixlen 64  scopeid 0x0<global>
        ppp  txqueuelen 3  (Point-to-Point Protocol)
        RX packets 1732327  bytes 2172384238 (2.0 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 655248  bytes 62609831 (59.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.186  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fd01::c9d:954a:2bc6:eeb5  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::607b:21f6:dd8:cee7  prefixlen 64  scopeid 0x20<link>
        inet6 fd01::ea2c:6811:b6f0:c243  prefixlen 64  scopeid 0x0<global>
        ether 14:d4:24:74:da:9d  txqueuelen 1000  (Ethernet)
        RX packets 1733353  bytes 2262569215 (2.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 655870  bytes 115102430 (109.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Aplicaciones**:
  - Comprobar si el equipo tiene IP asignada.
  - Ver direcciones de puerta de enlace, subred y DNS.
  - Diagnosticar problemas de configuración.

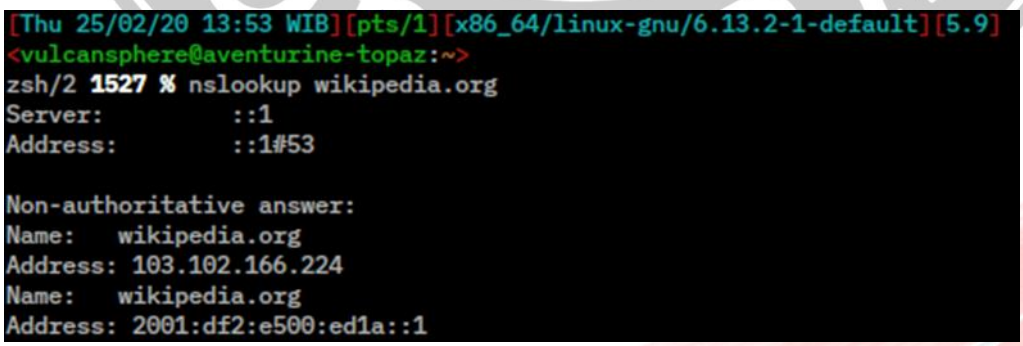
4.3. Traceroute / Tracert

Traceroute (Linux/macOS) o **Tracert (Windows)** permite conocer la ruta exacta que siguen los paquetes desde el origen hasta el destino, identificando cada uno de los **routers intermedios**.



- **Comando básico**:
  - Linux/macOS: `traceroute www.google.com`
  - Windows: `tracert www.google.com`
- **Funcionamiento**:
  - Envía paquetes con TTL creciente (Time To Live).
  - Cada router intermedio reduce el TTL en 1; cuando llega a 0, el router responde con un mensaje ICMP.
  - Se identifica cada salto (nodo) y el tiempo que tardan en responder.
- **Aplicaciones**:
  - Localizar fallos o cortes en la ruta de comunicación.
  - Identificar cuellos de botella o latencias elevadas.
  - Verificar si un problema es interno (red local) o externo (proveedor de internet).

4.4. Nslookup

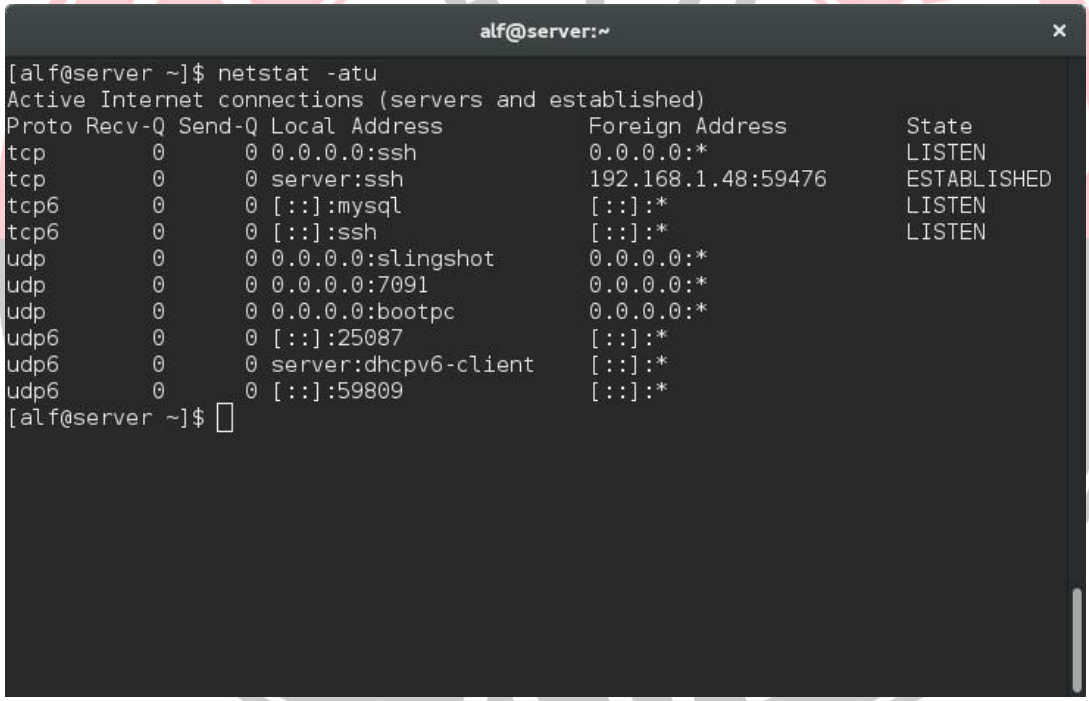


Nslookup (Name Server Lookup) es una herramienta que permite consultar los **servidores DNS** para resolver nombres de dominio a direcciones IP (y viceversa).

- **Uso básico**:
  - `nslookup www.google.com`
    Devuelve la IP asociada al dominio.
- **Modo interactivo**:
  - Ejecutar `nslookup` sin argumentos entra en modo interactivo.
  - Se pueden hacer consultas específicas: MX (correo), NS (servidores), A (dirección IPv4), AAAA (IPv6), etc.
- **Aplicaciones**:
  - Verificar si la resolución DNS funciona correctamente.
  - Comprobar si un dominio está mal configurado.
  - Investigar registros DNS de dominios (correo, subdominios, etc.).
  - Utilizado en tareas de administración de redes y ciberseguridad.

4.5. Netstat

Netstat (Network Statistics) permite examinar **las conexiones de red activas, los puertos abiertos, las estadísticas de red** y más.



- **Comando básico**:
  - Windows: `netstat`
  - Linux/macOS: `netstat` o `ss` (más moderno)
- **Opciones comunes**:
  - `netstat -a`: muestra todas las conexiones y puertos en escucha.
  - `netstat -n`: muestra direcciones y puertos en formato numérico.
  - `netstat -o` (Windows): muestra el ID del proceso que está usando cada puerto.
  - `netstat -r`: muestra la tabla de rutas del sistema.
  - `netstat -s`: estadísticas por protocolo (TCP, UDP, ICMP...).

- **Aplicaciones**:
  - Ver qué aplicaciones están usando la red.
  - Detectar conexiones no autorizadas.
  - Identificar posibles procesos maliciosos.
  - Auditar puertos abiertos o servicios en ejecución.

Conclusión:

El uso combinado de estas herramientas ofrece un **enfoque completo para el diagnóstico y análisis de redes**, desde la conectividad básica hasta la detección de rutas, resolución de dominios, inspección de puertos y análisis de configuración IP. Son indispensables tanto para técnicos de soporte como para administradores de sistemas, profesionales de ciberseguridad y estudiantes del ámbito informático.

Caso real: Si un PC no accede a Internet, se puede usar ping 8.8.8.8 para ver si tiene salida y tracert google.es para localizar el fallo.

Resumen práctico de instalación

1. Planificar el diseño de red (topología, puntos de conexión).
2. Instalar físicamente el cableado y dispositivos.
3. Configurar routers, switches, APs y servidores.
4. Establecer políticas de IP estáticas/dinámicas.
5. Realizar pruebas de conectividad y rendimiento.
6. Documentar la red para mantenimiento futuro.

9.3. SEGURIDAD EN REDES LAN

Una red local (LAN), aunque se limite a un entorno cerrado como una oficina, centro educativo o planta industrial, **no está exenta de amenazas**. Las redes actuales, por estar conectadas a Internet o incorporar dispositivos móviles y servicios en la nube, requieren **medidas de seguridad robustas** para proteger los datos, garantizar la disponibilidad del sistema y prevenir accesos no autorizados.

La seguridad de una red LAN no es solo una cuestión de configuración técnica, sino también de **políticas de uso, concienciación del usuario y mantenimiento constante**.

9.3.1. PRINCIPALES AMENAZAS A LA SEGURIDAD EN REDES LAN

Las amenazas pueden ser **externas o internas**, accidentales o deliberadas. A continuación, se describen las más comunes:

Accesos no autorizados

- Ocurren cuando un usuario, dispositivo o atacante externo se conecta a la red sin permisos.
- En redes Wi-Fi, esto puede suceder si la red no está protegida con cifrado o si se utiliza una contraseña débil.
- En redes cableadas, puede suceder si hay puertos de red activos accesibles públicamente.

Ejemplo: Un visitante que se conecta a la red interna con su portátil sin ser detectado puede tener acceso a recursos confidenciales si no hay control de acceso.

Intercepción de datos

- También conocida como **sniffing**, es la captura no autorizada de paquetes de datos que circulan por la red.
- Puede permitir a un atacante leer correos electrónicos, contraseñas u otra información sensible.
- En redes inalámbricas o redes sin cifrado, el riesgo es aún mayor.
- Uno de los métodos más utilizados es el ataque **MITM (Man-In-The-Middle)**, donde el atacante se sitúa entre dos dispositivos para interceptar y modificar la comunicación.

Ejemplo: Un atacante puede interceptar una sesión web no cifrada (HTTP) y suplantar al usuario.

Malware

- Incluye **virus, gusanos, troyanos, ransomware**, spyware y otras variantes.
- Se propaga fácilmente por la red mediante archivos compartidos, correos electrónicos, dispositivos USB o vulnerabilidades de software.
- Puede generar daños como:
    - Pérdida o robo de información.
    - Inhabilitación de sistemas críticos.
    - Cifrado de datos (ransomware) y solicitud de rescate económico.

Ejemplo: El ransomware WannaCry infectó redes empresariales y hospitalarias en todo el mundo en 2017 a través de una vulnerabilidad de red en Windows.

Ataques de denegación de servicio (DoS / DDoS)

- Intentan saturar los recursos de la red o de un servidor específico para dejarlo inoperativo.
- En **DoS**, el ataque proviene de un único origen; en **DDoS (Distribuido)**, proviene de múltiples equipos zombis (botnet).
- Aunque más comunes en redes públicas, también pueden afectar LAN cuando hay dispositivos internos comprometidos.

Ejemplo: En una red empresarial, un equipo infectado puede generar tráfico excesivo y bloquear el acceso a los servidores de archivos.

Amenazas internas

- Provienen de empleados, técnicos o usuarios autorizados que, intencionalmente o no, comprometen la seguridad:
  - Mal uso de privilegios.
  - Descarga de software no autorizado.
  - Configuración insegura de dispositivos.

Ejemplo: Un trabajador que conecta un USB con malware sin saberlo o que comparte credenciales con otros compañeros.

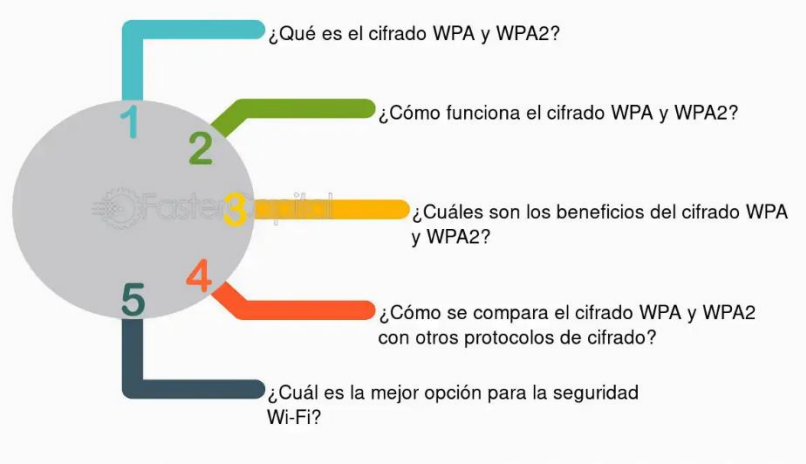
9.3.2. MEDIDAS DE SEGURIDAD EN REDES LAN

Para proteger una red LAN, se deben aplicar **medidas técnicas, organizativas y preventivas**. No hay una única solución, sino un conjunto de prácticas conocidas como **defensa en profundidad**.

Cifrado de las comunicaciones (WPA2/WPA3)

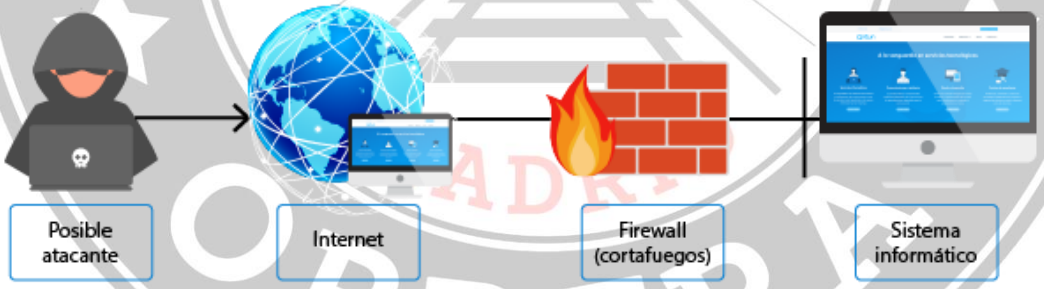
	WEP	WPA	WPA2	WPA3
Año salida	1997	2003	2004	2018
Cifrado	RC4	TKIP con RC4	AES-CCMP	AES-CCMP y AES-GCMP
Tamaño de clave	64 y 128 bits	128 bits	128 bits	128 y 256 bits
Tipo de cifrado	Flujo	Flujo	Bloque	Bloque
Autenticación	Sistema abierto y clave compartida	Clave precompartida (PSK) y 802.1x con variante EAP	Clave precompartida (PSK) y 802.1x con variante EAP	Simultaneous Authentication of Equals (SAE) y 802.x con variante EAP

- Especialmente relevante en redes Wi-Fi.
- **WPA2** (Wi-Fi Protected Access 2) es el mínimo exigido hoy en día; utiliza AES para cifrar los datos.
- **WPA3**, más moderno, mejora la resistencia a ataques por diccionario y protege mejor las redes abiertas (modo OWE).
- En redes cableadas, el cifrado puede aplicarse a través de **VPNs internas** o protocolos como **IPsec**.



Consejo técnico: Nunca usar WEP (inseguro) ni dejar redes Wi-Fi abiertas. WPA3 debe ser la opción por defecto.

Firewalls (cortafuegos)



- Filtran el tráfico que entra y sale de la red según reglas de seguridad.
- **Firewalls perimetrales**: integrados en el router o en dispositivos dedicados.
- **Firewalls host**: instalados en los dispositivos individuales (Windows Defender Firewall, por ejemplo).
- Permiten bloquear puertos, direcciones IP sospechosas o protocolos no autorizados.

Ejemplo: Bloquear el puerto 445 para evitar la propagación de malware como WannaCry.

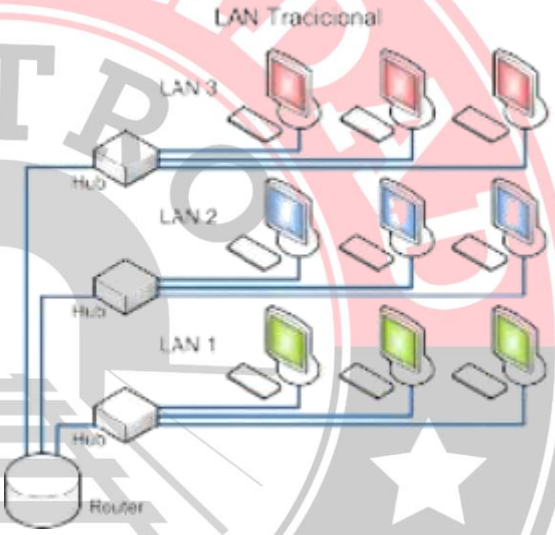
Autenticación robusta

- Se deben establecer mecanismos sólidos para verificar la identidad de los usuarios:
  - Contraseñas seguras (mínimo 12 caracteres, con mayúsculas, números y símbolos).
  - Políticas de caducidad y renovación periódica.
  - **MFA (Autenticación Multifactor)**: combinación de algo que sabes (contraseña), algo que tienes (token o app) y algo que eres (huella, rostro).
- Integración con **Active Directory** o servicios LDAP en entornos empresariales.

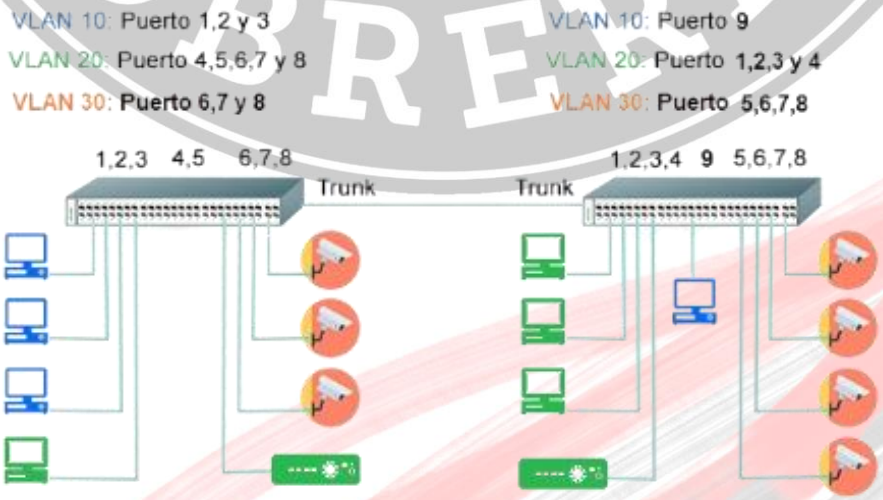
Ejemplo: Un técnico que accede al panel del router debe introducir una contraseña segura y un código temporal desde su móvil.

Segmentación de red (VLANs)

- Dividir la red física en **subredes lógicas (Virtual LANs)** para aislar tráfico según funciones, departamentos o dispositivos.
- Ejemplos comunes:
  - VLAN para administración.
  - VLAN para aulas de formación.
  - VLAN para invitados (acceso limitado a Internet).
- Mejora la seguridad y evita que un ataque afecte a toda la red.



Ejemplo: Si un equipo de alumnos queda infectado, el servidor del profesor permanece protegido en otra VLAN.



Otras medidas complementarias

- **Control de acceso físico** a salas de servidores y armarios de red.
- **Filtrado MAC**: permite el acceso solo a dispositivos autorizados por su dirección MAC.
- **IDS/IPS**:
  - **IDS (Intrusion Detection System)**: detecta comportamientos anómalos o ataques.
  - **IPS (Intrusion Prevention System)**: bloquea automáticamente el tráfico malicioso.
- **Actualización de firmware y software** de todos los dispositivos de red.
- **Copias de seguridad periódicas** (backup) de configuraciones de red y datos críticos.
- **Política de seguridad informática** documentada, conocida y firmada por los usuarios.

Buenas prácticas en seguridad LAN

Recomendación	Objetivo
Desactivar puertos de red no usados	Evitar accesos físicos no deseados
Cambiar credenciales por defecto	Prevenir accesos automáticos
Revisar logs de conexión periódicamente	Detectar intentos de intrusión
Usar antivirus/antimalware actualizados	Prevenir infecciones por software malicioso
Formación de usuarios	Reducir el riesgo de errores humanos

Ejemplo práctico aplicado

En una pequeña empresa con 15 empleados:

- Se implementa una red híbrida: cable para los PCs fijos, Wi-Fi para móviles.
- El router tiene WPA3 activo y contraseña compleja.
- Cada departamento tiene su VLAN configurada en el switch gestionable.
- Se usa un servidor NAS con acceso limitado por usuarios autenticados.
- El cortafuegos bloquea todo tráfico entrante, salvo reglas explícitas.
- Se realiza una copia de seguridad diaria automática en la nube.

9.4. MONITORIZACIÓN Y GESTIÓN DE REDES

La **monitorización de redes** es una actividad esencial en la administración de sistemas informáticos y redes locales. Consiste en la **supervisión constante del estado de los dispositivos, servicios y enlaces** de una red para detectar y anticipar fallos, así como para garantizar el correcto funcionamiento y optimizar el rendimiento global.

La **gestión de redes** complementa a la monitorización, ya que implica la **toma de decisiones basadas en los datos recogidos** para resolver problemas, mantener la seguridad y asegurar un rendimiento óptimo según los objetivos del entorno de trabajo.

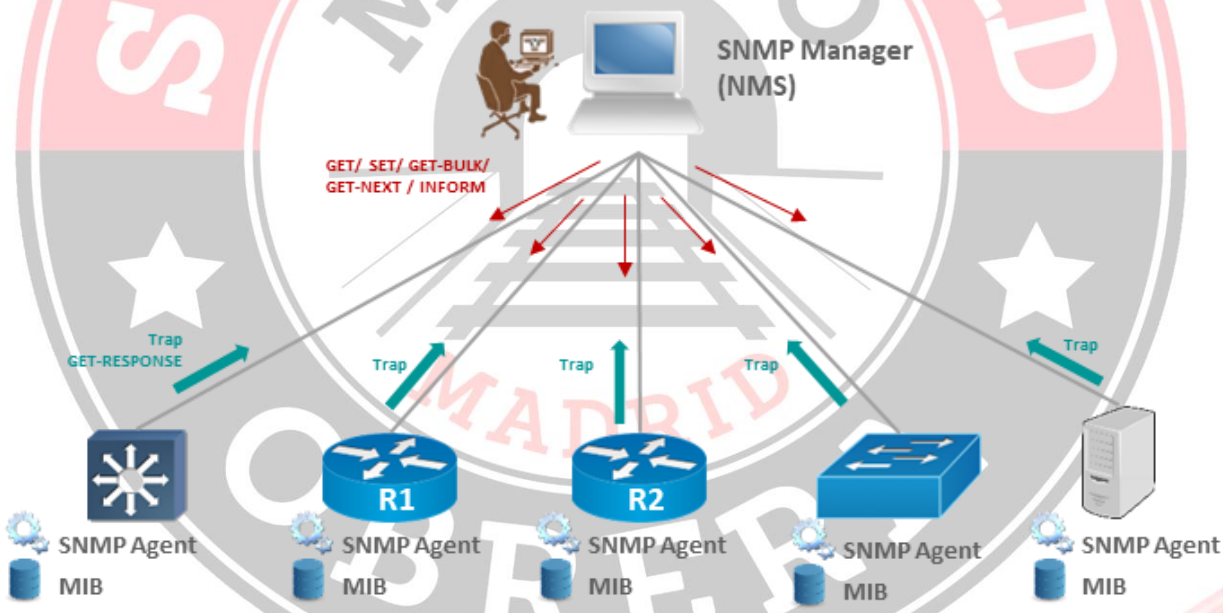
Los principales beneficios de una correcta monitorización y gestión son:

- **Detección temprana de incidencias o caídas de servicio**.
- **Optimización del uso de recursos**, como ancho de banda o capacidad de procesamiento.
- **Priorización del tráfico crítico** (por ejemplo, videollamadas, servicios en la nube).
- **Mejor planificación de ampliaciones** o mejoras en la red.
- **Reducción del tiempo de inactividad** y mejora de la experiencia del usuario.

