**Red:** una red en informática, es un grupo de dispositivos conectados, como puede ser una computadora, teléfonos móviles y distintos dispositivos inteligentes. Los dispositivos de una red pueden comunicarse entre sí a través de cables de red o conexiones inalámbricas, además se pueden comunicar con redes de otras ubicaciones

Los dispositivos necesitan encontrarse en una red para establecer comunicaciones. Estos dispositivos utilizarán direcciones únicas, o identificadores, para localizarse entre sí. Las direcciones garantizarán que las comunicaciones se produzcan con el dispositivo correcto. Se denominan direcciones IP y MAC.

Los dispositivos pueden comunicarse en dos tipos de redes: una red de área local, también conocida como LAN, y una red de área extensa, también conocida como WAN.

La seguridad de red es importante porque queremos asegurarnos de que nuestros sistemas de red sean seguros y resistentes para poder defendernos de los piratas informáticos malintencionados, y de que tenemos la capacidad de proteger los datos de nuestros usuarios.

# Dispositivos de red

Los dispositivos de red mantienen información y servicios para los usuarios de una red. Estos dispositivos se conectan a través de conexiones cableadas e inalámbricas. Tras establecer una conexión con la red, los dispositivos envían paquetes de datos. Los paquetes de datos proporcionan información sobre el origen y el destino de los datos. Así es como se envía y recibe la información a través de los distintos dispositivos de una red.

La red es la infraestructura general que permite a los dispositivos comunicarse entre sí. Los dispositivos de red son vehículos especializados, como enrutadores y conmutadores, que gestionan lo que se envía y recibe a través de la red. Además, dispositivos como ordenadores y teléfonos se conectan a la red a través de dispositivos de red.

**Concentrador:** dispositivo de red que emite información a todos los dispositivos de red, piénselo como en una torre de radio que emite una señal a cualquier radio sintonizada con la frecuencia correcta

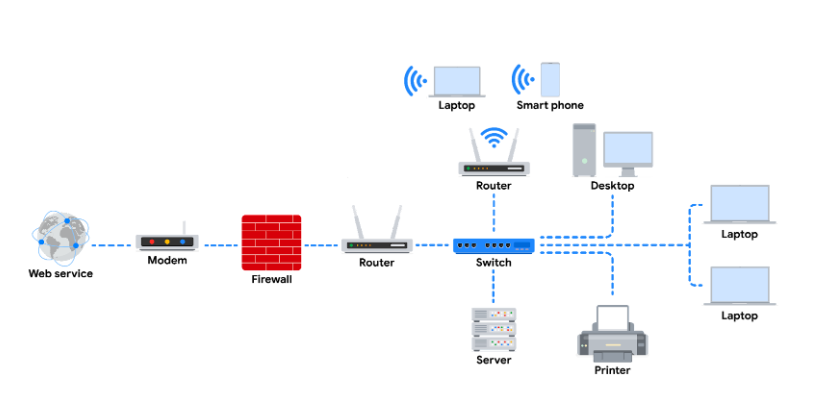
**Switch:** un conmutador o switch establece conexiones entre dispositivos específicos de una red enviando y recibiendo datos entre ellos, es mas inteligente que un concentrador ya que solo transmite datos al destino previsto, lo que los hace mas seguros y les permite controlar el flujo de trafico y mejorar el rendimiento de la red. Un conmutador reenvía paquetes entre dispositivos conectados directamente a él. Analizan la dirección de destino de cada paquete de datos y lo envían al dispositivo previsto. Los conmutadores mantienen una tabla de direcciones MAC que coteja las direcciones MAC de los dispositivos de la red con los números de puerto del conmutador y reenvía los paquetes de datos entrantes según la dirección MAC de destino. Los conmutadores forman parte de la capa de vínculo de datos en el Modelo TCP/IP.

**Router:** dispositivo de red que conecta varias redes entre si, basándose en la dirección IP de la red de destino. Los routers permiten que los dispositivos de diferentes redes se comuniquen entre sí. En el Modelo TCP/IP, los routers forman parte de la capa de red. La dirección IP de la red de destino está contenida en la cabecera IP. El router lee la información de la cabecera IP y reenvía el paquete al siguiente router en la ruta hacia el destino. Esto continúa hasta que el paquete llega a la red de destino.