9.4.1. HERRAMIENTAS DE MONITORIZACIÓN

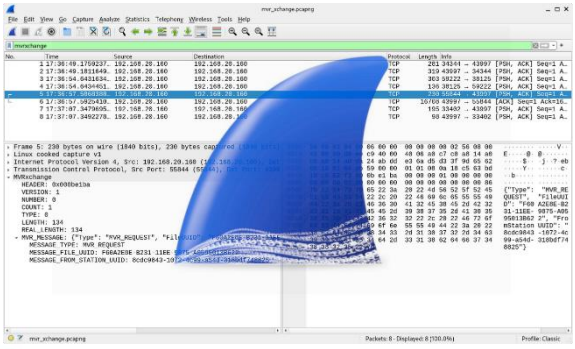
Existen múltiples herramientas para supervisar el estado de una red, que pueden ser desde simples comandos de diagnóstico hasta plataformas completas de gestión.

SNMP (Simple Network Management Protocol)



- Es un **protocolo estándar** utilizado para recoger y organizar información sobre dispositivos de red como **routers, switches, impresoras, servidores, etc.**
- Permite **consultar el estado de un dispositivo remotamente** (uso de CPU, tráfico, fallos, temperatura) y también modificar parámetros en algunos casos.
- Se basa en un modelo cliente-servidor: el **agente SNMP** se ejecuta en el dispositivo, y el **gestor SNMP** (una aplicación externa) recoge la información.

Wireshark



- Es un **analizador de protocolos de red** de código abierto.
- Permite **capturar en tiempo real todos los paquetes que pasan por una interfaz de red** y analizarlos detalladamente (direcciones IP, puertos, protocolos, contenido...).
- Se utiliza para:
  - **Diagnóstico de problemas de conectividad.**
  - **Detección de tráfico anómalo o malicioso.**
  - **Estudio del rendimiento de la red** a nivel de paquetes.
- Requiere conocimientos técnicos, ya que ofrece un nivel muy bajo de análisis (nivel de capa 2 a 7 del modelo OSI).

Nagios y Zabbix

- Son **plataformas de monitorización de infraestructuras IT**, muy completas y utilizadas en entornos empresariales.
- Permiten:
  - Monitorizar **disponibilidad, carga, tráfico, espacio en disco, estado de procesos y servicios.**
  - Enviar **alertas por correo, Telegram, SMS o paneles web** cuando se detecta un fallo o umbral crítico.
  - Crear **paneles gráficos y estadísticas históricas.**
- **Zabbix** destaca por su integración con bases de datos y visualización detallada.
- **Nagios** es más modular y permite integraciones mediante plugins.

Comandos básicos de diagnóstico

Estos comandos son herramientas esenciales para el análisis inicial de problemas en la red:

- ping: Comprueba si un host está activo y mide el tiempo de respuesta.
- netstat: Muestra conexiones activas, puertos abiertos y estadísticas de red.
- traceroute (o tracert en Windows): Muestra el recorrido de los paquetes hasta un destino, útil para detectar **saltos lentos o bloqueos**.
- nslookup: Realiza consultas DNS para verificar si los dominios están bien configurados y resuelven correctamente.

9.4.2. GESTIÓN DEL RENDIMIENTO

Además de supervisar la red, es fundamental **gestionar su rendimiento** para garantizar que los recursos se distribuyen eficientemente y que los servicios críticos tienen prioridad.

Calidad de servicio (QoS - Quality of Service)

- Es un conjunto de tecnologías que **prioriza determinados tipos de tráfico** sobre otros.
- Muy útil cuando hay **ancho de banda limitado**.
- Ejemplo: se puede configurar QoS para que el tráfico de **VoIP (voz por IP)** o videoconferencia tenga más prioridad que las descargas o la navegación web.
- Se gestiona mediante políticas en routers, switches y firewalls.

Análisis de cuellos de botella

- Consiste en **identificar puntos de congestión o saturación** en la red.
- Puede deberse a enlaces con poco ancho de banda, demasiados dispositivos conectados, errores de configuración, etc.
- Una vez detectados, se pueden aplicar soluciones como:
  - **Actualizar el hardware o enlaces.**
  - **Balancear la carga.**
  - **Optimizar el tráfico con QoS.**

Estado de los dispositivos de red

- La monitorización del hardware también es fundamental: si un switch está **sobrecalentado, con uso alto de CPU o errores de transmisión**, puede degradar el rendimiento.
- Herramientas como SNMP, Zabbix o interfaces web de los dispositivos permiten:
  - Verificar **temperaturas internas.**
  - Revisar **uso de memoria y CPU.**
  - Analizar **paquetes perdidos o errores de transmisión.**

9.5. VIRTUALIZACIÓN Y ALMACENAMIENTO EN REDES

En los entornos actuales, las infraestructuras de red no solo conectan dispositivos, sino que también proporcionan plataformas para ejecutar múltiples servicios y almacenar grandes cantidades de datos. En este contexto, dos tecnologías se han vuelto esenciales: la **virtualización** y el **almacenamiento en red**.

Estas tecnologías permiten:

- Mejor aprovechamiento del hardware.
- Reducción de costes y espacio físico.

- Mayor flexibilidad y escalabilidad.
- Acceso compartido y centralizado a los recursos.

9.5.1. VIRTUALIZACIÓN

La **virtualización** consiste en crear versiones virtuales de sistemas o recursos informáticos, como servidores, sistemas operativos, dispositivos de almacenamiento o incluso redes.

Gracias a la virtualización, un solo ordenador físico puede ejecutar **varias máquinas virtuales (VMs)** de manera simultánea, cada una con su propio sistema operativo, recursos asignados y configuración.

Máquinas virtuales (VMs)

- Una máquina virtual es un **entorno informático aislado** que simula un ordenador físico completo.
- Cada VM dispone de su propio sistema operativo, memoria, CPU, almacenamiento y conexiones de red virtualizadas.
- Se gestionan desde un **hipervisor** y pueden crearse, copiarse, migrarse y eliminarse fácilmente.

Ventajas de usar VMs:

- **Ahorro de hardware:** se ejecutan múltiples sistemas en un solo servidor físico.
- **Facilidad de prueba:** ideal para entornos de desarrollo y pruebas.
- **Mayor seguridad:** al aislar sistemas entre sí.
- **Portabilidad:** se pueden mover entre servidores o centros de datos.

Hypervisores

El **hipervisor** es el software que permite crear y gestionar máquinas virtuales. Existen dos tipos:

Tipo 1 (bare-metal)

- Se instalan **directamente sobre el hardware** físico, sin necesidad de un sistema operativo previo.
- Ofrecen mayor **rendimiento, fiabilidad y seguridad**.

- Son los más utilizados en **entornos profesionales o empresariales**.

Ejemplos:

- VMware ESXi
- Microsoft Hyper-V (modo servidor)
- XenServer

Tipo 2 (hosted)

- Funcionan sobre un **sistema operativo ya instalado** (como Windows o Linux).
- Son más fáciles de usar, pero **menos eficientes** en rendimiento.
- Ideales para **uso personal, educativo o pruebas**.

Ejemplos:

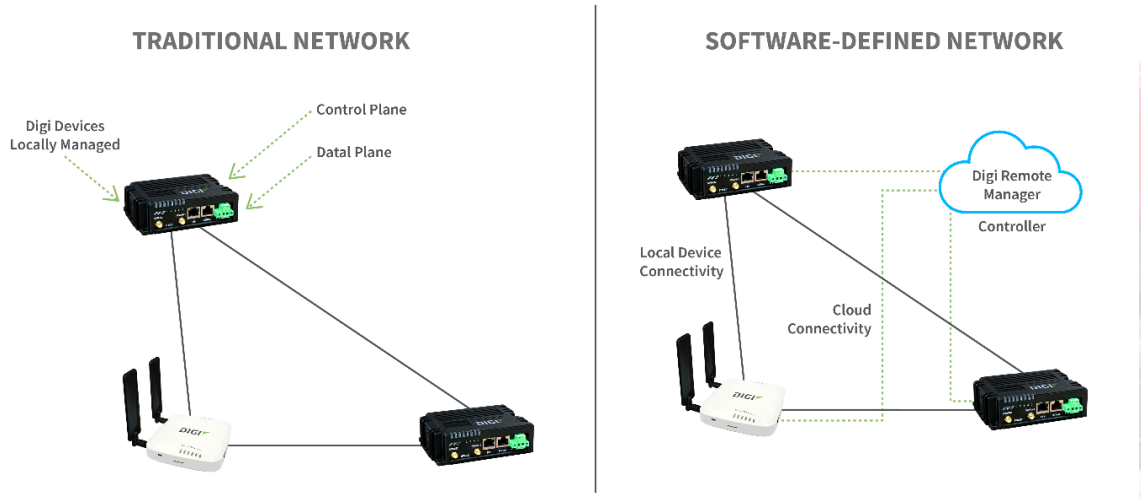
- Oracle VirtualBox
- VMware Workstation
- Parallels Desktop (macOS)

Redes Definidas por Software (SDN)

Las **SDN (Software Defined Networking)** son una evolución de la virtualización aplicada a las redes. En lugar de configurar físicamente los dispositivos de red (routers, switches), se controla todo mediante **software centralizado**.

Características:

- Separa el **plano de control** (decisiones de enrutamiento) del **plano de datos** (movimiento real de los paquetes).
- Se gestiona desde un **controlador central** que administra toda la red de forma automatizada y programable.



Ventajas:

- Mayor **flexibilidad** para modificar la red sin necesidad de reconfigurar equipos físicos.
- Facilita la **automatización**, segmentación y ajuste dinámico del tráfico.
- Escalable para grandes centros de datos o redes virtualizadas.

Ejemplo de uso: Data centers que alojan servicios en la nube, donde se crean y eliminan redes virtuales según demanda.

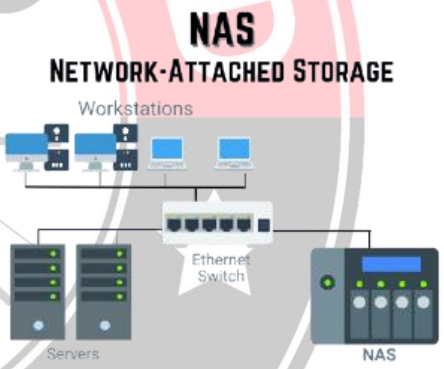
9.5.2. ALMACENAMIENTO EN RED

El almacenamiento en red permite que **múltiples usuarios y dispositivos accedan y compartan archivos** desde un punto centralizado, eliminando la necesidad de copiar datos en cada equipo.

Existen tres formas principales de almacenamiento en red:

NAS (Network Attached Storage)

- Es un **dispositivo de almacenamiento conectado a la red local**, que actúa como un **servidor de archivos**.
- Utiliza **protocolos de red** como SMB/CIFS (Windows), NFS (Linux/Unix) o FTP para compartir carpetas o archivos.
- Suele incluir múltiples discos duros configurados en **RAID** para ofrecer redundancia y protección de datos.



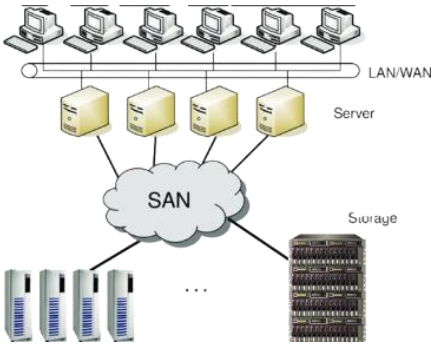
Ventajas:

- Fácil de instalar y administrar.
- Accesible desde cualquier equipo conectado a la red.
- Ideal para hogares, pequeñas oficinas o centros educativos.

Ejemplos de uso:

- Copias de seguridad automáticas.
- Servidor multimedia doméstico.
- Almacenamiento compartido para un equipo de trabajo.

SAN (Storage Area Network)



- Es una **red de alta velocidad dedicada exclusivamente al almacenamiento**, que conecta servidores con dispositivos de almacenamiento a nivel de bloque (no de archivo).
- Utiliza tecnologías como **Fibre Channel o iSCSI** para lograr transferencias muy rápidas y fiables.

Características:

- Muy utilizada en **entornos corporativos o centros de datos** donde se requiere **alta disponibilidad y rendimiento**.
- Puede escalar fácilmente para añadir más capacidad o velocidad.

Diferencia con NAS: Mientras que NAS se gestiona a nivel de archivos, SAN trabaja a nivel de bloques, como si los discos duros estuvieran conectados directamente al servidor.

Almacenamiento en la nube

Consiste en utilizar **recursos de almacenamiento ubicados en Internet**, proporcionados por empresas especializadas (proveedores de servicios en la nube).

Ventajas:

- Acceso remoto desde cualquier dispositivo con conexión.
- Escalabilidad instantánea.
- Alta disponibilidad y copias de seguridad automáticas.
- Evita inversión en hardware físico.

Tipos de uso:

<u>Personales:</u>

- Google Drive, Dropbox, OneDrive.
- Permiten sincronizar documentos, fotos y vídeos entre dispositivos.

<u>Empresa:</u>

- Amazon S3, Microsoft Azure Storage, Google Cloud Storage.
- Diseñados para aplicaciones web, backup masivo, big data, etc.
- Integración con APIs y control de permisos avanzados.

10. SISTEMAS OPERATIVOS EN RED

10.1. INTRODUCCIÓN A LOS SISTEMAS OPERATIVOS EN RED

Concepto general Un sistema operativo en red (SOR) es un tipo de software de base diseñado para permitir la interconexión, coordinación y control de múltiples dispositivos dentro de una infraestructura informática. Su función principal es proporcionar un entorno común donde los recursos, como archivos, impresoras o bases de datos, puedan ser compartidos y gestionados de manera eficiente y segura entre múltiples usuarios y dispositivos conectados a través de una red.

Los SOR facilitan la cooperación entre equipos y usuarios que se encuentran en diferentes ubicaciones físicas, permitiendo el trabajo colaborativo, la centralización de servicios y el acceso remoto. Estos sistemas operativos están diseñados para funcionar como parte integral de una arquitectura distribuida, donde los recursos están disponibles bajo demanda, gestionados por políticas de red y con soporte para una amplia gama de servicios de red.

Además de sus funciones básicas, los SOR actúan como plataforma para ejecutar aplicaciones de red, bases de datos, entornos de desarrollo, servicios web y sistemas de comunicación, convirtiéndose en una pieza clave dentro de cualquier sistema informático profesional, educativo o industrial.

Evolución histórica y contexto El concepto de sistema operativo en red surgió con la necesidad de interconectar equipos en entornos empresariales. Inicialmente, las redes eran cerradas y locales (LAN), y los sistemas operativos como UNIX comenzaron a ofrecer servicios de red rudimentarios en los años 70 y 80. Con el desarrollo de protocolos de comunicación estandarizados como TCP/IP y la aparición de Internet, surgieron versiones de sistemas operativos especialmente diseñadas para gestionar entornos conectados.

En los años 90, con la masificación del uso de computadoras personales y servidores, sistemas como Windows NT y Linux comenzaron a incorporar de manera nativa servicios de red, permitiendo un despliegue más ágil de entornos colaborativos. Hoy en día, los SOR no solo se limitan al ámbito empresarial, sino que se han expandido a entornos domésticos, móviles y embebidos, gracias a la conectividad ubicua y la computación en la nube.

10.1.1. APLICACIONES DE LOS SOR:

Los sistemas operativos en red tienen una amplia variedad de aplicaciones en distintos entornos:

- **Empresas y oficinas**: Donde es necesario que varios empleados trabajen simultáneamente con archivos compartidos, bases de datos comunes o sistemas ERP.
- **Centros de datos y servidores**: Como base para ofrecer servicios como alojamiento web, correo electrónico, acceso remoto o almacenamiento en la nube.
- **Centros educativos**: Para la gestión de aulas de informática, control de accesos, distribución de software y supervisión de actividades.
- **Entornos industriales**: Para supervisar, controlar y automatizar procesos de producción mediante sistemas conectados en red.
- **Redes domésticas avanzadas**: Donde se integran sistemas multimedia, almacenamiento compartido (NAS), y dispositivos inteligentes.

10.1.2. CARACTERÍSTICAS PRINCIPALES

- **Gestión centralizada**: Un administrador puede controlar usuarios, permisos, dispositivos, servicios y recursos desde un único punto, normalmente un servidor o consola de administración.
- **Soporte multiusuario**: Permite que múltiples personas accedan de manera simultánea a recursos comunes, cada una con su perfil y permisos.
- **Conectividad y protocolos estándar**: Implementan protocolos de red como TCP/IP, SMB (Server Message Block), FTP, LDAP y NFS para la interoperabilidad.
- **Seguridad y control de accesos**: Integran sistemas de autenticación, cifrado, control de sesiones y registro de eventos para proteger los datos y evitar accesos no autorizados.
- **Escalabilidad**: Pueden crecer fácilmente añadiendo nuevos usuarios, dispositivos o servicios sin afectar al rendimiento general.
- **Redundancia y alta disponibilidad**: Incluyen funciones como balanceo de carga, replicación y tolerancia a fallos para asegurar la continuidad del servicio.
- **Diversidad de servicios integrados**: Ofrecen funciones esenciales como servidores de archivos, impresión, correo electrónico, bases de datos, acceso remoto, servicios web, DNS, DHCP, etc.
- **Interoperabilidad**: Compatibilidad entre diferentes sistemas operativos (Windows, Linux, macOS) gracias a estándares y protocolos universales.
- **Automatización y gestión remota**: Integración con herramientas para la automatización de tareas administrativas y el monitoreo de rendimiento.

10.1.3. TIPOS DE SISTEMAS OPERATIVOS EN RED

Los sistemas operativos en red pueden clasificarse en función del rol que desempeñan en la infraestructura informática, el tipo de dispositivo donde se instalan y las características de administración que ofrecen. A continuación, se detallan los principales tipos:

SISTEMAS OPERATIVOS DE SERVIDOR:

Están diseñados para gestionar múltiples servicios de red, ofrecer alta disponibilidad y manejar grandes volúmenes de usuarios y datos. Están optimizados para tareas de rendimiento, virtualización y seguridad.

WINDOWS SERVER

Windows Server es una de las plataformas más utilizadas a nivel empresarial para la gestión de redes, usuarios y servicios. Se integra de forma nativa con el ecosistema de Microsoft, lo que lo convierte en la opción preferida en entornos con estaciones de trabajo Windows.

Características principales:

- Interfaz gráfica y herramientas de administración remota intuitivas.
- Gran compatibilidad con software empresarial y soluciones de terceros.
- Estabilidad, escalabilidad y soporte oficial prolongado.

Servicios y funcionalidades destacadas:

- **Active Directory Domain Services (AD DS):** Permite la administración centralizada de usuarios, equipos y recursos, así como la aplicación de políticas de grupo.
- **DNS y DHCP integrados:** Facilitan la configuración automática de red y la resolución de nombres.
- **Hyper-V:** Plataforma de virtualización nativa, que permite gestionar múltiples máquinas virtuales.
- **IIS (Internet Information Services):** Servidor web nativo para aplicaciones ASP.NET, sitios HTML, y servicios REST.
- **WSUS:** Gestión centralizada de actualizaciones para todos los equipos de la red.
- **Failover Clustering y Storage Spaces Direct:** Soluciones de alta disponibilidad.
- **Compatibilidad con Azure y servicios híbridos en la nube.**

Versiones comunes: Essentials (Pymes), Standard (entornos medianos), Datacenter (virtualización masiva y grandes organizaciones).

LINUX SERVER

Linux es un sistema operativo de código abierto, robusto, seguro y flexible. Se utiliza ampliamente en servidores web, bases de datos, entornos de desarrollo y centros de datos. Existen numerosas distribuciones adaptadas a distintos fines.

Distribuciones más comunes:

- **Ubuntu Server:** Fácil de usar, ideal para principiantes y entornos DevOps.
- **Debian:** Estable, altamente seguro y con gran soporte comunitario.
- **CentOS / AlmaLinux / Rocky Linux:** Alternativas a Red Hat Enterprise Linux, pensadas para entornos de producción.
- **Red Hat Enterprise Linux (RHEL):** Versión comercial con soporte profesional.

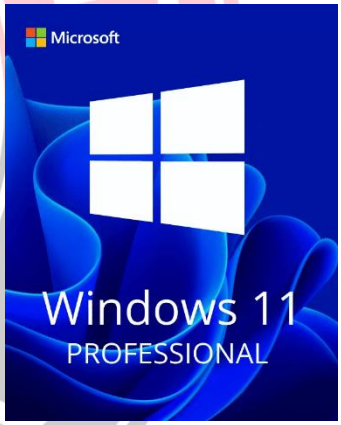
Ventajas de Linux Server:

- Configuración personalizable desde la línea de comandos.
- Uso eficiente de recursos, ideal para entornos con hardware limitado.
- Soporte nativo para protocolos de red estándar como SSH, FTP, HTTP, NFS, SMB.
- Seguridad reforzada mediante SELinux, iptables/nftables y AppArmor.
- Amplia disponibilidad de herramientas de automatización (Ansible, Bash, cron).

Ámbitos de aplicación: Hosting web (Apache, Nginx), bases de datos (MySQL, PostgreSQL), servidores de archivos (Samba), DNS (Bind), correo electrónico (Postfix, Dovecot), VPN, entre otros.

SISTEMAS OPERATIVOS DE CLIENTE

Los sistemas operativos cliente permiten a los usuarios conectarse a una red y utilizar servicios y recursos compartidos proporcionados por servidores. Son más comunes en estaciones de trabajo, aulas y oficinas.



1. WINDOWS 10/11 PROFESSIONAL Y ENTERPRISE:

- Pueden unirse a un dominio de Active Directory.
- Soportan directivas de grupo, escritorios remotos y BitLocker.
- Muy utilizados en entornos empresariales.

2. LINUX (UBUNTU, FEDORA, MINT):

- Usados en formación técnica, administración pública y entornos con software libre.
- Compatibles con Samba para compartir archivos y unirse a redes Windows.

3. macOS:

- Integrado en redes gracias a su compatibilidad con SMB, AFP, y LDAP.
- Ampliamente usado en entornos creativos, diseño y educación.

Los sistemas cliente dependen de servidores para funciones críticas como autenticación, almacenamiento centralizado y acceso a servicios de red.

SISTEMAS OPERATIVOS ESPECIALIZADOS

Estos sistemas están diseñados para cumplir funciones muy concretas dentro de la red. Son ligeros, eficientes y altamente configurables.

1. FreeNAS / TrueNAS:

- Soluciones NAS (Network Attached Storage) basadas en FreeBSD.
- Gestionan volúmenes de datos, RAID, snapshots y replicación.

2. RouterOS (MikroTik):

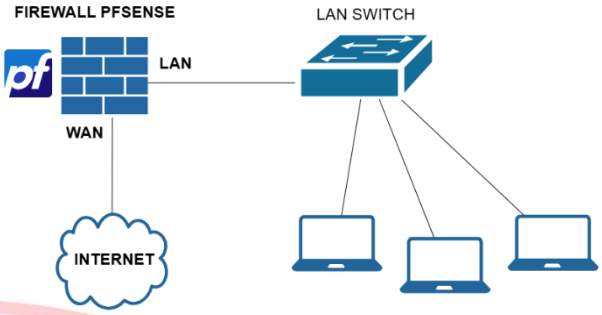
- Sistema basado en Linux para routers.
- Administra interfaces de red, firewall, balanceo de carga y VPN.

3. OpenWRT:

- Firmware de código abierto para routers domésticos y profesionales.
- Permite configuraciones avanzadas de red y uso de paquetes personalizados.

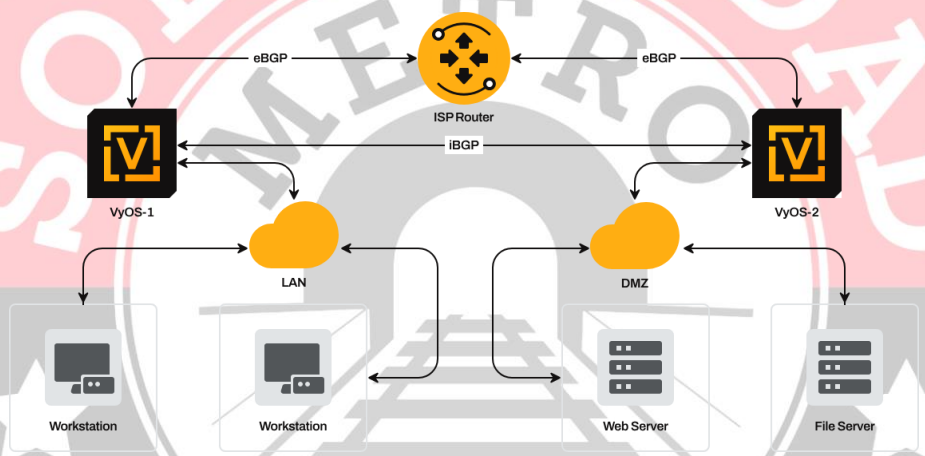
4. pfSense:

- Firewall y router avanzado basado en FreeBSD.
- Muy utilizado en seguridad perimetral, filtrado de contenido y redes empresariales.



5. VyOS:

- Sistema operativo para routers empresariales.
- Soporta BGP, OSPF, VPNs, NAT y otras funciones avanzadas de red.



Estos sistemas son ideales para redes que requieren servicios específicos, como seguridad, enrutamiento, almacenamiento centralizado o acceso remoto.

Comparativa general:

- Los **servidores** priorizan estabilidad, rendimiento y administración remota.
- Los **clientes** priorizan usabilidad, compatibilidad y rendimiento gráfico.
- Los **especializados** están centrados en tareas críticas o específicas como almacenamiento, routing o seguridad.

Seleccionar el tipo de sistema operativo en red adecuado depende del contexto de uso, la infraestructura existente, las necesidades de seguridad y el presupuesto disponible. En entornos mixtos, es habitual la convivencia de varios tipos de sistemas operativos en red funcionando de forma integrada.

10.1.4. VENTAJAS Y DESVENTAJAS

Ventajas:

- Mayor control y administración centralizada.
- Compartición eficiente de recursos.
- Mejora de la productividad y la colaboración.
- Seguridad avanzada y protección de datos.
- Escalabilidad y flexibilidad.

Desventajas:

- Mayor complejidad en la instalación y configuración.
- Necesidad de personal técnico capacitado.
- Requiere infraestructura y mantenimiento continuo.
- Costes asociados en algunas soluciones propietarias.

Esta variedad permite que cada entorno profesional o educativo pueda seleccionar el sistema operativo en red más adecuado a sus necesidades, equilibrio entre costes, seguridad, facilidad de uso y soporte técnico.

10.2. INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS OPERATIVOS EN SERVIDORES

La instalación y configuración de un sistema operativo en red representa uno de los procesos más críticos en la administración de entornos informáticos. A través de esta fase se establece la base sobre la cual funcionarán los distintos servicios de red, la seguridad de los sistemas, la gestión de usuarios y la eficiencia operativa.

10.2.1. REQUISITOS PREVIOS A LA INSTALACIÓN

1. Compatibilidad del hardware: Antes de realizar la instalación, es necesario asegurarse de que el servidor cumple con los requisitos técnicos del sistema operativo seleccionado. Entre los aspectos a verificar se encuentran:

- **Procesador (CPU):** Debe contar con arquitectura compatible (x64, ARM, etc.) y velocidad adecuada.
- **Memoria RAM:** Se recomienda un mínimo de 4 GB para servidores básicos, aunque para tareas como virtualización o bases de datos se requieren 16 GB o más.
- **Disco duro/almacenamiento:** Espacio suficiente para sistema operativo, logs, servicios y archivos. Discos SSD mejoran el rendimiento.
- **Placa base y chipset:** Deben estar soportados oficialmente.

- **Interfaces de red:** Al menos una tarjeta de red compatible (idealmente más de una para redundancia o segmentación de redes).
- **Compatibilidad con tecnologías de virtualización:** Si se utilizarán máquinas virtuales, es necesario habilitar funciones como VT-x o AMD-V desde la BIOS/UEFI.

2. Planificación de la red: Antes de instalar, hay que definir cómo se integrará el servidor en la red:

- **Topología de red:** Estrella, bus, árbol, etc.
- **Direcciones IP:** Reservar IPs estáticas para servidores. Definir subredes y planificación de direccionamiento.
- **Nombres de host y dominio:** Nombrar de forma coherente para facilitar la gestión.
- **Servicios de red asociados:** DNS, DHCP, servidores de archivos, proxy, etc.
- **Requisitos de acceso remoto:** VPN, SSH, RDP.
- **Segmentación de red (VLAN):** Útil en entornos con múltiples servicios o departamentos.

3. Configuración del almacenamiento:

- **Tipo de almacenamiento:** HDD, SSD, almacenamiento en red (NAS, SAN).
- **Particionamiento de discos:** Definir estructura de particiones (/, /home, /var, etc. en Linux o C:, D: en Windows).
- **Sistemas de archivos:** NTFS, ReFS (Windows); ext4, Btrfs, XFS (Linux).
- **RAID:** Para redundancia y rendimiento (RAID 1 para espejo, RAID 5 para paridad, RAID 10 para alto rendimiento).
- **Backups y snapshots:** Planificación de respaldo desde el inicio.

10.2.2. PROCESO DE INSTALACIÓN

El proceso varía dependiendo del sistema operativo, pero sigue una estructura común.

1. Selección del sistema operativo: Debe hacerse en función del entorno y requisitos:

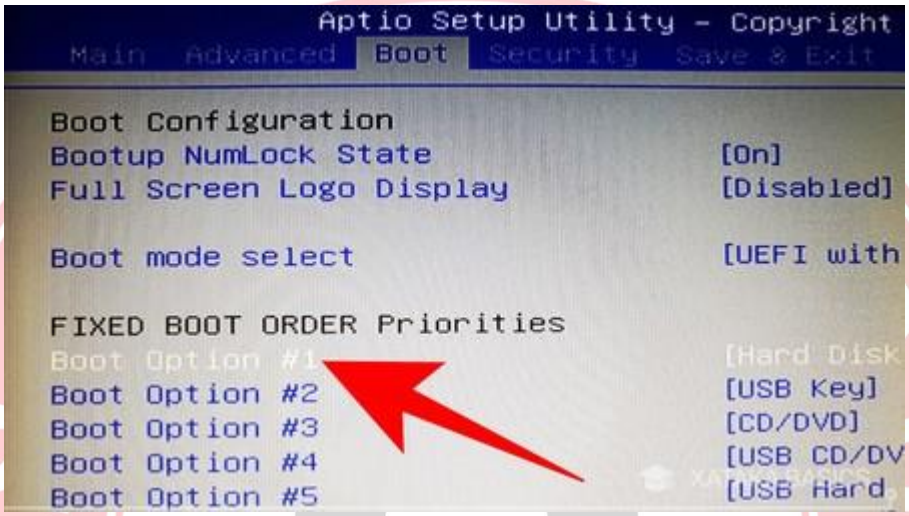
- **Windows Server:** Buena compatibilidad, GUI amigable, ideal para entornos Microsoft.
- **Linux Server (Ubuntu, Debian, CentOS, AlmaLinux):** Libre, estable, muy usado en servidores web.
- **Distribuciones especializadas:** FreeNAS para almacenamiento, pfSense para cortafuegos.

2. Preparación del medio de instalación:

- Crear un USB de arranque con herramientas como Rufus o Etcher.
- Grabar en DVD o utilizar imágenes ISO en servidores virtuales.
- Preparar instalación desatendida (Windows Answer File, Kickstart para Linux).
- Usar PXE para despliegues masivos por red.

3. Configuración de BIOS/UEFI:

- Prioridad de arranque.
- Activación de virtualización.
- Configuración de Secure Boot y Fast Boot.



4. Instalación básica del sistema operativo:

- Elegir el idioma, zona horaria, teclado.
- Crear particiones según lo planificado.
- Asignar contraseña al usuario administrador (root o Administrator).

5. Configuración inicial de red:

- Asignación de IP estática o configuración DHCP.
- Nombre del equipo y grupo de trabajo o dominio.
- Configuración de DNS, gateway y hostname.
- Comprobación de conectividad básica (ping, nslookup).

6. Instalación de controladores y actualizaciones:

- En Windows: Windows Update, herramientas del fabricante.
- En Linux: apt install, dnf update, modprobe, etc.
- Verificar compatibilidad con dispositivos como tarjetas gráficas o RAID.

7. Instalación de servicios esenciales: Según el rol del servidor:

- Web: Apache, Nginx, IIS.
- Base de datos: MySQL, PostgreSQL, MariaDB.

- FTP/SFTP: vsftpd, FileZilla Server.
- Administración remota: SSH, RDP.
- Compartición de archivos: Samba, NFS.
- Monitoreo: Nagios, Zabbix, Prometheus.
- Backups: Rsync, Bacula, Veeam.

8. Configuración de seguridad básica:

- Cambiar puertos por defecto si es posible.
- Activar cortafuegos (UFW, FirewallD, Windows Defender).
- Deshabilitar servicios innecesarios.
- Activar auditoría de eventos.

10.2.3. ADMINISTRACIÓN DE USUARIOS Y PERMISOS

1. Creación y gestión de cuentas:

- **Windows Server:** Uso de Active Directory para control centralizado.
  - Consolas: Usuarios y Equipos de AD, GPMC para políticas.
- **Linux:** Gestión mediante terminal o herramientas como Webmin.
  - Comandos: *useradd*, *usermod*, *passwd*, *groupadd*, *deluser*.

2. Estructura de grupos y permisos:

- **Modelo UGO:** Permisos para usuario, grupo y otros (rwx).
- **ACLs:** Permiten definir permisos más finos sobre archivos o carpetas.
- **Windows:** Permisos NTFS, herencia de permisos, permisos explícitos vs. efectivos.

3. Autenticación y cifrado:

- **MFA:** Tokens físicos, apps móviles (Google Authenticator, Microsoft Authenticator).
- **Hash de contraseñas:** SHA-256, bcrypt, Argon2.
- **Cifrado de disco completo:** BitLocker, LUKS.
- **Cifrado en tránsito:** SSH, HTTPS, VPN.

4. Políticas y buenas prácticas:

- Contraseñas con caducidad y complejidad.
- Bloqueo de cuenta tras intentos fallidos.
- Desactivación de cuentas inactivas.
- Registro y monitorización de accesos (logs del sistema).
- Auditoría de privilegios y revisión periódica.

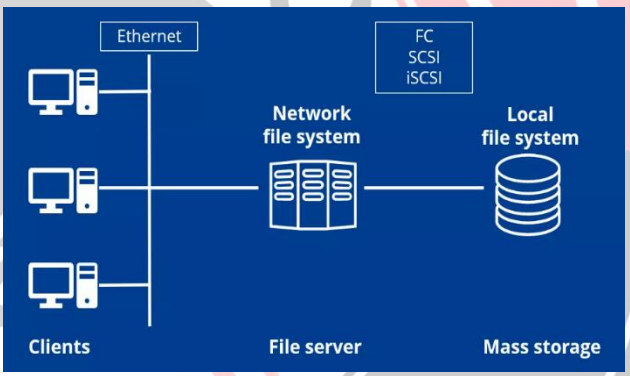
10.3. SERVICIOS Y ROLES EN UN SISTEMA OPERATIVO EN RED

Los servicios y roles de un sistema operativo en red permiten que el servidor desempeñe funciones específicas dentro de una infraestructura informática. Estos servicios facilitan la compartición de recursos, la administración centralizada, la seguridad, el trabajo colaborativo y la escalabilidad del sistema. Una adecuada planificación, instalación y configuración de estos servicios asegura el correcto funcionamiento de las redes locales y de área extensa (LAN y WAN).

10.3.1. SERVICIOS COMUNES EN SERVIDORES DE RED

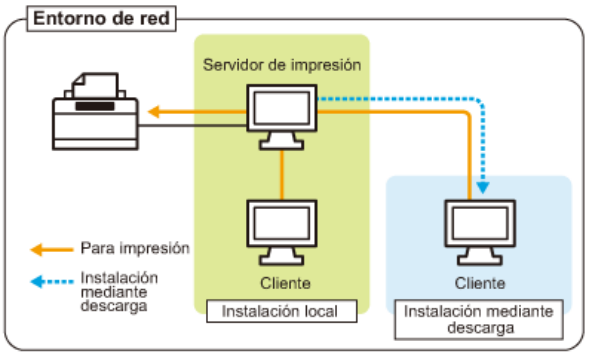
1. Servidor de archivos:

- Permite a los usuarios almacenar, acceder y compartir archivos desde cualquier dispositivo conectado a la red.
- Soporta control de versiones, auditoría de accesos, sincronización de carpetas y recuperación ante eliminaciones accidentales.
- Las cuotas de disco pueden establecer límites por usuario o grupo para evitar el uso excesivo de espacio.
- Es común en entornos corporativos, centros educativos y servidores domésticos.
- En redes Windows, se configura mediante el rol de "File and Storage Services" y se puede integrar con DFS para replicación geográfica.



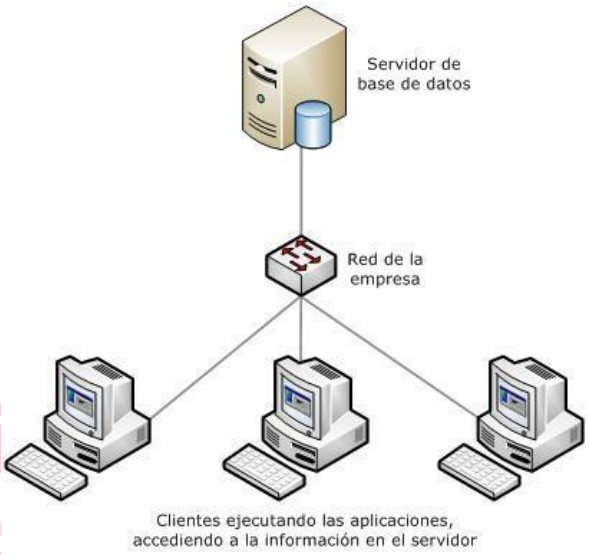
2. Servidor de impresión:

- Permite compartir impresoras en red, reducir costes y mejorar la eficiencia.
- Gestiona colas de impresión, control de acceso por usuarios o departamentos y administración remota.
- Puede generar informes de uso y establecer políticas como impresión a doble cara por defecto.
- Su integración con Active Directory facilita la asignación de impresoras según ubicación o pertenencia a grupos.



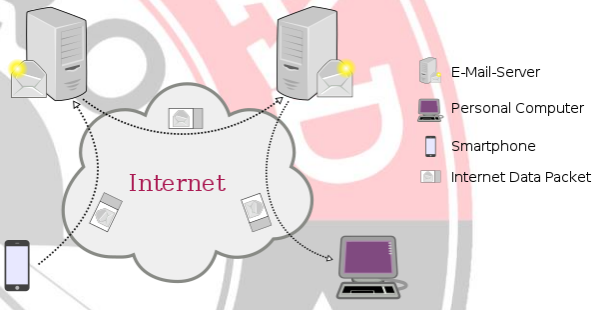
3. Servidor de bases de datos:

- Almacena y administra datos estructurados accesibles por múltiples usuarios y aplicaciones.
- Soporta operaciones concurrentes, transacciones seguras, replicación y respaldo.
- Puede estar alojado en un servidor dedicado o en una máquina virtual dentro de un clúster de alta disponibilidad.
- Configuraciones comunes incluyen bases relacionales (SQL Server, MySQL) y no relacionales (MongoDB).



4. Servidor de correo:

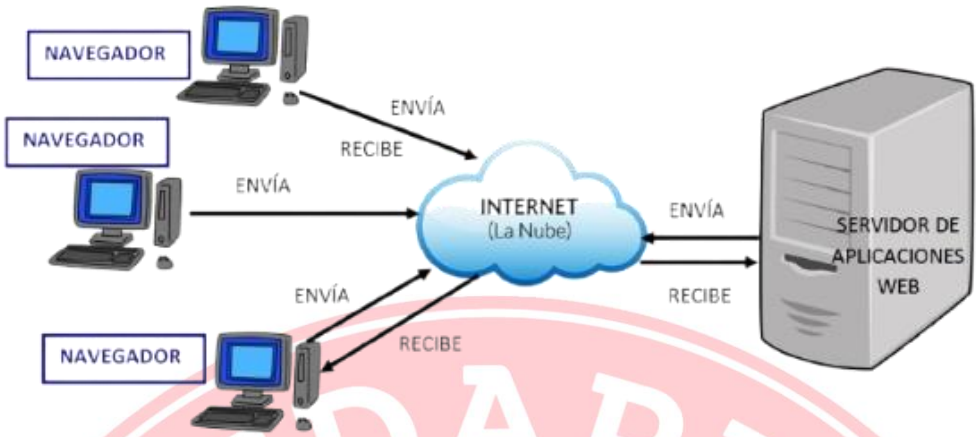
- Proporciona servicios de mensajería electrónica interna y externa.
- Puede incluir buzones de correo, agendas compartidas, contactos globales y acceso desde dispositivos móviles.
- Incluye filtros de spam, antivirus, cifrado de mensajes (S/MIME, TLS), y archivo automático.
- En Windows, Microsoft Exchange es ampliamente utilizado en entornos empresariales.
- En Linux, Postfix y Dovecot permiten construir soluciones completas con Webmail.



5. Servidor web:

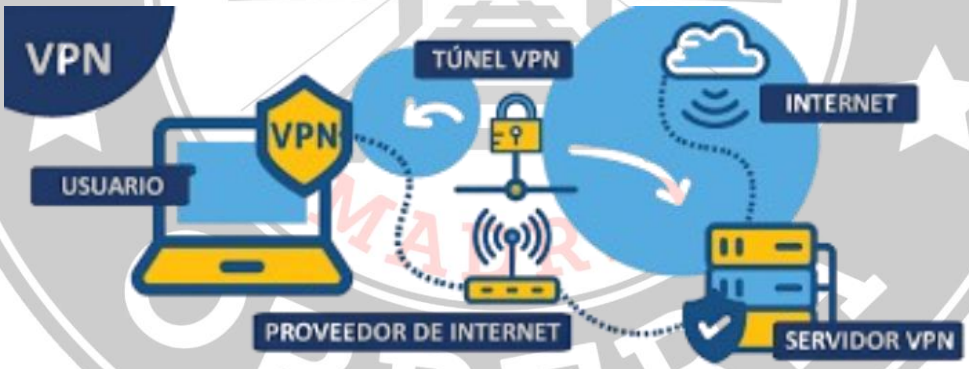
- Publica y aloja sitios web, aplicaciones web y APIs.
- Soporta contenido estático (HTML, CSS, JS) y dinámico (PHP, Python, Ruby, ASP.NET).
- Permite la instalación de CMS como WordPress, Joomla o Drupal.
- Incluye opciones de virtual hosting para alojar múltiples sitios en el mismo servidor físico o virtual.

- Implementa seguridad mediante certificados SSL/TLS, políticas CORS y cabezeras de seguridad HTTP.



6. Servidor VPN:

- Establece una red privada sobre una red pública mediante túneles cifrados.
- Garantiza la confidencialidad, integridad y autenticación de los datos.
- Es esencial para el acceso remoto seguro a la red corporativa, permitiendo el teletrabajo.
- Soporta múltiples protocolos: PPTP (obsoleto), L2TP/IPSec, OpenVPN, WireGuard.
- La configuración incluye certificados, claves precompartidas, túneles divididos o completos y control de acceso basado en políticas.



10.3.2. CONFIGURACIÓN DE ROLES EN SERVIDORES

1. Controlador de dominio:

- Centraliza la autenticación, autorización y control de políticas dentro de un entorno Windows.
- Implementa Active Directory, con objetos como usuarios, grupos, equipos, impresoras y unidades organizativas (OUs).
- Las políticas de grupo (GPO) permiten definir configuraciones comunes: contraseñas, escritorio, red, seguridad.

- Puede estar acompañado de servicios complementarios como DNS, DHCP y servidor de certificados (CA).
- En infraestructuras redundantes se implementan controladores adicionales para alta disponibilidad.

2. Servidor proxy:

- Media entre los dispositivos cliente y los recursos externos (Internet).
- Permite establecer políticas de navegación: bloqueo de sitios, programación horaria de acceso, reglas por usuario o grupo.
- Almacena en caché contenido web para reducir el ancho de banda y mejorar la velocidad.
- Puede actuar como proxy directo (transparente) o con autenticación (restringido).
- Algunas soluciones incluyen filtrado de contenido, control parental, y protección frente a malware (ej. Squid + ClamAV).

3. Servidor de almacenamiento:

- Administra grandes volúmenes de datos, respaldos y recursos compartidos.
- Integra protocolos como SMB/CIFS, NFS, iSCSI o WebDAV para compatibilidad con múltiples sistemas operativos.
- Permite configurar volúmenes compartidos, snapshots automáticos y replicación entre servidores.
- Muchas soluciones permiten el acceso vía navegador, autenticación por LDAP y cifrado en reposo.
- Sistemas como FreeNAS/TrueNAS ofrecen una interfaz web intuitiva para la gestión.

4. Servidor de virtualización:

- Centraliza la ejecución de múltiples sistemas operativos (máquinas virtuales) sobre un solo hardware físico.
- Cada máquina virtual puede actuar como servidor independiente (web, correo, bases de datos).
- Permite la creación de entornos aislados para pruebas, desarrollo y despliegue seguro de aplicaciones.
- Funciones avanzadas: snapshots, migración en caliente (vMotion), balanceo dinámico de carga (DRS), almacenamiento compartido (vSAN).
- Ejemplos:
    - **VMware ESXi**: solución comercial muy robusta.
    - **Microsoft Hyper-V**: integrado en Windows Server.
    - **KVM + Proxmox**: opción de código abierto y alto rendimiento.

Una infraestructura profesional puede contar con servidores especializados o combinaciones híbridas (por ejemplo, virtualización + almacenamiento + VPN en el mismo equipo). La definición clara de roles optimiza recursos, facilita el mantenimiento y mejora la seguridad de la red.

10.4. SEGURIDAD Y BACKUP EN SISTEMAS OPERATIVOS EN RED

La seguridad y las copias de seguridad son pilares fundamentales en la administración de sistemas operativos en red. Un sistema mal protegido o sin mecanismos de respaldo está expuesto a pérdidas de información, accesos no autorizados, interrupciones del servicio y ataques informáticos. Este apartado aborda las principales estrategias de protección y continuidad de servicio en entornos de red.

10.4.1. ESTRATEGIAS DE SEGURIDAD

1. Firewalls:

- Actúan como una barrera entre redes confiables (interna) y no confiables (externa), filtrando el tráfico entrante y saliente.
- Pueden ser **firewalls por hardware** (como los de Cisco, Fortinet) o **por software** (iptables, firewalld en Linux, Windows Defender Firewall).
- Permiten definir reglas basadas en:
  - Dirección IP origen/destino.
  - Puerto de origen/destino (TCP/UDP).
  - Aplicación o servicio.
- Suelen trabajar con políticas de listas blancas (permitir explícitamente) y negras (bloquear).
- Los firewalls avanzados incluyen funcionalidades como detección de intrusiones (IDS/IPS), inspección profunda de paquetes (DPI) y segmentación de red.

2. Autenticación segura:

- La autenticación garantiza que el acceso a los recursos se otorga solo a usuarios autorizados.
- Se aplican métodos tradicionales (usuario + contraseña) y métodos avanzados:
  - **Autenticación multifactor (MFA):** Combinación de algo que se sabe (contraseña), algo que se tiene (token físico o app) y algo que se es (biometría).
  - **Protocolos seguros:** TLS/SSL para conexiones web cifradas, SSH para acceso remoto, RADIUS y Kerberos para autenticación centralizada.
  - **Autenticación basada en certificados digitales:** Frecuente en VPNs, servidores web y entornos empresariales con PKI (Infraestructura de Clave Pública).

3. Monitorización de eventos:

- Consiste en registrar, visualizar y analizar eventos del sistema que puedan indicar intentos de intrusión, fallos o mal uso.
- En Windows, se utiliza el Visor de Eventos; en Linux, el archivo */var/log/syslog* o herramientas como *journalctl*.

- Sistemas avanzados:
  - **SIEM (Security Information and Event Management):** herramientas como Splunk, Graylog, ELK Stack.
  - **Monitoreo de integridad:** herramientas como AIDE o Tripwire para detectar modificaciones no autorizadas en archivos del sistema.
- Las alertas automatizadas permiten detectar amenazas en tiempo real.

4. Seguridad física y lógica:

- **Seguridad física:** Incluye la protección del hardware ante accesos no autorizados, robo, sabotaje o catástrofes (temperatura, humedad, fuego). Se aplican medidas como:
  - Cerraduras, cámaras de videovigilancia, alarmas.
  - Controles de acceso biométrico o con tarjetas.
- **Seguridad lógica:** Consiste en la asignación correcta de permisos y roles, minimizando privilegios innecesarios (principio de menor privilegio).
  - Auditoría de accesos.
  - Desactivación de cuentas inactivas o innecesarias.
  - Segmentación de redes (VLAN, DMZ).
  - Aplicación de parches de seguridad y actualizaciones periódicas.

10.4.2. COPIAS DE SEGURIDAD Y RECUPERACIÓN

Una política de copias de seguridad (backup) eficaz garantiza la continuidad del negocio frente a pérdida de datos por fallos, ataques o errores humanos.

1. Tipos de backup:

- **Completo:** Copia todos los archivos seleccionados. Mayor seguridad, pero requiere más tiempo y espacio.
- **Incremental:** Solo copia los archivos modificados desde el último backup (completo o incremental). Ahorra espacio, pero la restauración es más lenta.
- **Diferencial:** Copia los archivos modificados desde el último backup completo. Intermedio en tiempo de copia y restauración.
- **Snapshots:** Capturas de estado del sistema o volúmenes, útiles para restauraciones rápidas.
- **Backup continuo:** Guarda cambios en tiempo real o casi real.

2. Herramientas de backup:

- **Linux:** *rsync*, *tar*, *borg*, *duplicity*, Bacula, Amanda.

- **Windows:** Windows Server Backup, Veeam, Acronis.
- **Multiplataforma o empresariales:** Veeam Backup & Replication, CommVault, Synology Active Backup.

- **Servicios en la nube:** Google Drive, OneDrive, Dropbox, Amazon S3, Backblaze, Azure Backup.
- Las herramientas permiten programar tareas, encriptar respaldos, comprimir archivos y almacenar en destinos locales o remotos.

3. Planes de contingencia:

- Involucran medidas para restaurar la operatividad del sistema tras un fallo o desastre.
- **Procedimientos de recuperación ante desastres (DRP):** Definen pasos detallados para restaurar servidores, servicios y datos críticos.
- **Pruebas periódicas de recuperación:** Es fundamental validar que los backups son funcionales y restaurables.
- **Regla 3-2-1:** Mantener 3 copias, en 2 medios distintos, y al menos 1 copia fuera de la ubicación principal (off-site).
- **Alta disponibilidad:** Uso de redundancia en hardware y software para evitar caídas.
- **Clústeres de recuperación, réplicas y failover automático:** Aumentan la resiliencia del sistema ante fallos.

Una política de seguridad y backup bien implementada no solo protege la información, sino que también da confianza a usuarios y clientes, reduce los riesgos operativos y cumple con normativas legales como el RGPD.

11. SEGURIDAD INFORMÁTICA

11.1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

La seguridad informática es una disciplina esencial en el mundo digital actual. Su objetivo principal es proteger los sistemas informáticos, las redes, los dispositivos y la información que en ellos se almacena y transmite. En un entorno cada vez más conectado, donde las amenazas evolucionan constantemente, contar con conocimientos sólidos en seguridad informática es imprescindible tanto para usuarios como para profesionales del sector tecnológico.

11.1.1. DEFINICIÓN Y OBJETIVOS DE LA SEGURIDAD INFORMÁTICA

La seguridad informática (también conocida como ciberseguridad) se define como el conjunto de medidas, prácticas y tecnologías diseñadas para proteger la información digital y los sistemas que la procesan frente a accesos no autorizados, alteraciones, destrucción o robo.

Los principales objetivos de la seguridad informática son:

- **Proteger la confidencialidad** de los datos, asegurando que solo los usuarios autorizados puedan acceder a ellos.
- **Garantizar la integridad** de la información, evitando alteraciones no autorizadas.
- **Asegurar la disponibilidad** de los sistemas y servicios, permitiendo su funcionamiento continuo sin interrupciones.
- **Prevenir y detectar incidentes**, así como recuperar los sistemas en caso de fallo.
- **Cumplir con las normativas legales y estándares** aplicables a la protección de datos.Principios fundamentales: confidencialidad, integridad y disponibilidad (CIA)

Estos tres pilares constituyen el modelo base en el que se apoya cualquier estrategia de seguridad informática:

- **Confidencialidad:** Garantiza que la información solo esté disponible para aquellos con autorización. Se consigue mediante mecanismos como el cifrado, el control de acceso y la autenticación de usuarios.
- **Integridad:** Asegura que la información no ha sido modificada de forma no autorizada. Se implementa con técnicas como el hashing, la firma digital y la gestión de versiones.
- **Disponibilidad:** Implica que los sistemas, servicios y datos deben estar accesibles cuando se necesiten. Se logra mediante redundancia, sistemas de respaldo, mantenimiento preventivo y planes de recuperación ante desastres.

11.1.2. TIPOS DE AMENAZAS Y VULNERABILIDADES

Una amenaza es cualquier circunstancia o evento con el potencial de causar daño a los sistemas o a la información. Las vulnerabilidades, en cambio, son debilidades o fallos en el sistema que pueden ser aprovechados por las amenazas.

- **Amenazas comunes:**
  - **Malware:** Virus, troyanos, gusanos, ransomware, spyware.
  - **Errores humanos:** Acciones accidentales como borrado de archivos, envío de información a destinatarios erróneos.
  - **Fallos de hardware o software:** Pueden provocar pérdida de datos o interrupción del servicio.
  - **Ataques de red:** Accesos no autorizados, escaneos de puertos, ataques de denegación de servicio (DoS/DDoS).
- **Vulnerabilidades frecuentes:**
  - Software sin actualizar o con errores de programación.
  - Contraseñas débiles o predecibles.
  - Configuraciones incorrectas en servidores y dispositivos.
  - Ausencia de cifrado en transmisiones de datos sensibles.

11.1.3. CONTEXTOS DE APLICACIÓN

La seguridad informática se aplica en múltiples entornos, adaptándose a las necesidades y riesgos específicos de cada uno:

- **Empresas:** Protección de redes internas, bases de datos de clientes, propiedad intelectual y recursos económicos. Implementación de políticas de seguridad corporativas.
- **Instituciones públicas:** Salvaguarda de información sensible de los ciudadanos, cumplimiento de normativas como el Esquema Nacional de Seguridad.
- **Hogares:** Uso seguro de dispositivos personales, redes Wi-Fi, protección infantil, gestión de dispositivos inteligentes (IoT).

- **Sector industrial:** Ciberseguridad aplicada a infraestructuras críticas, sistemas de control industrial (ICS/SCADA), redes de sensores, automatización y domótica.

La concienciación y la formación en ciberseguridad son claves para minimizar los riesgos en todos estos ámbitos. A lo largo del temario se abordarán con mayor profundidad las herramientas, técnicas y buenas prácticas necesarias para garantizar una protección efectiva frente a las amenazas digitales.

11.2. MALWARE Y AMENAZAS INFORMÁTICAS

Las amenazas informáticas representan uno de los mayores riesgos para la integridad, disponibilidad y confidencialidad de los datos en cualquier sistema informático. El malware, o software malicioso, es una de las principales herramientas utilizadas por los atacantes para comprometer sistemas, obtener información, dañar infraestructuras o extorsionar a los usuarios y organizaciones.

11.2.1. CLASIFICACIÓN DEL MALWARE

El malware se presenta en múltiples formas, cada una con características específicas:

- **Virus:** Programas maliciosos que se adjuntan a archivos legítimos. Necesitan intervención humana para ejecutarse y propagarse. Pueden dañar archivos, sistemas y redes completas.
- **Gusanos (worms):** Se propagan automáticamente por redes y sistemas sin necesidad de intervención del usuario. Consumen recursos y pueden colapsar redes enteras.

- **Troyanos:** Se presentan como programas legítimos para engañar al usuario. Permiten al atacante el acceso remoto al sistema.
- **Spyware:** Su objetivo es espiar la actividad del usuario. Recopila información como credenciales, historial de navegación, hábitos de consumo, etc.

- **Ransomware:** Cifra los archivos del sistema y exige un rescate económico para su recuperación. Ha causado pérdidas millonarias a empresas y organismos públicos.
- **Rootkits:** Diseñados para ocultar procesos o archivos maliciosos en el sistema, permitiendo que otros tipos de malware operen sin ser detectados.

ROOTKIT

11.2.2. MÉTODOS DE PROPAGACIÓN

El malware puede infiltrarse en los sistemas de múltiples maneras:

- **Dispositivos USB y almacenamiento externo:** Una de las vías más tradicionales y todavía efectiva. Puede activar scripts maliciosos automáticamente (autorun).
- **Correo electrónico (email):** Uno de los vectores más comunes. Correos con archivos adjuntos maliciosos o enlaces a sitios comprometidos. Técnica conocida como spear phishing si se dirige a personas concretas.
- **Navegación web:** Sitios web comprometidos o falsos (pharming) descargan malware sin conocimiento del usuario mediante técnicas como drive-by-download.
- **Redes P2P y descargas no oficiales:** Plataformas de intercambio de archivos sin control de seguridad.
- **Redes sociales y mensajería instantánea:** Enlaces acortados, mensajes engañosos, bots distribuyendo malware.

11.2.3. TÉCNICAS DE INGENIERÍA SOCIAL

La ingeniería social explota el factor humano como el eslabón más débil en la cadena de seguridad:

- **Phishing:** Suplantación de identidad mediante correos electrónicos o sitios web falsos que imitan entidades legítimas (bancos, plataformas de pago, servicios públicos).

Conoces que es el Phishing?

Son las estafas mediante engaños (ingeniería social), con el objetivo de obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Como saber si puede ser Phishing:

- Utilizan técnicas de ingeniería social o engaños para manipular información en la red y hacerse pasar por usuarios legítimos de servicios de internet, entidades económicas o algún servicio que realice transacciones online.
- Utilizan redes sociales para contactare con personas de forma masiva, enviando link de páginas de servicios básicos.

- Si te envían correos de forma masiva con información falsa y que tiene en su mayoría archivos .rar, los cuales contienen algún tipo de malware.
- Utilizan como gancho regalos o la perdida de la propia cuenta existente.

Consejos de seguridad para prevenir ser víctimas de Phishing

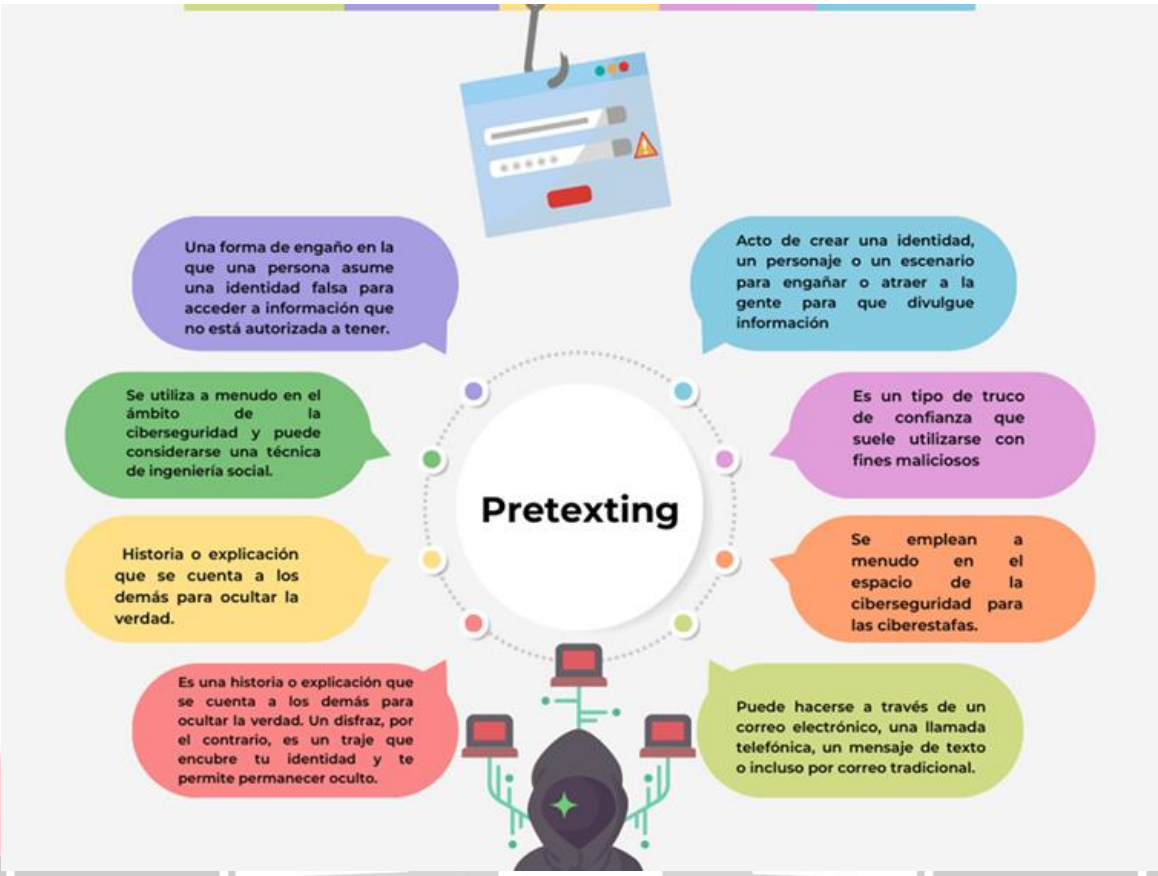
1. Infórmate solo a través de canales oficiales. No ingreses a sitios web a través de enlaces proporcionados en un mensaje o email.
2. Ten precaución con las solicitudes web sobre datos personales. Una entidad legal y responsable no te solicitará información confidencial por correo electrónico o vía telefónica.
3. Evita hacer clic en enlaces de sitios web que llegan por correo electrónico, de preferencia escribe tú mismo la dirección en tu navegador de internet.
4. Procura no aceptar solicitudes que te pidan acceder o ingresar datos con urgencias injustificadas.
5. Duda de mensajes con faltas de ortografía, errores gramaticales, fechas pasadas y saludos muy generales, es decir, sin que tenga ningún dato tuyo.
6. Si evidencias alguna anomalía de enlaces o sitios web, guarda la calma y denúnciala.

Comunicación Estratégica

- **Smishing:** Variante del phishing que utiliza mensajes SMS para engañar al usuario y redirigirlo a sitios fraudulentos.

- **Vishing:** Engaño mediante llamadas telefónicas. El atacante se hace pasar por un técnico de soporte, una entidad bancaria o una autoridad para obtener información sensible.

Pretexting: Creación de un escenario falso (pretexto) para manipular a la víctima y conseguir que revele información o realice acciones específicas.



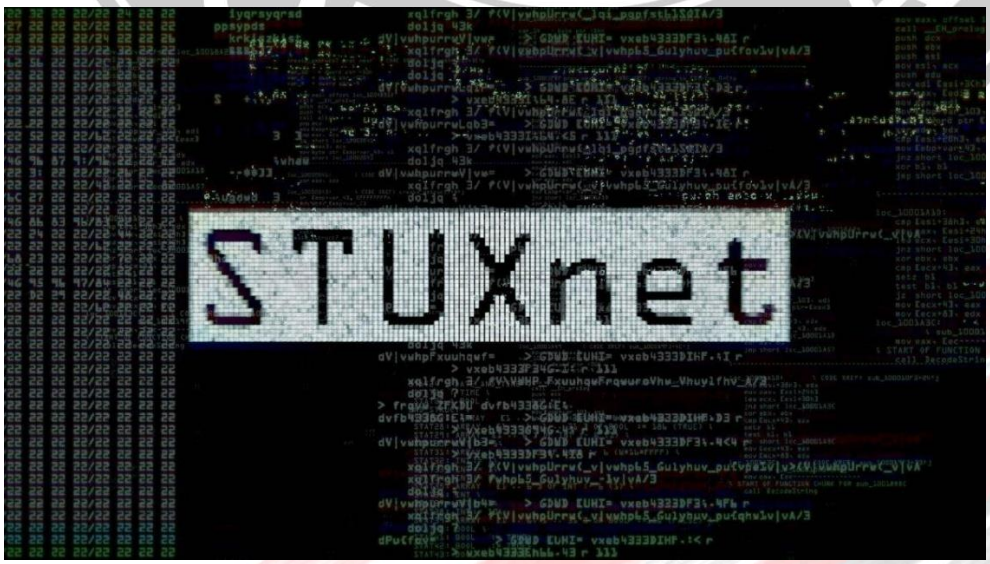
Estas técnicas se basan en la confianza, el miedo, la urgencia o la falta de conocimientos del usuario para lograr su objetivo.

11.2.4. CASOS REALES Y ANÁLISIS DE IMPACTO

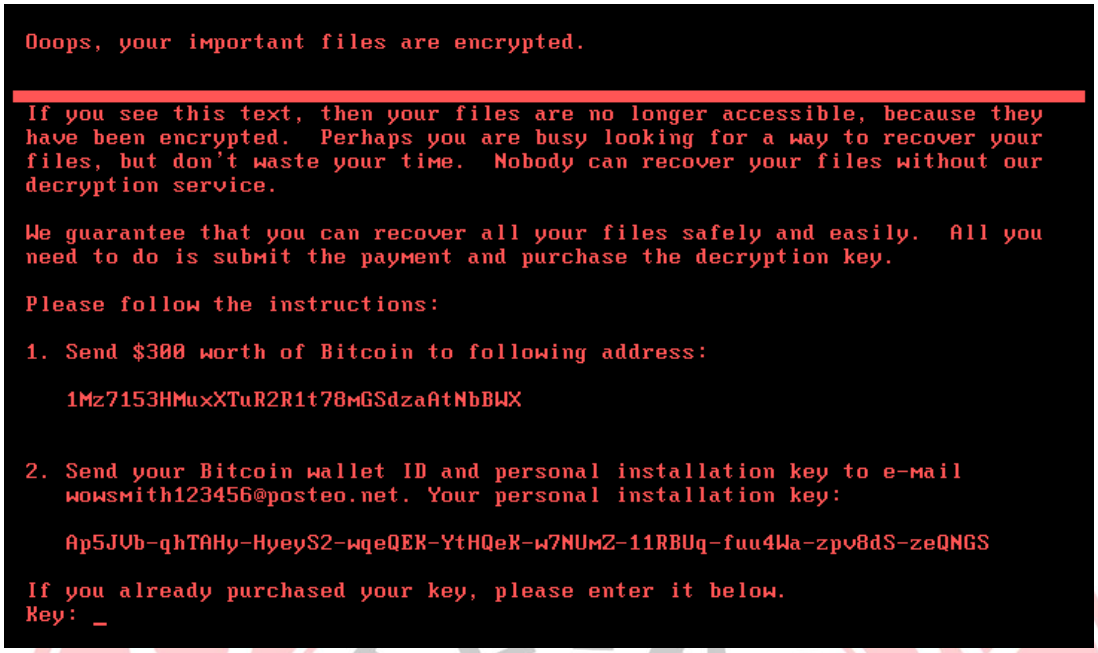
La historia de la seguridad informática está llena de incidentes causados por malware y ataques cibernéticos con gran repercusión:

- **WannaCry (2017):** Ransomware que afectó a más de 200.000 sistemas en más de 150 países. Aprovechó una vulnerabilidad en sistemas Windows. Afectó a hospitales, empresas, universidades y administraciones públicas.

- **Stuxnet (2010):** Gusano altamente sofisticado diseñado para sabotear sistemas industriales SCADA. Su objetivo fue afectar al programa nuclear iraní, y demostró la capacidad del malware para causar daño físico.



- **NotPetya (2017):** Similar a WannaCry, pero con intención destructiva. Afectó a empresas multinacionales como Maersk, causando millones en pérdidas.



- **Ataques a través de macros de Office:** Muchos ataques utilizan documentos de Word o Excel con macros maliciosas que ejecutan código cuando se abre el archivo.

El análisis forense de estos casos permite aprender de los errores, identificar patrones y mejorar las defensas.

11.3. POLÍTICAS DE SEGURIDAD Y NORMATIVAS

La implementación de políticas de seguridad y el cumplimiento de normativas son elementos fundamentales para garantizar una protección eficaz de los sistemas informáticos. Establecen el marco normativo y técnico que guía las actuaciones en materia de seguridad en cualquier organización, pública o privada.

11.3.1. DEFINICIÓN DE POLÍTICAS DE SEGURIDAD EN UNA ORGANIZACIÓN

Una **política de seguridad** es un conjunto de normas, procedimientos y directrices que define como una organización protege sus activos de información. Su objetivo es minimizar los riesgos asociados al uso de sistemas informáticos y garantizar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

Características de una buena política de seguridad:

- **Documentada** y accesible para todos los usuarios.
- **Flexible**, para adaptarse a cambios tecnológicos y organizativos.
- **Clara** y específica en cuanto a responsabilidades y procedimientos.
- **Alineada** con los objetivos estratégicos de la organización.

Elementos típicos de una política de seguridad:

- Control de accesos y privilegios de usuarios.
- Normas sobre el uso aceptable de los sistemas y recursos.
- Procedimientos de gestión de incidentes de seguridad.
- Reglas sobre instalación y uso de software.
- Directrices sobre copias de seguridad y recuperación de datos.
- Protección de dispositivos móviles y teletrabajo.
- Revisión y actualización periódica de la política.

Ventajas de implantar una política de seguridad:

- Mejora de la **resiliencia** frente a incidentes de ciberseguridad.
- **Reducción de riesgos** asociados al factor humano.
- **Cumplimiento legal y normativo** (ej. RGPD, ENS).
- **Concienciación** de los empleados y creación de una cultura de ciberseguridad.

11.3.2. PERFILES Y ROLES DE SEGURIDAD: ADMINISTRADOR, AUDITOR, USUARIO

Dentro de una organización, se establecen diferentes perfiles o roles relacionados con la gestión de la seguridad. Cada uno tiene responsabilidades específicas:

- **Administrador de seguridad**:
  - Configura, supervisa y mantiene los sistemas de seguridad.
  - Controla los accesos, configura firewalls, IDS/IPS, antivirus, etc.
  - Aplica actualizaciones, realiza auditorías internas y gestiona incidentes.
  - Es el responsable técnico de que la infraestructura esté segura.
- **Auditor de seguridad**:
  - Evalúa el nivel de cumplimiento de la política de seguridad.
  - Realiza informes de vulnerabilidades, pruebas de penetración (pentest) y revisiones periódicas.
  - Proporciona recomendaciones para mejorar los controles de seguridad.
- **Usuario**:
  - Utiliza los recursos de forma adecuada y conforme a las normas establecidas.
  - Informa de posibles incidentes y colabora en la protección de los sistemas.
  - Es responsable de mantener la confidencialidad de sus credenciales.

Asignar y definir correctamente estos roles es fundamental para evitar ambigüedades, fomentar la responsabilidad y facilitar la trazabilidad de acciones.

11.3.3. NORMAS Y ESTÁNDARES INTERNACIONALES: ISO 27001, ENS, RGPD, NIST

L a seguridad informática no solo se basa en tecnologías, sino también en el cumplimiento de **normas, estándares y marcos regulatorios** que proporcionan una base sólida y reconocida para establecer políticas, procedimientos y controles eficaces. A continuación, se describen los más relevantes a nivel internacional y nacional:

11.3.3.1. ISO/IEC 27001

La **ISO/IEC 27001** es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Su objetivo principal es proporcionar un marco para establecer, implementar, mantener y mejorar un **Sistema de Gestión de Seguridad de la Información (SGSI)**.

- Esta norma adopta un **enfoque basado en el análisis de riesgos**, lo que significa que cada organización debe identificar las amenazas y vulnerabilidades específicas a las que está expuesta.
- Define un conjunto de **controles técnicos, físicos y organizativos** que deben aplicarse para proteger la confidencialidad, integridad y disponibilidad de la información.
- Incluye políticas como el control de acceso, la seguridad en redes, la gestión de incidentes y la continuidad de negocio.
- La correcta implantación del SGSI permite a una organización **obtener la certificación oficial ISO 27001**, demostrando así a terceros (clientes, socios, autoridades) su compromiso con la seguridad.
- Es aplicable a cualquier tipo de organización, independientemente de su tamaño o sector.

11.3.3.2. ENS (Esquema Nacional de Seguridad)

El **Esquema Nacional de Seguridad** es un marco legal **obligatorio en España**, regulado por el **Real Decreto 311/2022**, destinado a garantizar la seguridad de los sistemas de información utilizados por las Administraciones Públicas y por aquellas entidades privadas que prestan servicios al sector público.

- Establece los **principios básicos** y **requisitos mínimos** que deben cumplir los sistemas para asegurar la protección de la información.
- Introduce una **clasificación por niveles de seguridad** (bajo, medio, alto), que determina el grado de exigencia de las medidas a aplicar según el impacto que tendría un incidente en la organización o en los ciudadanos.
- Incluye medidas de **carácter organizativo (como la asignación de responsabilidades)**, **operativo (como la gestión de incidentes)** y de **protección tecnológica (como el cifrado o el control de accesos)**.
- Su cumplimiento es evaluado mediante auditorías, y su implantación es necesaria para garantizar la **confianza en la administración electrónica y los servicios digitales públicos**.

11.3.3.3. RGPD (Reglamento General de Protección de Datos)

El **Reglamento General de Protección de Datos (RGPD)**, aprobado por la Unión Europea y en vigor desde 2018, es el marco legal que regula el tratamiento de **datos personales de los ciudadanos europeos**, tanto por parte de entidades públicas como privadas.

- Reconoce una serie de **derechos fundamentales** a los individuos, como el derecho al acceso, rectificación, supresión (derecho al olvido), oposición y portabilidad de sus datos personales.
- Introduce el principio de **"responsabilidad proactiva"**, exigiendo a las organizaciones que tomen medidas adecuadas desde el diseño de cualquier sistema o proceso que implique datos personales (**"privacy by design"** y **"privacy by default"**).
- El consentimiento del usuario debe ser **explícito, informado y revocable**.

- Obliga a notificar violaciones de seguridad (brechas de datos) en un plazo máximo de 72 horas.
- Impone **sanciones severas** en caso de incumplimiento, que pueden alcanzar hasta el **4% de la facturación global anual de la empresa infractora**.

11.3.3.4. NIST (National Institute of Standards and Technology)

El **NIST**, dependiente del Departamento de Comercio de los Estados Unidos, es una entidad de referencia internacional en la publicación de **normas, guías y marcos técnicos** relacionados con la ciberseguridad.

- Su **Cybersecurity Framework** es ampliamente utilizado por organizaciones públicas y privadas en todo el mundo para mejorar la protección de infraestructuras críticas.
- Este marco se organiza en cinco funciones clave:
    1. **Identificar**: comprender los activos, riesgos y entorno empresarial.
    2. **Proteger**: desarrollar medidas para salvaguardar los sistemas y datos.
    3. **Detectar**: identificar eventos de ciberseguridad de forma oportuna.
    4. **Responder**: actuar ante incidentes para minimizar su impacto.
    5. **Recuperar**: restaurar las capacidades afectadas y mejorar tras el incidente.
- Además, el NIST desarrolla publicaciones técnicas como la **SP 800-53**, que detalla más de 900 controles de seguridad clasificados por categorías y niveles de criticidad.
- Aunque se trata de una iniciativa estadounidense, **su enfoque modular y flexible ha sido adoptado por muchas organizaciones a nivel internacional**, especialmente en sectores altamente regulados.

Conclusión

El conocimiento y aplicación de estas normas y marcos es esencial para cualquier profesional de la ciberseguridad. No solo ayudan a proteger los sistemas y los datos, sino que también permiten cumplir con requisitos legales, obtener certificaciones reconocidas y generar confianza en clientes y usuarios. Adoptar estos estándares no es solo una cuestión técnica, sino también estratégica y organizativa.

Comparativa:

Norma/Reglamento	Aplicación	Enfoque	Certificación
ISO/IEC 27001	Global	SGSI basado en riesgos	Sí
ENS	España	Obligatorio para sector público	No (evaluación externa)
RGPD	UE	Protección de datos personales	No, pero exige cumplimiento
NIST	EE.UU./Global	Marco técnico de referencia	No, orientado a buenas prácticas

11.3.4. AUDITORÍA DE SEGURIDAD INFORMÁTICA

Una **auditoría de seguridad informática** es un proceso estructurado que tiene como objetivo evaluar el estado de la seguridad en una organización y detectar posibles deficiencias o vulnerabilidades.

Fases de la auditoría:

1. **Planificación**:
   - Se definen los objetivos, alcance, recursos y metodología.
   - Se identifican los sistemas y procesos a auditar.
2. **Recolección de información**:
   - Inventario de activos, análisis de configuraciones, entrevistas, revisión documental.
3. **Análisis de vulnerabilidades**:
   - Se realizan escaneos con herramientas especializadas (ej. Nessus, OpenVAS).
   - Se simulan ataques controlados (pentesting).
4. **Evaluación de cumplimiento**:
   - Se comparan los resultados con las políticas internas y las normativas aplicables (ISO, ENS, RGPD...).
5. **Informe de resultados**:
   - Se documentan las vulnerabilidades, riesgos y recomendaciones de mejora.
   - Se priorizan las acciones según el nivel de criticidad.

Tipos de auditoría:

- **Interna**: Realizada por personal de la propia organización.
- **Externa**: Llevada a cabo por un tercero independiente.
- **De cumplimiento**: Evalúa el grado de alineación con normativas o certificaciones.
- **Técnica**: Focalizada en aspectos puramente tecnológicos (firewalls, contraseñas, cifrado...).
- **Operativa**: Centrada en los procedimientos y prácticas del día a día.

Una auditoría bien ejecutada permite:

- Detectar **vulnerabilidades antes de que sean explotadas**.
- **Mejorar la postura de seguridad** general de la organización.
- Cumplir con **requisitos legales o contractuales**.
- Establecer un **plan de mejora continua** en ciberseguridad.

11.4. AUTENTICACIÓN Y CONTROL DE ACCESO

La autenticación y el control de acceso son pilares esenciales de la seguridad informática. Su correcta implementación permite garantizar que solo las personas autorizadas accedan a los recursos y que lo hagan con los privilegios adecuados. Estos mecanismos son fundamentales para mantener la confidencialidad, integridad y disponibilidad de los sistemas.

11.4.1. MÉTODOS DE AUTENTICACIÓN: CONTRASEÑAS, BIOMETRÍA, TOKENS

Autenticación es el proceso mediante el cual un sistema verifica la identidad de un usuario, dispositivo o entidad. Existen diversos métodos, que se pueden clasificar según el tipo de factor que utilizan:

Factores de autenticación:

- **Algo que sabes**: contraseñas, PIN, preguntas de seguridad.
- **Algo que tienes**: tarjetas inteligentes, tokens, certificados digitales.
- **Algo que eres**: huellas dactilares, reconocimiento facial, iris, voz.

Tipos de autenticación:

- **Contraseñas**:

- Método más común y tradicional.
- Requieren buenas prácticas: longitud mínima, complejidad, renovación periódica.
- Vulnerables al robo, reutilización, ataques de fuerza bruta y diccionario.

- **Biometría**:
  - Utiliza rasgos físicos o conductuales únicos del individuo.
  - Ejemplos: huella digital, reconocimiento facial, escaneo del iris, geometría de la mano.
  - Ventajas: difícil de falsificar, cómoda.
  - Desventajas: pueden verse comprometidos los datos biométricos (no se pueden cambiar), posibles falsos positivos o negativos.
- **Tokens**:
  - Dispositivos físicos o virtuales que generan códigos temporales.
  - Pueden ser tokens hardware (ej. llaveros OTP), o software (apps tipo Google Authenticator).
  - Se usan en autenticación de dos factores (2FA) y MFA.

Otros métodos adicionales:

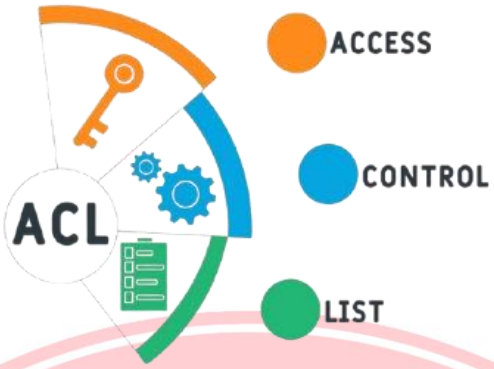
- **Certificados digitales**: utilizados en entornos empresariales, cifrados y firmados por una autoridad certificadora.
- **Autenticación basada en conocimiento contextual**: ubicación, horario habitual, dispositivo habitual, etc.

11.4.2. CONTROL DE ACCESOS: LISTAS DE CONTROL DE ACCESO (ACL), RBAC, MFA

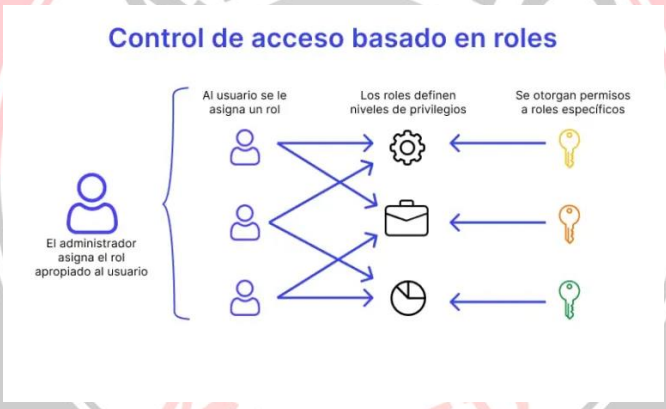
Una vez autenticado el usuario, es necesario controlar **a qué recursos puede acceder** y **con qué nivel de privilegio**. Esto se denomina **control de acceso**.

Modelos de control de acceso:

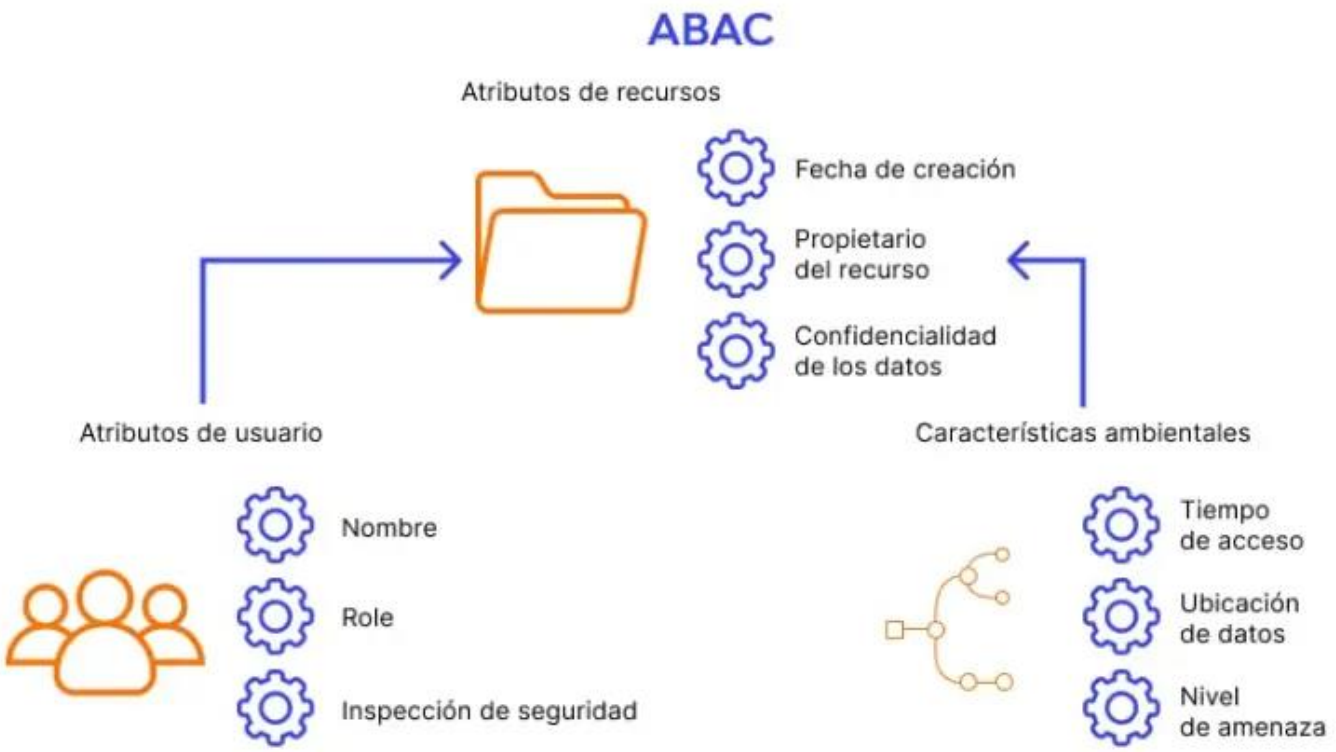
- **Listas de Control de Acceso (ACL)**:



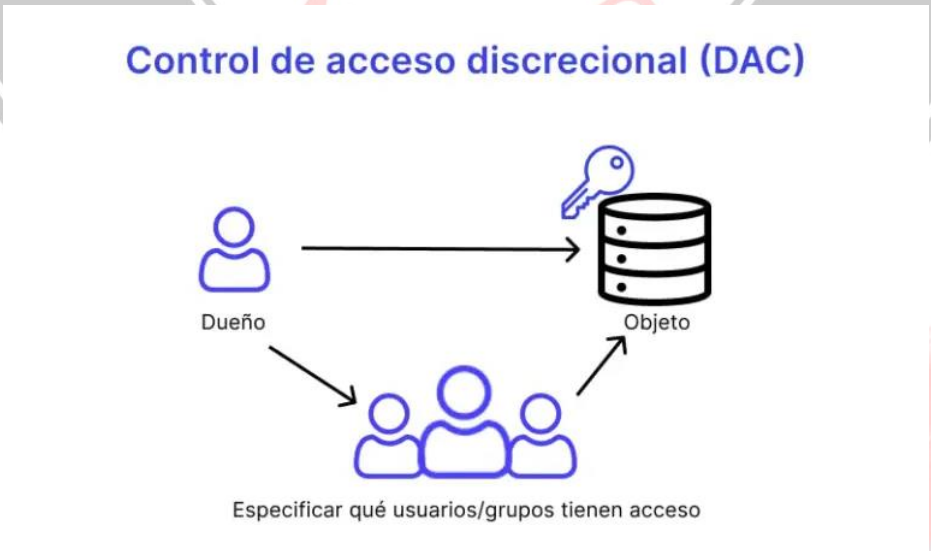
  - Asocian permisos concretos (lectura, escritura, ejecución) a cada usuario o grupo para un recurso determinado.
  - Se usan en sistemas operativos, routers, cortafuegos.
  - Flexibles, pero difíciles de mantener en entornos grandes.
- **RBAC (Control de Acceso Basado en Roles)**:



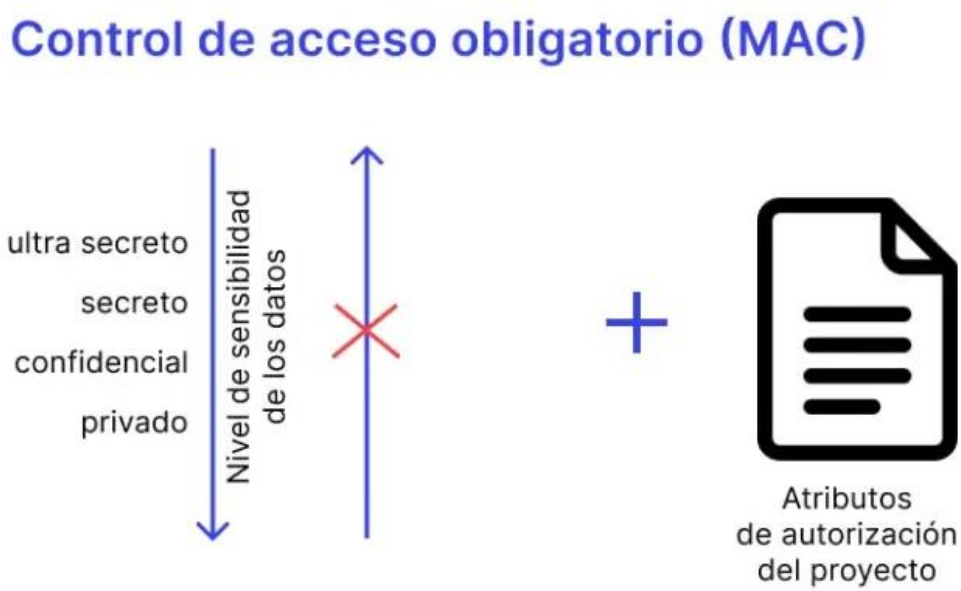
  - Asigna permisos a roles, y roles a usuarios.
  - Ejemplo: el rol "Contabilidad" puede acceder al sistema de facturación; el rol "Soporte" puede ver incidencias.
  - Ventajas: escalabilidad, gestión centralizada y más ordenada.
- **ABAC (Control de Acceso Basado en Atributos)**:
  - Usa atributos del usuario, del recurso, del entorno y de la acción para tomar decisiones.
  - Más dinámico y flexible, pero más complejo de implementar.



- **DAC (Control de Acceso Discrecional)**:
  - El propietario del recurso decide quién puede acceder.
  - Ejemplo típico: permisos en archivos de Windows o Linux.



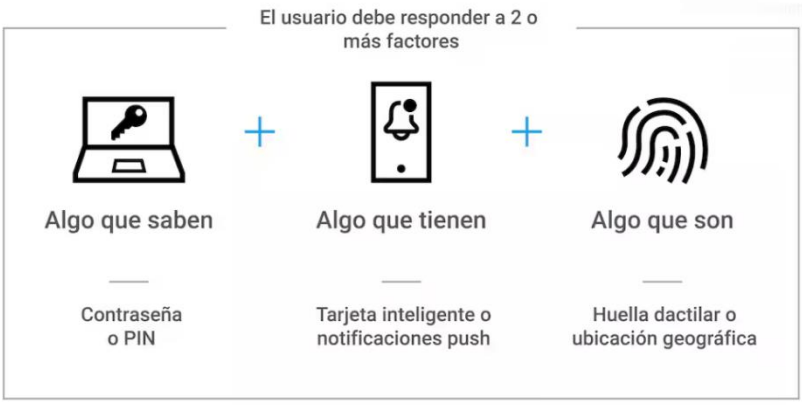
- **MAC (Control de Acceso Obligatorio)**:



  - El sistema impone políticas rígidas de acceso basadas en etiquetas de seguridad.
  - Utilizado en entornos militares o con alta confidencialidad.

MFA (Autenticación Multifactor):

- Requiere más de un factor de autenticación para acceder.
- Ejemplo: contraseña (algo que sabes) + código de un token (algo que tienes).
- Aumenta significativamente la seguridad frente al robo de credenciales.
- Ya es obligatoria en muchas plataformas de banca, administración pública y servicios cloud.



11.4.3. GESTIÓN DE IDENTIDADES DIGITALES

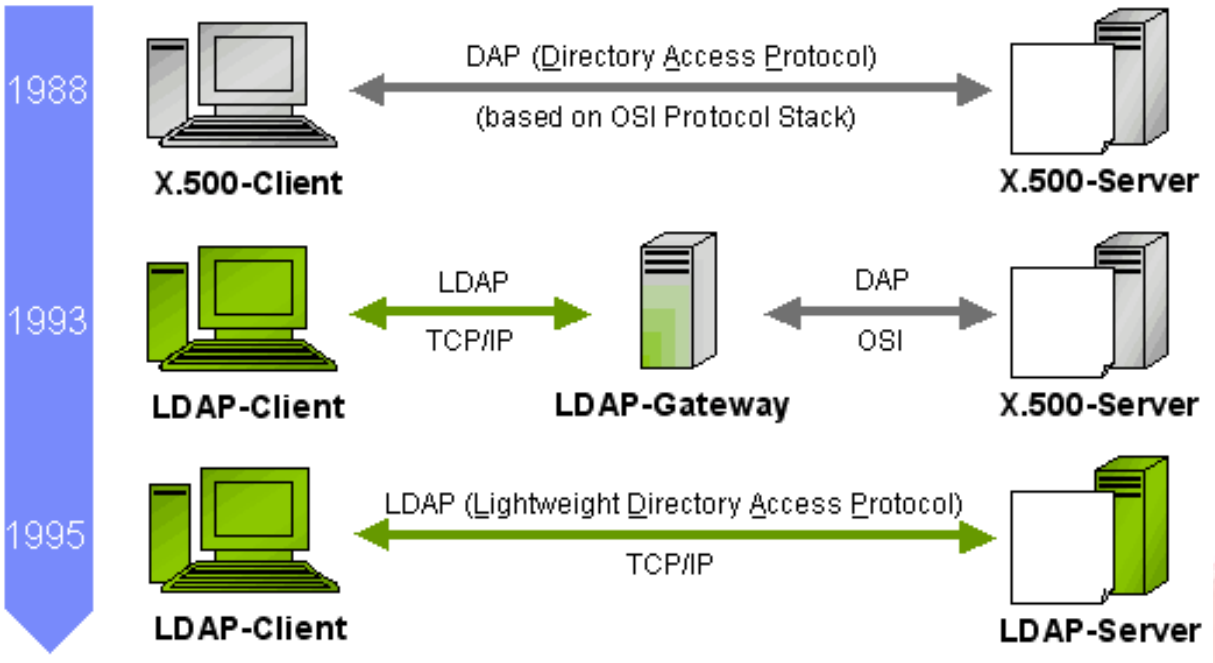
La **gestión de identidades (Identity Management)** se refiere a los procesos y herramientas que permiten administrar de forma segura las identidades digitales y los derechos de acceso de los usuarios en una organización.

Funciones clave:

- **Alta, modificación y baja de usuarios**: también llamado ciclo de vida del usuario.
- **Asignación de roles y permisos** según el puesto y funciones.
- **Sincronización entre sistemas** (correo, directorio activo, CRM...).
- **Autenticación centralizada**: uso de sistemas SSO (Single Sign-On) o federación de identidades.

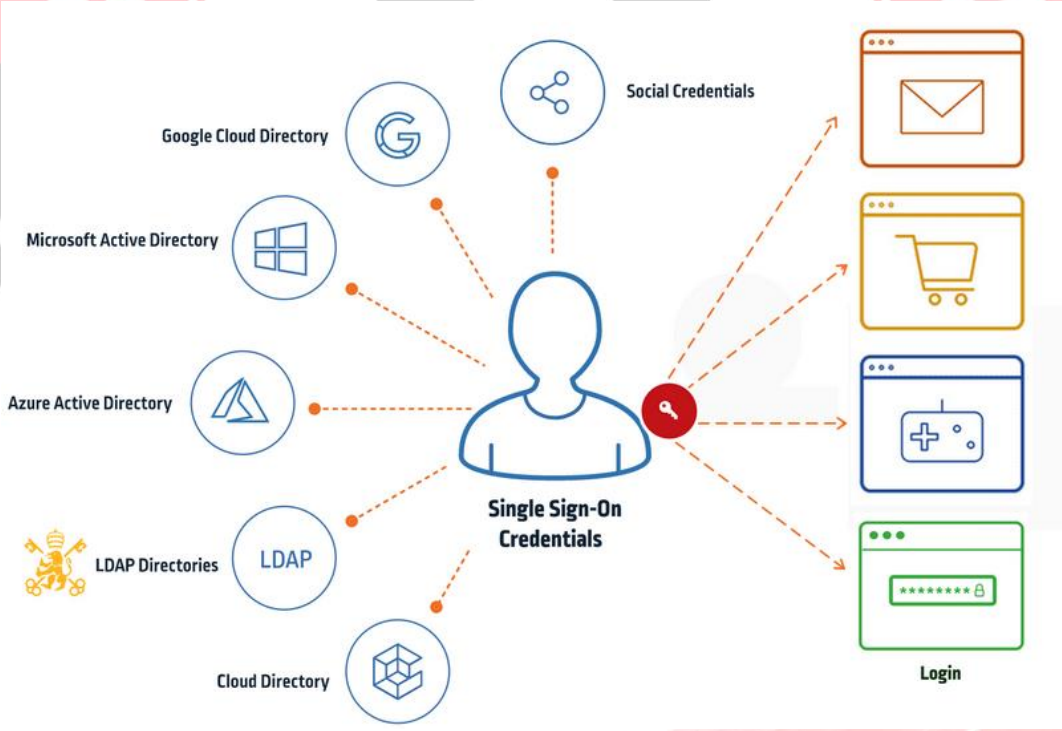
Tecnologías utilizadas:

- **LDAP (Lightweight Directory Access Protocol)**: protocolo de acceso a servicios de directorio. Se usa en Active Directory, OpenLDAP, etc.

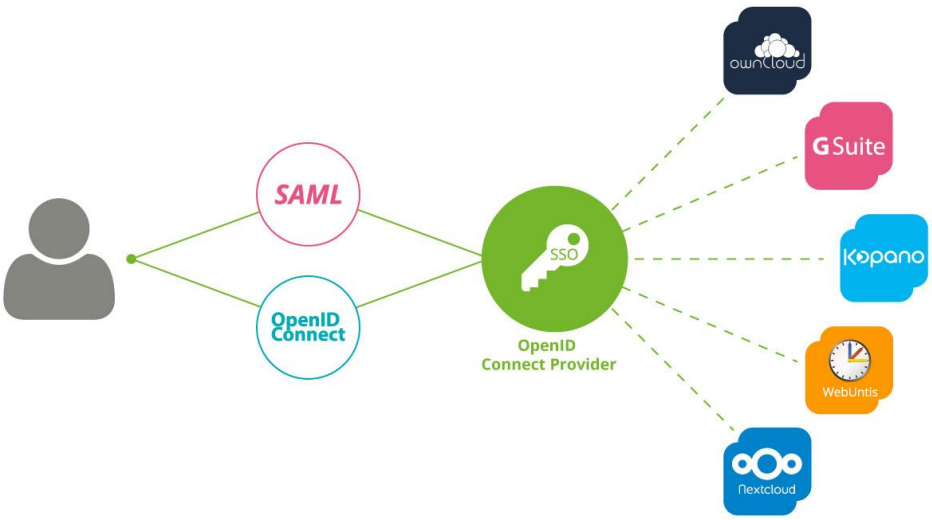


- **Active Directory**: servicio de directorio de Microsoft que gestiona usuarios, equipos y políticas de seguridad.

- **SSO (Single Sign-On)**: permite que un usuario acceda a múltiples sistemas con una única autenticación.



- **SAML / OAuth / OpenID Connect**: protocolos de autenticación y autorización para entornos web y móviles.



Ventajas de una buena gestión de identidades:

- Mejora de la **seguridad** y la trazabilidad.
- Reducción del **riesgo de accesos indebidos**.
- Facilita el cumplimiento de normativas como RGPD, ENS, ISO 27001.
- Mejora la **eficiencia operativa** en el alta y baja de empleados.

11.4.4. BUENAS PRÁCTICAS EN LA CREACIÓN Y MANTENIMIENTO DE CREDENCIALES

Las credenciales (normalmente nombre de usuario y contraseña) siguen siendo el método de autenticación más utilizado, aunque su vulnerabilidad exige la aplicación de buenas prácticas:

Recomendaciones para contraseñas seguras:

- Longitud mínima: al menos 12 caracteres.
- Uso de combinaciones de letras mayúsculas/minúsculas, números y símbolos.
- No reutilizar contraseñas entre servicios.
- No usar palabras del diccionario, fechas, nombres propios, etc.
- Cambiar periódicamente las contraseñas sensibles.
- Evitar escribirlas en papel o archivos sin cifrar.

Gestión segura de contraseñas:

- Uso de **gestores de contraseñas**: KeePass, Bitwarden, LastPass, etc.
- Implementar **MFA** como capa adicional.

- Configuración de **bloqueo de cuenta** tras varios intentos fallidos.
- Monitorización de **filtraciones de contraseñas** (ej. con "Have I Been Pwned").

Otras prácticas generales:

- Deshabilitar cuentas inactivas o sin uso.
- Implementar políticas de caducidad de contraseñas en entornos corporativos.
- Formar a los usuarios en la **concienciación del riesgo** (phishing, ingeniería social).

11.5. SEGURIDAD EN SISTEMAS OPERATIVOS Y APLICACIONES

Los sistemas operativos y las aplicaciones son componentes fundamentales de cualquier infraestructura informática. Por ello, asegurar su correcto funcionamiento y protegerlos frente a amenazas es clave para garantizar la seguridad de la información y la continuidad de los servicios.

11.5.1. ACTUALIZACIONES Y PARCHES

Las **actualizaciones** y **parches** son elementos esenciales para mantener los sistemas protegidos frente a vulnerabilidades conocidas. Los desarrolladores de sistemas operativos y software publican regularmente parches para corregir errores, cerrar brechas de seguridad y mejorar el rendimiento.

Tipos de actualizaciones:

- **Parches de seguridad**: Corrigen vulnerabilidades que pueden ser explotadas por atacantes.
- **Actualizaciones funcionales**: Añaden nuevas características o mejoran funcionalidades existentes.
- **Actualizaciones críticas**: Solucionan errores graves que afectan a la estabilidad o seguridad del sistema.

Buenas prácticas:

- Activar la **actualización automática** en sistemas y software, siempre que sea posible.
- Comprobar regularmente la disponibilidad de parches en sistemas que no se actualizan automáticamente.
- Aplicar primero los parches en un entorno de pruebas en infraestructuras críticas.

- Priorizar la instalación de **parches de seguridad urgentes** (zero-day, CVE críticos).

Gestión de parches (patch management):

- Herramientas como **WSUS**, **SCCM** (Microsoft), **Landscape** (Ubuntu), **YUM/DNF** (Red Hat/CentOS), o **Munki** (macOS).
- Automatización de despliegue de actualizaciones en grandes redes.
- Generación de informes de cumplimiento.

Riesgos de no aplicar parches:

- Exposición a malware, ransomware, y exploits conocidos.
- Incumplimiento de normativas de seguridad.
- Pérdida de datos y reputación institucional.

11.5.2. SEGURIDAD EN WINDOWS, LINUX Y MACOS

Cada sistema operativo tiene sus propias herramientas, características y mecanismos de seguridad. Es fundamental conocerlos para aplicar buenas prácticas y medidas específicas.

Windows:

- Uso del **Control de Cuentas de Usuario (UAC)** para limitar acciones administrativas.
- Configuración de **políticas de grupo (GPO)** para aplicar restricciones a nivel de dominio.
- Herramientas de seguridad integradas: **Windows Defender**, **BitLocker** (cifrado de disco), **Firewall de Windows**.
- **NTFS**: sistema de archivos que permite aplicar permisos granulares a carpetas y archivos.

Linux:

- Gestión de permisos mediante sistema de archivos tipo **ext4** con atributos de usuario, grupo y otros.
- Uso de **sudo** para tareas administrativas (evita usar directamente la cuenta root).
- Aplicación de **iptables/nftables** para la gestión de reglas de firewall.
- Herramientas como **SELinux** (en Red Hat/CentOS) o **AppArmor** (en Ubuntu) para el control de acceso obligatorio (MAC).
- Registro de actividad mediante **syslog**, **journald** y archivos de log del sistema.

macOS:

- Basado en Unix, similar en estructura de seguridad a Linux.
- Cifrado de disco con **FileVault**.
- Sistema de permisos y sandboxing de aplicaciones.
- **Gatekeeper**: bloquea la instalación de software no firmado por Apple.
- **XProtect**: protección integrada contra malware.

Comparativa rápida:

Característica	Windows	Linux	macOS
Cifrado de disco	BitLocker	LUKS, eCryptfs	FileVault
Firewall	Windows Defender Firewall	iptables/nftables	pf (Packet Filter)
Control de acceso	ACL, GPO	permisos, SELinux/AppArmor	Sandbox, Gatekeeper
Antivirus integrado	Sí (Windows Defender)	No (requiere externo)	Sí (XProtect)

11.5.3. CONTROL DE SERVICIOS, PUERTOS Y PROCESOS

Una de las medidas más importantes para asegurar un sistema operativo es **controlar qué servicios están activos**, qué **puertos están abiertos** y qué **procesos se están ejecutando**.

Servicios:

- Solo deben estar activos los **servicios necesarios** para la operativa del sistema.
- Cada servicio activo es un punto potencial de ataque.
- Se deben **desactivar o eliminar** servicios innecesarios o inseguros.

Comandos útiles:

- **Windows**: *services.msc*, *sc query*, *tasklist*
- **Linux**: *systemctl*, *service*, *ps aux, netstat*, *ss*

Puertos:

- Cada servicio utiliza un puerto para comunicarse. Algunos puertos comunes:
  - HTTP (80), HTTPS (443), SSH (22), FTP (21), RDP (3389), SMB (445).
- Escanear puertos abiertos ayuda a identificar exposiciones innecesarias.
  - Herramientas: **nmap**, **netstat**, **ss**, **TCPView**.

Procesos:

- Monitorizar procesos activos permite detectar comportamientos anómalos o malware en ejecución.
- Es fundamental registrar:
    - Consumo de CPU/RAM anormal.
    - Procesos desconocidos o sin firma digital.
    - Ejecuciones repetitivas o programadas sin justificación.

Buenas prácticas:

- Aplicar el principio de **mínimos privilegios**: solo ejecutar lo estrictamente necesario.
- Habilitar **sistemas de detección de intrusos (HIDS)**: ej. OSSEC, Wazuh.
- Auditar periódicamente el estado de servicios y puertos.

11.5.4. ENDURECIMIENTO DEL SISTEMA (HARDENING)

El **endurecimiento o hardening** consiste en aplicar un conjunto de configuraciones y medidas que refuercen la seguridad de un sistema operativo o aplicación, reduciendo la superficie de ataque.

Principios del hardening:

- **Eliminar** o desinstalar software y servicios innecesarios.
- **Deshabilitar funciones no utilizadas** (scripts, puertos, cuentas por defecto).
- **Configurar correctamente permisos** y accesos.
- **Aplicar parches de seguridad** y mantener el sistema actualizado.
- **Monitorizar** y registrar continuamente eventos relevantes.

Medidas comunes de hardening:

- Cambiar **puertos por defecto** (ej. SSH en el 22, RDP en el 3389).
- Forzar el uso de **contraseñas seguras y caducidad periódica**.
- Desactivar **USB o dispositivos externos** si no son necesarios.
- Implementar **cifrado de disco y comunicaciones** (TLS, VPN).
- Configurar **logs de auditoría** y rotación de registros.
- Restringir el **arranque desde dispositivos externos** en BIOS/UEFI.

Herramientas y guías:

- **CIS Benchmarks**: guías de hardening por sistema operativo, reconocidas internacionalmente.
- **Lynis**: auditoría y recomendaciones automáticas para Linux/Unix.
- **Microsoft Security Compliance Toolkit**: plantillas de seguridad para Windows.

Ansible/Salt/Puppet: automatización del hardening en entornos grandes.

11.6. SEGURIDAD EN REDES LOCALES Y TELECOMUNICACIONES

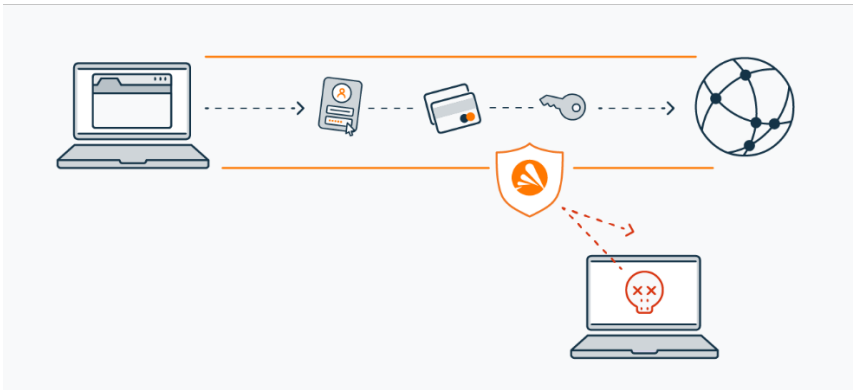
Las redes locales (LAN), inalámbricas (WLAN) y los sistemas de telecomunicaciones son componentes fundamentales en cualquier infraestructura de TI. Su seguridad es crítica para evitar accesos no autorizados, interceptaciones de datos, interrupciones del servicio y ataques a gran escala.

11.6.1. AMENAZAS EN REDES LAN/WLAN

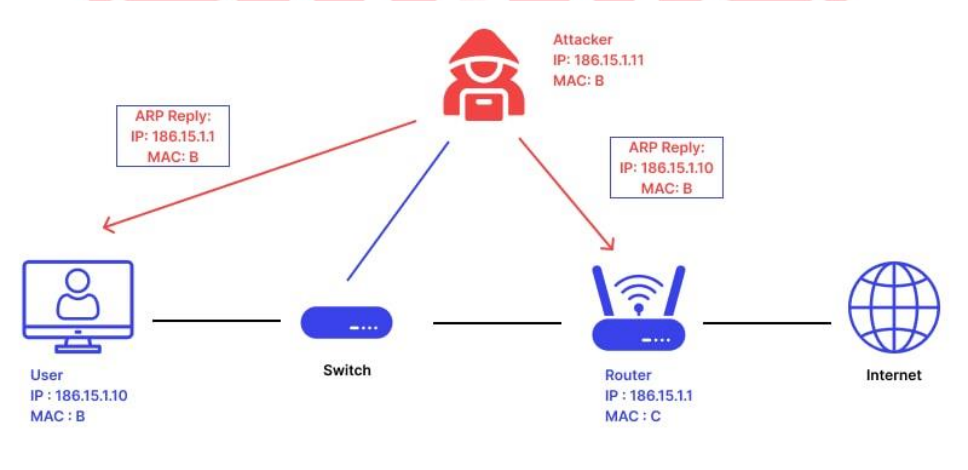
Tanto las redes cableadas (LAN) como las inalámbricas (WLAN) están expuestas a diversas amenazas, muchas de las cuales pueden comprometer la confidencialidad, integridad o disponibilidad de los sistemas conectados.

Amenazas en redes LAN:

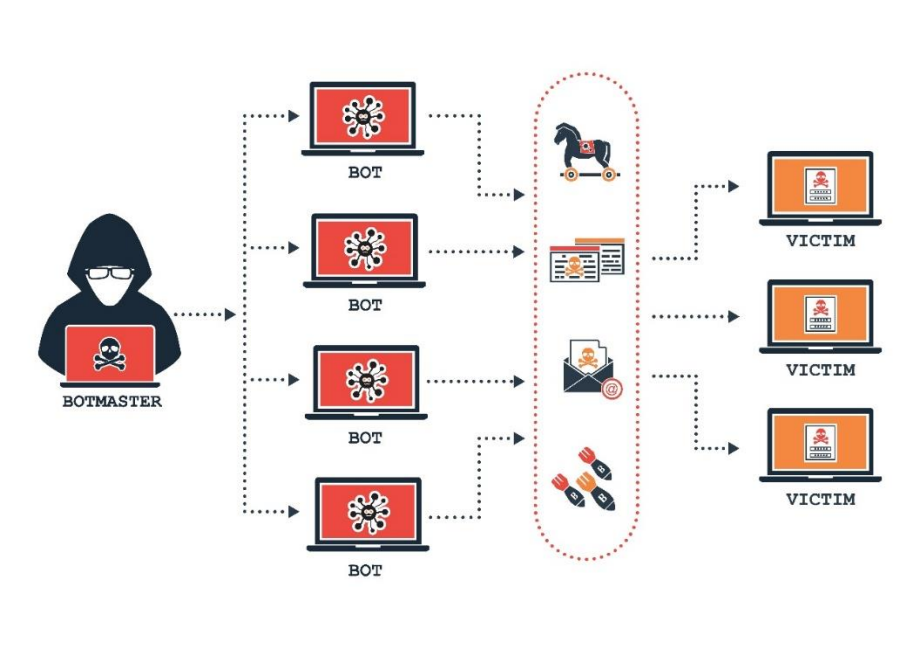
- **Sniffing o captura de tráfico**: mediante herramientas como Wireshark o tcpdump, un atacante puede interceptar información no cifrada.



- **ARP Spoofing / ARP Poisoning**: manipulación de la tabla ARP de la red para interceptar o redirigir tráfico.



- **Ataques DoS/DDoS**: saturan el ancho de banda o los dispositivos de red, causando denegación de servicio.



- **Exploits en switches o routers**: errores en la configuración o vulnerabilidades del firmware.

Amenazas en redes WLAN:

- **Robo de credenciales**: especialmente si se usa cifrado débil (WEP, WPA).
- **Redes falsas (Evil Twin)**: punto de acceso falso con nombre similar al legítimo.
- **Wardriving**: búsqueda activa de redes Wi-Fi vulnerables desde un vehículo.
- **Interferencias y jamming**: bloqueos deliberados de señal inalámbrica.
- **Fuerza bruta al WPA2/WPA3**: especialmente con contraseñas débiles.

Buenas prácticas de mitigación:

- Uso de cifrado **WPA2 o WPA3** con contraseñas fuertes.
- Ocultación del SSID (aunque no es una medida infalible).
- Filtrado MAC (aunque también falsificable).
- Segmentación del tráfico y monitoreo continuo.
- Desactivación del DHCP en redes críticas.

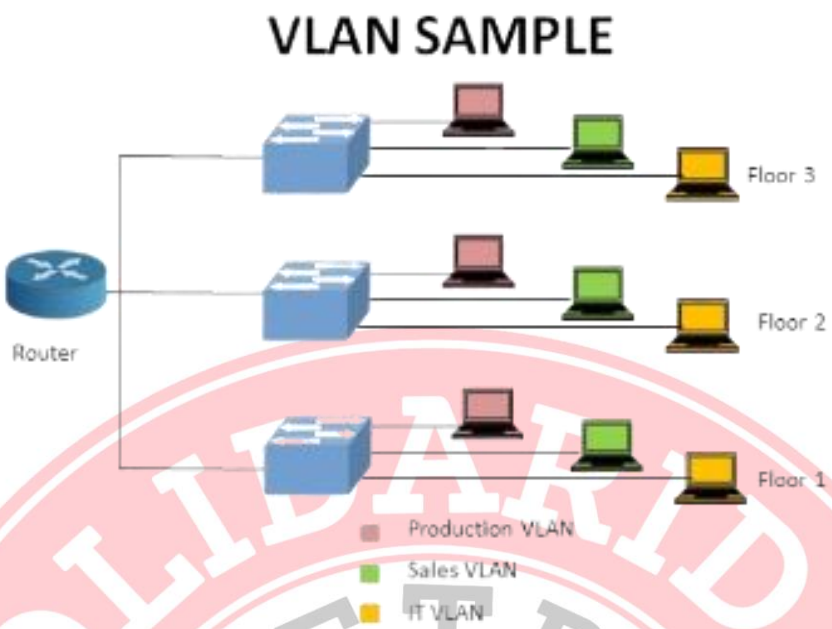
11.6.2. ARQUITECTURAS SEGURAS: VLAN, DMZ, FIREWALLS, IDS/IPS

Diseñar una arquitectura de red segura implica segmentar el tráfico, aplicar controles perimetrales y monitorizar el comportamiento de los dispositivos conectados.

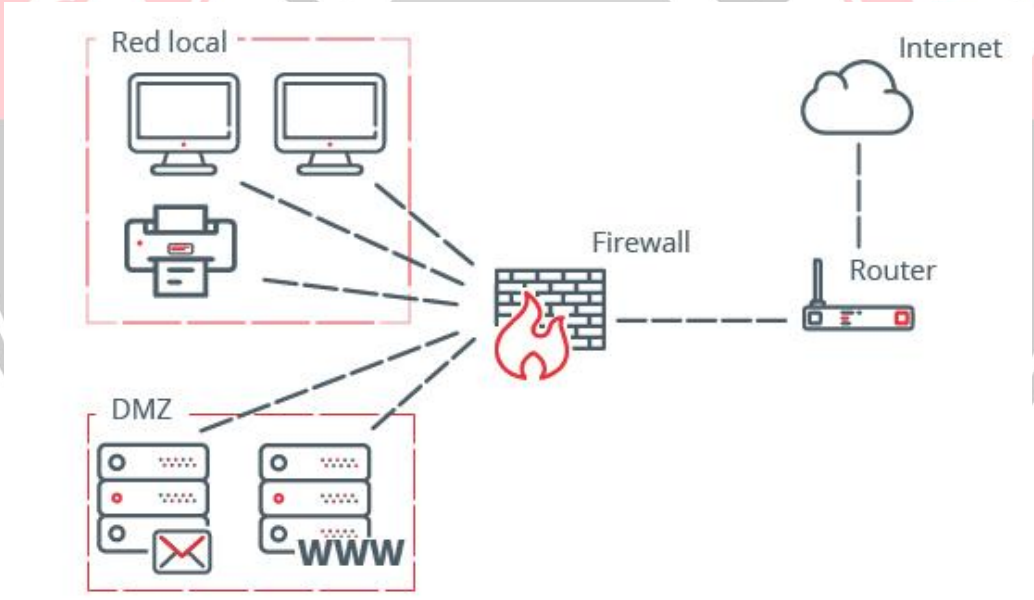
VLAN (Virtual LAN):

- Permiten dividir una red física en varias redes lógicas independientes.
- Ayudan a aislar departamentos o servicios (ej. administración, desarrollo, invitados).

- Mejoran la seguridad y el rendimiento, reduciendo el tráfico broadcast.

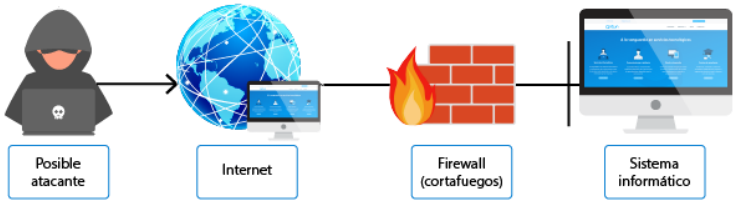


DMZ (Zona Desmilitarizada):



- Zona intermedia entre la red interna y la red externa (Internet).
- Aloja servicios accesibles públicamente (web, correo, DNS).
- Se separa del resto de la red mediante firewalls, evitando que un ataque desde fuera comprometa la red interna.

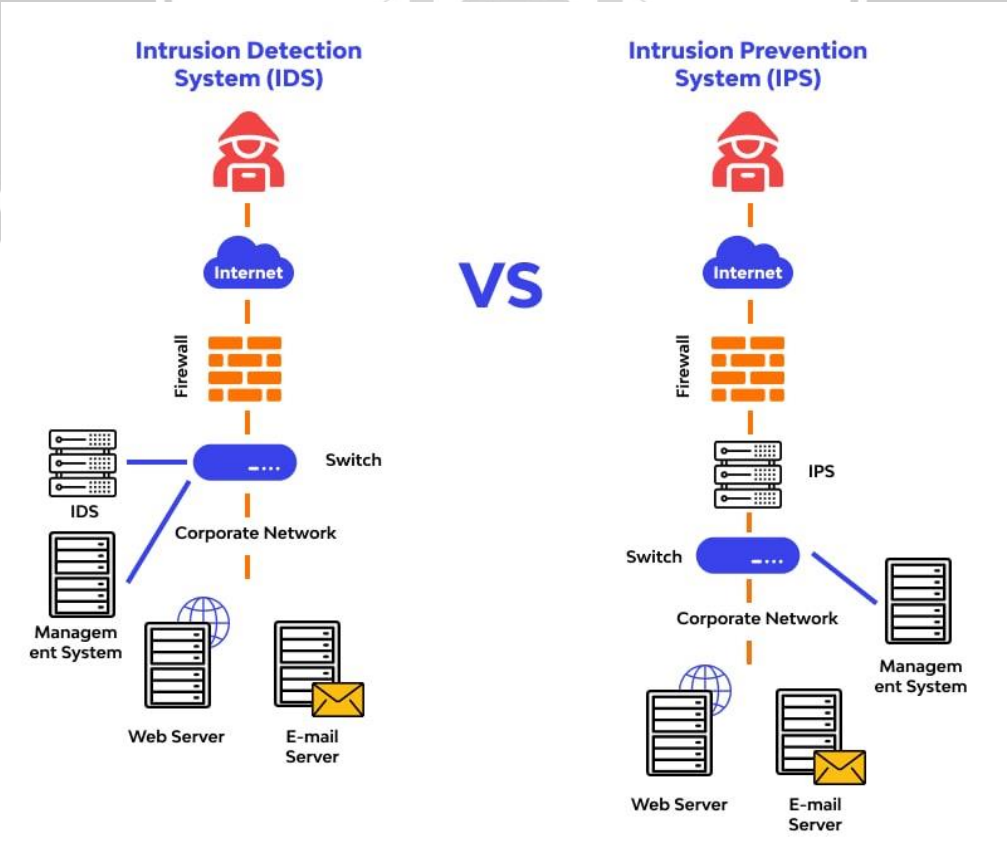
Firewalls (cortafuegos):



- Dispositivos o software que filtran el tráfico según reglas definidas.
- Tipos:
  - **Firewalls de red**: controlan el tráfico entre redes.
  - **Firewalls de host**: instalados en equipos individuales.
- Pueden funcionar como **filtrado de paquetes**, **stateful inspection**, o **proxy**.

IDS (Intrusion Detection System) / IPS (Intrusion Prevention System):

- **IDS**: detectan comportamientos anómalos o patrones de ataque (no bloquean).
- **IPS**: además de detectar, actúan bloqueando el tráfico sospechoso.
- Ejemplos: Snort, Suricata, Zeek (IDS); Cisco Firepower, Palo Alto, Fortinet (IPS).



Topología segura recomendada:

```
css
[Internet] ↔ [Firewall externo] ↔ [DMZ con servidores públicos] ↔ [Firewall interno] ↔ [Red interna (VLANs)]
```

11.6.3. CIFRADO DE COMUNICACIONES: VPN, SSL/TLS, IPSEC

El **cifrado de las comunicaciones** garantiza la confidencialidad e integridad de los datos transmitidos a través de redes, especialmente cuando viajan por Internet o redes inseguras.

VPN (Red Privada Virtual):

- Crea un **túnel cifrado** entre dos puntos sobre una red pública.
- Utilizada para acceder a redes corporativas de forma segura desde ubicaciones remotas.
- Tipos comunes:
  - **VPN de acceso remoto**: conecta a usuarios externos.
  - **VPN sitio a sitio**: conecta dos sedes u oficinas.
- Protocolos usados: **IPsec**, **SSL**, **L2TP**, **OpenVPN**, **WireGuard**.

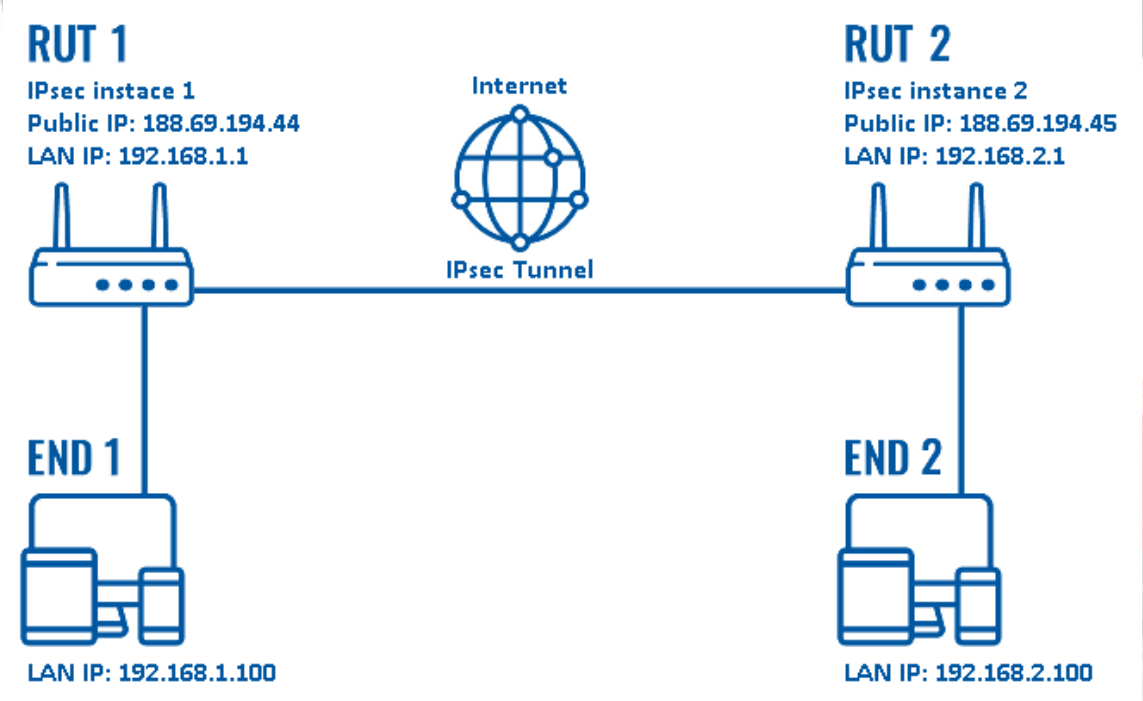
SSL/TLS (Secure Sockets Layer / Transport Layer Security):

- Protocolos criptográficos utilizados en navegadores, correo, FTP, etc.
- Garantizan **cifrado, autenticación y verificación de integridad**.
- Identificados por el "https://" y el candado en la barra del navegador.
- TLS ha reemplazado completamente a SSL (por vulnerabilidades en SSL).

Feature	SSL	TLS
Stands For	Secure Sockets Layer	Transport Layer Security
Purpose	To provide secure communication over the internet	To provide secure communication over the internet, replacing SSL
Version	SSL 3.0	TLS 1.0 and higher
Encryption Strength	40-bit and 128-bit encryption	Up to 256-bit encryption
Authentication	Server-only authentication	Server and client authentication
Handshake	Two-step handshake process	Three-step handshake process
Vulnerabilities	SSL 3.0 is vulnerable to POODLE and BEAST attacks	TLS 1.0 is vulnerable to the POODLE attack

IPsec (Internet Protocol Security):

- Conjunto de protocolos que protege el tráfico IP cifrándolo y autenticándolo.
- Se implementa a nivel de red (capa 3 del modelo OSI).
- Utilizado principalmente en VPNs.
- Modos de operación:
  - **Transporte**: solo cifra la carga útil del paquete.
  - **Túnel**: cifra todo el paquete IP original (más seguro).



Resumen comparativo:

Protocolo	Capa del modelo OSI	Uso principal	Cifrado extremo a extremo
SSL/TLS	Capa 7 (Aplicación)	Navegación, correo, etc.	Sí
IPsec	Capa 3 (Red)	VPN, comunicaciones IP	Sí
VPN	Multicapa (depende del protocolo)	Acceso remoto y redes privadas	Sí

11.6.4. SEGURIDAD EN REDES INDUSTRIALES, CCTV Y DOMÓTICA

Con el avance del IoT y la automatización, la ciberseguridad ya no se limita a redes informáticas tradicionales. También debe aplicarse en redes **industriales**, sistemas de videovigilancia (**CCTV**) y soluciones **domóticas**.

Redes industriales (ICS/SCADA):

- Controlan procesos automatizados en fábricas, infraestructuras críticas, energía, transporte, etc.
- Protocolos específicos: **Modbus**, **DNP3**, **Profinet**, **OPC**.
- Desafíos:
  - Equipos antiguos con escasa capacidad de actualización.
  - Falta de cifrado o autenticación en protocolos.
  - Prioridad operativa sobre la seguridad (tiempo real).
- Medidas de protección:
  - Segmentación de red estricta (air gap o firewalls).
  - Supervisión de anomalías con IDS industrial (ej. Nozomi, Dragos).
  - Actualización controlada de firmware y control físico de acceso.

CCTV (videovigilancia):

- Los sistemas modernos IP pueden ser vulnerables a accesos remotos.
- Riesgos: espionaje, acceso no autorizado, manipulación de grabaciones.
- Buenas prácticas:
  - Cambiar credenciales por defecto.
  - Cifrar transmisiones de vídeo.

- Aislar el sistema de videovigilancia del resto de la red.
- Actualizar firmware de cámaras y grabadores.

Domótica y dispositivos IoT:

- Riesgos: dispositivos inseguros, contraseñas por defecto, firmware sin soporte.
- Ejemplos de vulnerabilidades:
  - Cerraduras inteligentes, asistentes de voz, sensores de presencia, enchufes Wi-Fi.
- Recomendaciones:
  - Uso de redes separadas (VLANs para IoT).
  - Desactivación de servicios innecesarios (UPnP, acceso remoto).
  - Actualización regular del firmware y uso de contraseñas robustas.

11.7. SEGURIDAD EN INTERNET Y EN LA NUBE

En un mundo cada vez más interconectado, la seguridad en Internet y en los servicios en la nube es esencial para proteger los datos personales, profesionales y empresariales. Las amenazas en estos entornos pueden tener gran impacto si no se gestionan adecuadamente.

7.1. Riesgos en navegación web y correo electrónico

La navegación por Internet y el uso del correo electrónico son dos de los principales vectores de ataque en ciberseguridad:

Principales riesgos:

- **Phishing**: correos que suplantan identidades para robar credenciales.
- **Malware**: archivos adjuntos o enlaces maliciosos.
- **Sitios fraudulentos**: imitación de páginas web legítimas.
- **Drive-by-download**: descarga automática de malware al visitar sitios web comprometidos.
- **Exploit kits**: ataques automáticos aprovechando vulnerabilidades del navegador o plugins.

Buenas prácticas:

- No hacer clic en enlaces sospechosos.
- No descargar archivos de fuentes no verificadas.

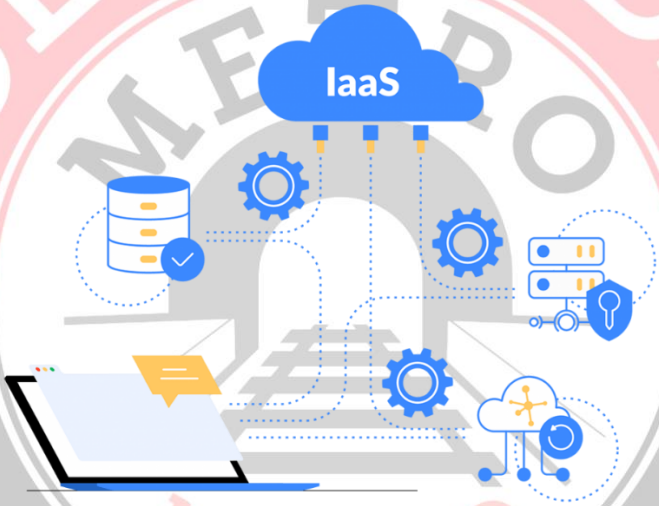
- Verificar el dominio de los remitentes.
- Usar extensiones de navegador de seguridad (HTTPS Everywhere, uBlock Origin).
- Activar filtros antiphishing y antivirus en el navegador y el correo.

11.7.1. PROTECCIÓN EN SERVICIOS EN LA NUBE: IAAS, PAAS, SAAS

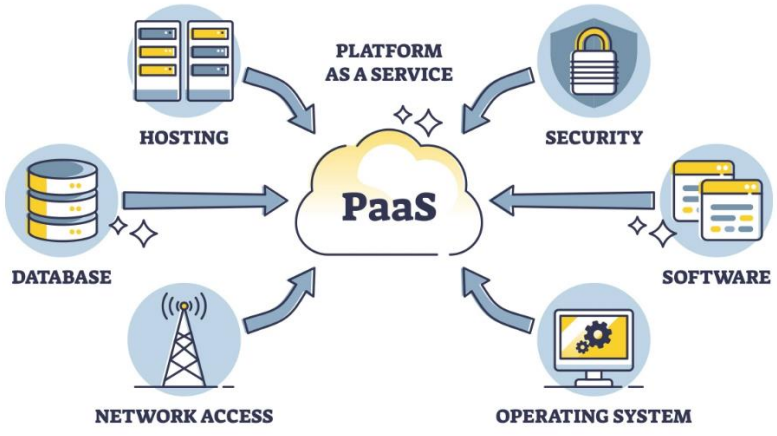
Los servicios en la nube ofrecen flexibilidad y escalabilidad, pero también introducen riesgos específicos:

Modelos de servicio:

- **IaaS (Infrastructure as a Service)**: el usuario gestiona el sistema operativo, aplicaciones y datos (ej. AWS EC2, Azure VM).



- **PaaS (Platform as a Service)**: el proveedor gestiona la infraestructura y el usuario solo sus aplicaciones (ej. Google App Engine).



- **SaaS (Software as a Service)**: el proveedor gestiona todo (ej. Gmail, Microsoft 365).

Riesgos comunes:

- Pérdida o robo de datos.
- Accesos indebidos por mala configuración.
- Falta de cifrado.
- Dependencia del proveedor (lock-in).

Medidas de protección:

- Configurar correctamente los permisos de acceso.
- Usar cifrado de datos en tránsito y en reposo.
- Activar autenticación multifactor.
- Revisar acuerdos de nivel de servicio (SLA).
- Realizar copias de seguridad fuera del entorno del proveedor.

11.7.2. SEGURIDAD EN REDES SOCIALES Y DISPOSITIVOS MÓVILES

El uso generalizado de redes sociales y dispositivos móviles conlleva nuevos vectores de ataque:

En redes sociales:

- Suplantación de identidad.
- Robo de datos personales.
- Enlaces maliciosos compartidos por contactos comprometidos.

En dispositivos móviles:

- Instalación de aplicaciones maliciosas.
- Phishing por SMS (smishing).
- Intercepción en redes Wi-Fi públicas.

Recomendaciones:

- Configurar adecuadamente la privacidad del perfil.
- No compartir datos sensibles públicamente.
- Instalar aplicaciones solo desde tiendas oficiales.
- Usar contraseñas robustas y activar biometría.
- Evitar redes Wi-Fi abiertas o usar VPN.

11.7.3. PRIVACIDAD Y REPUTACIÓN DIGITAL

La **privacidad digital** es el derecho a controlar qué información compartimos y con quién. La **reputación digital** es la imagen pública que proyectamos a través de nuestra actividad en línea.

Amenazas a la privacidad:

- Recopilación masiva de datos por plataformas y apps.
- Fugas de información personal.
- Seguimiento mediante cookies, scripts y trackers.

Protección de la privacidad:

- Revisar permisos de apps y redes sociales.

- Usar navegadores centrados en la privacidad (Brave, Firefox).
- Utilizar motores de búsqueda privados (DuckDuckGo).
- Configurar correctamente cookies y extensiones anti-tracking.

Reputación digital:

- Comentarios, publicaciones y fotos pueden afectar a nivel personal o profesional.
- Es difícil eliminar contenido una vez publicado.
- Importancia de la huella digital en procesos de selección y relaciones laborales.

Consejos:

- Pensar antes de publicar.
- Usar identidades diferenciadas si es necesario.
- Monitorizar nuestra presencia online con buscadores y alertas.
- Solicitar la eliminación de contenido según el derecho al olvido (RGPD).

11.8. COPIAS DE SEGURIDAD Y PLANES DE RECUPERACIÓN

Las copias de seguridad y los planes de recuperación son elementos clave en cualquier estrategia de ciberseguridad. Garantizan la continuidad de la actividad frente a incidentes como fallos del sistema, ciberataques o desastres naturales.

11.8.1. TIPOS DE BACKUP: COMPLETO, INCREMENTAL, DIFERENCIAL, CONTINUO

Copia de seguridad completa:

- Copia todos los archivos seleccionados cada vez.
- Mayor uso de espacio y tiempo.
- Simplifica la restauración (solo se necesita una copia).

Copia incremental:

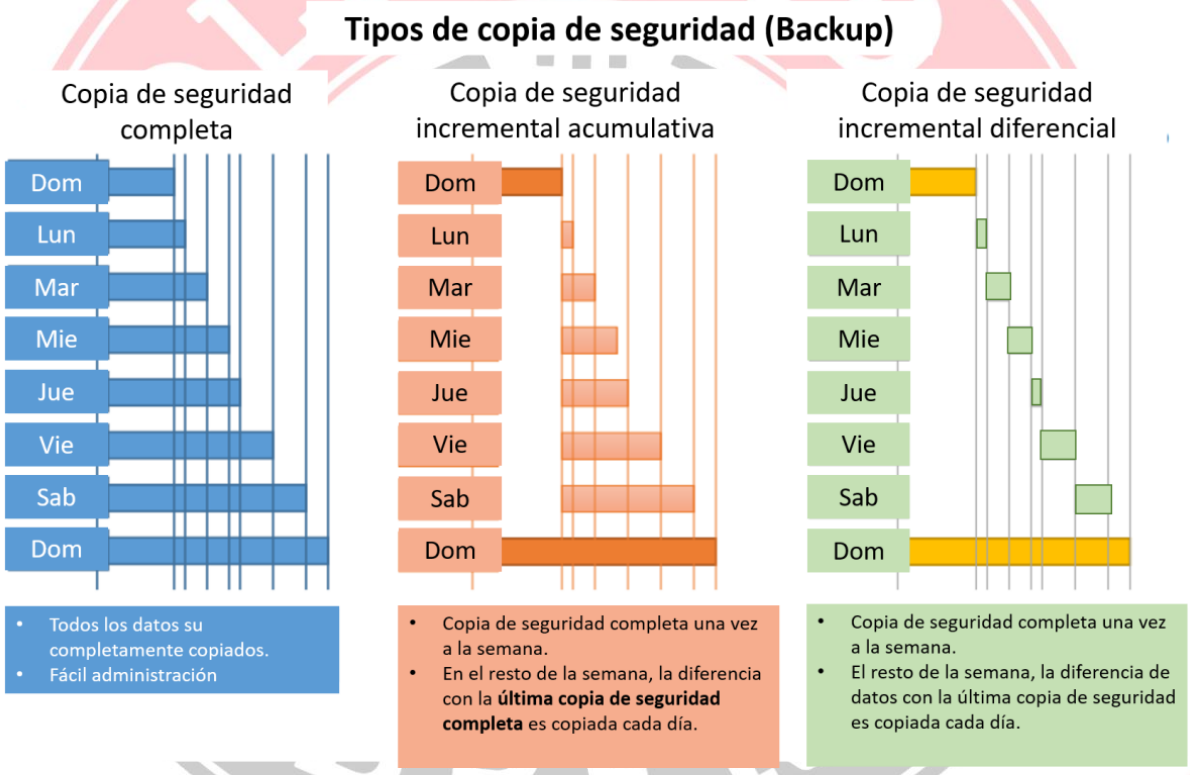
- Copia solo los archivos modificados desde la última copia (completa o incremental).
- Requiere menos espacio.
- Restauración más lenta, necesita todas las copias incrementales desde la última completa.

Copia diferencial:

- Copia los archivos modificados desde la última copia completa.
- Más rápida que la completa y más lenta que la incremental.
- Restauración más sencilla que la incremental.

Copia continua (CDP - Continuous Data Protection):

- Guarda los cambios en tiempo real o casi real.
- Ideal para entornos críticos.
- Mayor complejidad y coste.



11.8.2. HERRAMIENTAS DE BACKUP LOCALES Y EN LA NUBE

Backup local:

- Se realiza en discos duros, NAS, cintas o servidores físicos.
- Ventajas: rapidez de acceso, control físico de los datos.
- Inconvenientes: riesgo ante incendios, robos, fallos físicos.

Backup en la nube:

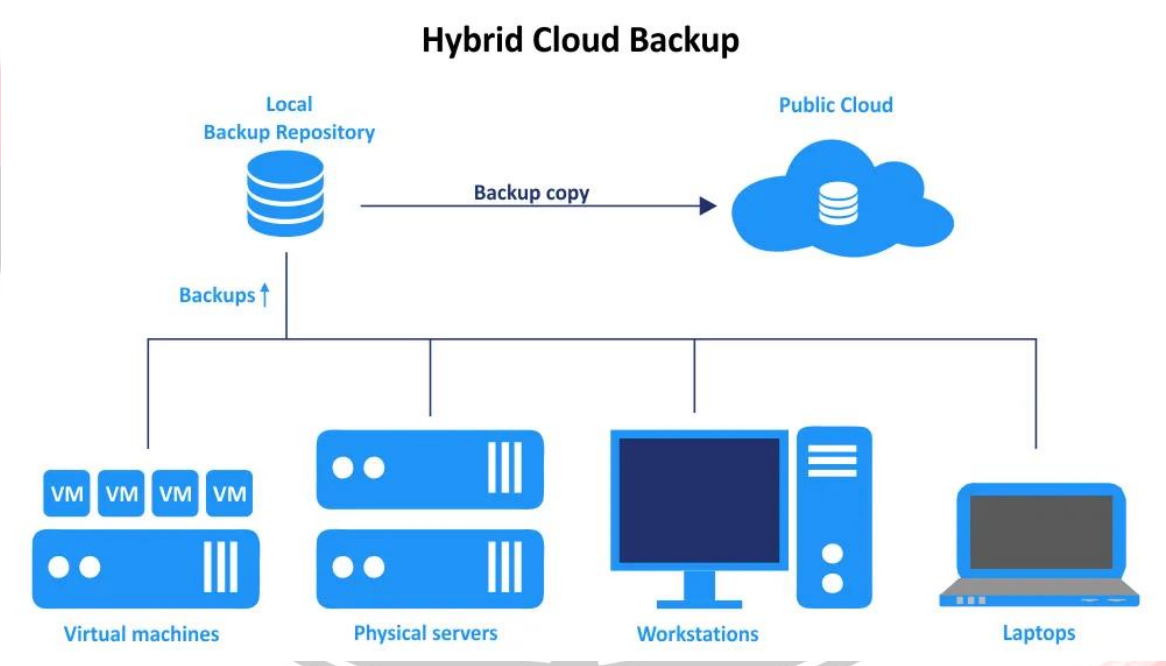
- Se almacena en servidores remotos gestionados por proveedores externos.
- Ventajas: escalabilidad, accesibilidad desde cualquier lugar, protección geográfica.
- Inconvenientes: dependencia del proveedor y de la conexión a Internet.

Herramientas comunes:

- **Locales**: Veeam, Acronis, Cobian Backup, Bacula.
- **En la nube**: Google Drive, Microsoft OneDrive, Amazon S3, Dropbox Backup.
- **Híbridas**: combinan ambos enfoques para mayor resiliencia.

Buenas prácticas:

- Aplicar la regla del **3-2-1**: 3 copias, 2 medios diferentes, 1 fuera del sitio.
- Verificar periódicamente que las copias se han realizado correctamente.



11.8.3. PLANES DE RECUPERACIÓN ANTE DESASTRES (DRP) Y CONTINUIDAD DE NEGOCIO (BCP)

DRP (Disaster Recovery Plan):

- Documento que define cómo recuperar los sistemas tras un desastre.

- Incluye responsables, procedimientos técnicos, tiempos de recuperación (RTO) y puntos de recuperación (RPO).

BCP (Business Continuity Plan):

- Abarca todos los aspectos críticos para continuar con la actividad empresarial tras una crisis.
- Más amplio que el DRP: incluye personal, instalaciones, proveedores, procesos esenciales.

Elementos clave:

- Evaluación de riesgos y análisis de impacto (BIA).
- Identificación de activos críticos.
- Procedimientos de emergencia.
- Comunicación interna y externa.
- Pruebas y actualizaciones periódicas del plan.

11.8.4. PRUEBAS PERIÓDICAS DE RESTAURACIÓN

Tener copias de seguridad sin verificar su funcionamiento es un riesgo. Por ello, se deben realizar **pruebas periódicas de restauración** para garantizar que los datos pueden recuperarse correctamente cuando sea necesario.

Tipos de pruebas:

- **Pruebas completas**: recuperación total de un sistema.
- **Pruebas parciales**: restauración de archivos concretos.
- **Simulacros**: recuperación en condiciones realistas, incluyendo personal y procedimientos.

Frecuencia recomendada:

- Al menos una vez al año, o tras cambios importantes.

Ventajas:

- Detectar fallos en los procedimientos de backup.
- Comprobar integridad de los datos respaldados.
- Medir tiempos reales de recuperación.

Errores comunes:

- No probar backups cifrados.
- No documentar los resultados de las pruebas.
- No incluir aplicaciones y configuraciones junto con los datos.

Una política de backup y recuperación bien implementada es una de las mejores defensas contra pérdidas de información y paradas de servicio inesperadas.

11.9. HERRAMIENTAS DE SEGURIDAD Y ANÁLISIS FORENSE

Las herramientas de seguridad y análisis forense permiten prevenir, detectar, analizar y responder ante incidentes de ciberseguridad. Forman parte del arsenal necesario para proteger los sistemas informáticos y garantizar la trazabilidad de los eventos.

11.9.1. ANTIVIRUS, ANTIMALWARE Y CORTAFUEGOS

Antivirus y antimalware:

- Detectan, bloquean y eliminan software malicioso (virus, troyanos, spyware, ransomware...).
- Utilizan bases de datos de firmas y técnicas heurísticas o basadas en comportamiento.
- Algunos productos destacados: Windows Defender, Avast, Kaspersky, Bitdefender, Malwarebytes.

Características clave:

- Análisis en tiempo real y bajo demanda.
- Cuarentena de archivos sospechosos.
- Actualizaciones frecuentes de firmas.

Cortafuegos (firewalls):

- Filtran el tráfico entrante y saliente según reglas predefinidas.
- Tipos:
  - **De red**: protegen toda la red (hardware o software).
  - **De host**: instalados en un equipo específico.
  - **Personales**: en ordenadores individuales (ej. Windows Firewall).

Ventajas combinadas:

- Preven el acceso no autorizado.
- Detectan y aíslan amenazas.
- Complementan otras capas de seguridad.

11.9.2. HERRAMIENTAS DE ESCANEO Y DETECCIÓN: NMAP, NESSUS, WIRESHARK

Nmap:

- Herramienta de código abierto para escaneo de redes y detección de puertos.
- Utilizada para identificar dispositivos, servicios activos, sistemas operativos, firewalls, etc.
- Comando típico: *nmap -sS -A 192.168.1.1*

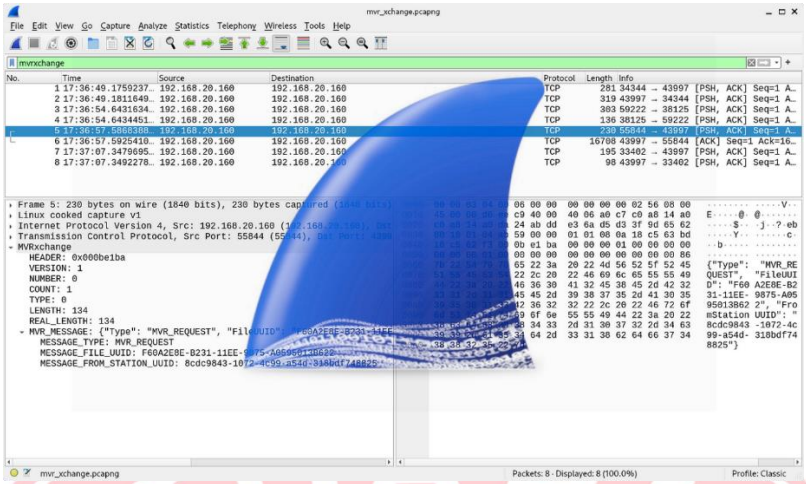
Nessus:

- Escáner de vulnerabilidades profesional.
- Detecta configuraciones erróneas, software obsoleto y fallos de seguridad.
- Genera informes detallados con niveles de criticidad y recomendaciones.

Wireshark:

- Analizador de protocolos de red.
- Captura y muestra tráfico en tiempo real.
- Permite estudiar conexiones HTTP, DNS, FTP, SSH, etc.

- Muy útil para análisis forense y resolución de problemas de red.



Otras herramientas destacadas:

- **Metasploit**: pruebas de penetración.
- **OpenVAS**: escaneo de vulnerabilidades de código abierto.
- **OSSEC / Wazuh**: monitorización de integridad y detección de intrusiones.

11.9.3. ANÁLISIS FORENSE DIGITAL: ADQUISICIÓN, PRESERVACIÓN, ANÁLISIS Y PRESENTACIÓN DE PRUEBAS

El **análisis forense digital** es el proceso mediante el cual se identifican, preservan, analizan y presentan evidencias electrónicas de manera legalmente válida.

Fases del análisis forense:

1. **Adquisición**:
   - Obtención de las evidencias sin alterarlas.
   - Se realiza una copia bit a bit del sistema o dispositivo.
   - Se usan herramientas como FTK Imager, dd, EnCase.
2. **Preservación**:
   - Garantiza que los datos no sean modificados durante el análisis.
   - Uso de hash (MD5, SHA-256) para verificar la integridad de las imágenes.
   - Documentación detallada de cada paso.
3. **Análisis**:
   - Búsqueda de archivos eliminados, rastros de malware, registros de actividad.

- Herramientas: Autopsy, X-Ways Forensics, Volatility (memoria RAM).

4. **Presentación**:
   - Elaboración de un informe técnico.
   - Exposición clara y comprensible para audiencias técnicas y legales.
   - Puede servir como prueba judicial en casos de ciberdelitos.

Principios clave:

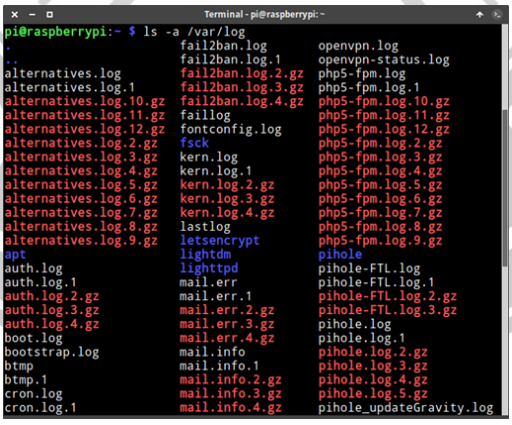
- Cadena de custodia.
- Reproducibilidad.
- Imparcialidad.

11.9.4. TÉCNICAS DE TRAZABILIDAD, REGISTRO Y AUDITORÍA

La **trazabilidad** y el **registro de eventos** son esenciales para detectar incidentes, investigar problemas y demostrar cumplimiento normativo.

Sistemas de registro (logs):

- Almacenan información sobre accesos, errores, cambios de configuración, tráfico de red, etc.
- Deben estar protegidos contra modificaciones.
- Es recomendable usar un servidor centralizado de logs.



Tipos de logs importantes:

- Sistema operativo: inicio de sesión, errores del sistema.
- Aplicaciones: accesos, fallos, actualizaciones.
- Red: conexiones entrantes/salientes, firewall.

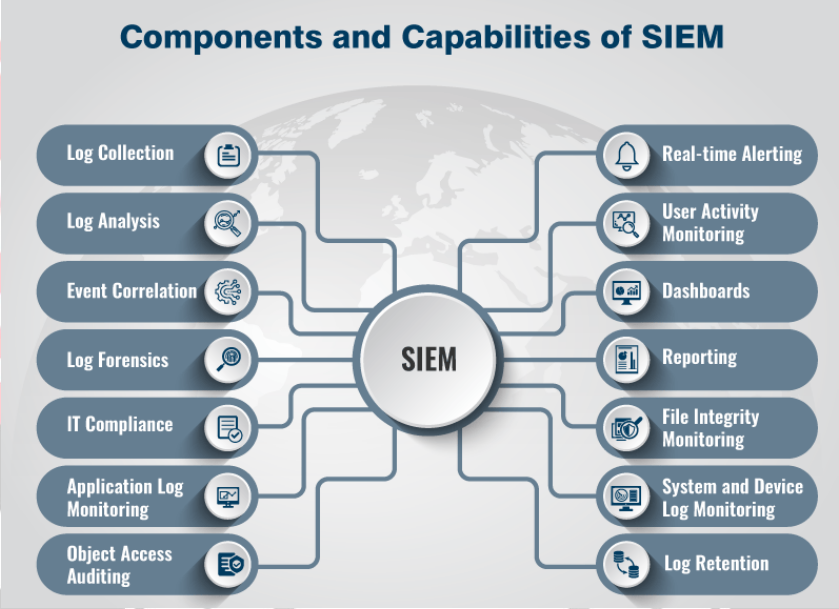
- Seguridad: eventos de autenticación, modificaciones de permisos.

Auditoría:

- Proceso de revisión sistemática de los registros y configuraciones.
- Puede ser manual o automatizada.
- Ayuda a detectar accesos indebidos, malware o malas prácticas.

Herramientas de auditoría y análisis:

- **SIEM (Security Information and Event Management)**: Splunk, AlienVault, Graylog, ELK Stack.



- **Syslog, journald (Linux) / Event Viewer (Windows)** para revisión local.

Buenas prácticas:

- Activar registros detallados en sistemas y aplicaciones críticas.
- Establecer políticas de retención de logs.
- Revisar periódicamente los registros.
- Correlacionar eventos para detectar patrones anómalos.

Una trazabilidad adecuada es clave tanto para la prevención de incidentes como para su análisis posterior en caso de que ocurran.

11.10. CONCIENCIACIÓN Y BUENAS PRÁCTICAS DE SEGURIDAD

La tecnología por sí sola no basta para garantizar la seguridad informática. El factor humano es determinante. La concienciación, formación y buenas prácticas adoptadas por los usuarios son clave para prevenir incidentes de seguridad.

11.10.1. FORMACIÓN DE USUARIOS Y CONCIENCIACIÓN INTERNA

La formación en ciberseguridad debe ser continua y adaptada al nivel técnico del personal. Todos los miembros de una organización, desde el personal técnico hasta los usuarios generales, deben estar informados de los riesgos y su papel en la prevención.

Objetivos de la formación:

- Reconocer amenazas como el phishing o el malware.
- Fomentar el uso de contraseñas seguras.
- Conocer las políticas internas de seguridad.
- Saber cómo actuar ante un incidente de seguridad.

Medios para concienciar:

- Cursos presenciales o en línea.
- Boletines internos y campañas de sensibilización.
- Cartelería, infografías y vídeos educativos.
- Jornadas de ciberseguridad y seminarios.

Beneficios:

- Reducción del número de incidentes.
- Mayor detección temprana de amenazas.
- Implicación del personal en la protección activa.

11.10.2. USO SEGURO DE DISPOSITIVOS PERSONALES (BYOD)

El modelo **BYOD (Bring Your Own Device)** permite a los empleados usar sus propios dispositivos (móviles, portátiles, tablets) para trabajar. Aunque aporta flexibilidad, también plantea serios riesgos de seguridad.

Riesgos asociados:

- Falta de control sobre el dispositivo.
- Acceso a datos corporativos desde entornos inseguros.
- Mezcla de datos personales y laborales.
- Mayor probabilidad de pérdida o robo del dispositivo.

Medidas de seguridad recomendadas:

- Uso obligatorio de cifrado y contraseñas.
- Instalación de antivirus y firewall personal.
- Control de acceso mediante VPN o autenticación multifactor.
- Políticas de borrado remoto en caso de pérdida.
- Segmentación de redes para dispositivos BYOD.

Política BYOD clara:

- Reglas específicas sobre qué dispositivos y apps están permitidos.
- Consentimiento del usuario para instalar controles mínimos de seguridad.
- Revisión y auditoría periódica de los dispositivos.

11.10.3. SIMULACROS Y TEST DE PENETRACIÓN INTERNOS

Los **simulacros de seguridad** y **test de penetración (pentest)** son ejercicios proactivos que permiten evaluar el nivel de resistencia de la organización frente a amenazas reales.

Simulacros:

- Ejercicios planificados que imitan incidentes de seguridad (ransomware, fuga de datos...).
- Involucran a personal técnico y no técnico.
- Evalúan capacidad de respuesta, comunicación interna y procedimientos de recuperación.

Pentest internos:

- Ataques controlados realizados desde dentro de la red.
- Identifican vulnerabilidades técnicas y errores de configuración.

- Herramientas: Metasploit, Burp Suite, Nessus.

Beneficios:

- Mejora de los tiempos de reacción.
- Detección de fallos ocultos.
- Fomento de la cultura de prevención.

Recomendaciones:

- Realizar simulacros al menos una vez al año.
- Documentar resultados y planificar mejoras.
- No usar entornos de producción sin controles adecuados.

11.10.4. CULTURA DE CIBERSEGURIDAD EN LA ORGANIZACIÓN

Crear una **cultura de ciberseguridad** implica que todos los miembros de la organización, independientemente de su función, comprendan la importancia de la seguridad y actúen en consecuencia.

Pilares de una cultura sólida:

- **Liderazgo comprometido**: directivos que apoyan e impulsan las medidas de seguridad.
- **Formación constante**: programas adaptados a todos los niveles.
- **Comunicación clara**: canales internos para informar y reportar incidentes.
- **Reconocimiento y motivación**: valorar el cumplimiento y las buenas prácticas.

Estrategias para fortalecer la cultura:

- Incorporar la seguridad en los procesos y decisiones del día a día.
- Medir y reportar métricas de seguridad.
- Incluir la ciberseguridad en el onboarding de nuevos empleados.

Una organización con una cultura fuerte en ciberseguridad será más resiliente, reaccionará más rápido ante incidentes y mantendrá protegidos sus activos digitales a largo plazo.

Uso de contenidos, fuentes y derechos de autor

1. Finalidad del presente material

El presente documento forma parte de un material didáctico elaborado exclusivamente con fines educativos y sin ánimo de lucro. Está destinado a su libre distribución para ser utilizado en contextos formativos, para la enseñanza y el aprendizaje de contenidos técnicos.

No está permitido su uso con fines comerciales.

---

2. Uso de fuentes externas

Para el desarrollo de este temario se han utilizado diversas fuentes de información, tales como:

- Manuales técnicos y libros especializados
- Documentación institucional (Ministerio de Educación, BOE, INTEF, etc.)
- Sitios web de acceso público (Wikipedia, blogs técnicos, foros especializados)
- Artículos académicos y divulgativos
- Imágenes y gráficos procedentes de bancos de imágenes libres o de dominio público

Siempre que ha sido posible, respetando el derecho moral de autoría.

---

3. Derecho de cita y uso educativo

De acuerdo con lo dispuesto en la **Ley de Propiedad Intelectual (RDL 1/1996)** en su artículo 32, se permite la inclusión de fragmentos de obras ajenas en materiales educativos **cuando se cumplan los siguientes requisitos**:

- La inclusión tiene un **propósito de ilustración con fines educativos**.
- Se utiliza **solo la parte necesaria** del contenido, no la obra completa.
- El uso se realiza **sin fines lucrativos**.

Ver uso de contenidos, fuentes y derechos de autor en la última página.

Este temario respeta estos principios en su totalidad. Cuando se han utilizado contenidos protegidos por derechos de autor, se ha hecho conforme a los límites legalmente establecidos o mediante el uso de licencias abiertas.

---

4. Contenido con licencias abiertas

Algunas imágenes, gráficos o textos utilizados en este documento se encuentran bajo licencias de uso libre (Creative Commons, dominio público u otras licencias abiertas). Estas licencias permiten su uso y adaptación siempre que se respete la condición de atribución cuando corresponda.

Por ejemplo, algunas imágenes han sido extraídas de:

- Wikimedia Commons
- Pixabay.com
- Unsplash.com
- Documentación oficial y normativa del Ministerio de Educación

---

5. Peticiones de modificación o retirada

Si algún autor, creador o entidad considera que el uso de su contenido no ha sido adecuado o desea solicitar su retirada o modificación, puede comunicarse con Solidaridad Obrera. Se revisará la situación y se aplicarán los cambios pertinentes con la mayor brevedad posible.

---

6. Agradecimientos

Se agradece a todos los autores, instituciones y plataformas que comparten contenido educativo de libre acceso, facilitando el aprendizaje y la formación técnica de calidad para todos.

Ver uso de contenidos, fuentes y derechos de autor en la última página.