**Modem:** un modem es un dispositivo que conecta el router a Internet, y lleva el acceso a Internet a la LAN

**Cortafuegos (firewall):** dispositivo de seguridad de red que supervisa el trafico hacia o desde su red, es como la primera línea de defensa. También pueden restringir el trafico de red especifico entrante y saliente, suelen situarse entre la red interna segura y controlada y los recursos de red no fiables fuera de la organización

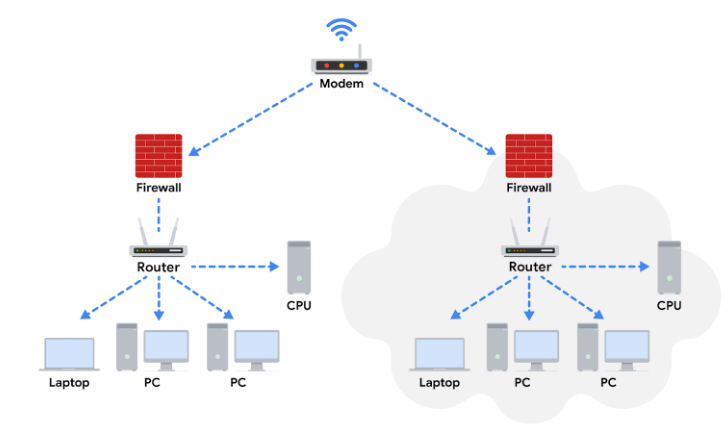
**Servidores:** proporcionan información y servicios para dispositivos



**Punto de acceso inalambrico:** envia y recibe señales digitales a través de ondas de radio creando una red inalámbrica, al punto de acceso se conecta mediante Wi-Fi. Wifi hace referencia a un conjunto de estándares que utilizan los dispositivos de redp ara comunicarse de forma inalámbrica. Los puntos de acceso inalámbricos y los dispositivos conectados a ellos utilizan protocolos Wi-Fi para enviar datos a través de ondas de radio, donde se envían a enrutadores y conmutadores y se dirigen a lo largo de la ruta hasta su destino final.



**Diagramas de red:** mapas que muestran los dispositivos de la red y como se conectan. Mediante el estudio de los mismos, los analistas de seguridad desarrollan y perfeccionan sus estrategias para proteger las arquitecturas de red



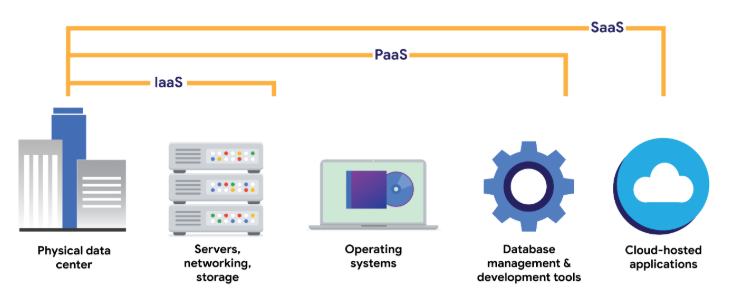
Las empresas hoy en día utilizan el modelo en la nube ya que este ayuda a ahorrar mucho dinero a la vez que les da acceso a mas recursos de red. La computación en la nube es la practica de utilizar servidores, aplicaciones y servicios de red remotos que se alojan en Internet en lugar de en dispositivos físicos locales

**Red en la nube:** conjunto de servidores u ordenadores que almacenan recursos y datos en un centro de datos remoto al que se puede acceder a través de internet. La seguridad en la nube será cada vez mas relevante para muchos profesionales de la seguridad a medida que mas organizaciones migren a los servicios en la nube. Los proveedores de servicios en la nube ofrecen computación en la nube para mantener las aplicaciones. También proporcionan análisis empresariales y web que las organizaciones pueden utilizar para supervisar su trafico web y ventas

Las empresas pueden pagar por el almacenamiento y los servicios que necesitan y consumirlos a través de la interfaz de programación de aplicaciones (API) o la consola web del CSP.

Los CSP ofrecen tres categorías principales de servicios:

1. **Software como servicio (SaaS):** se refiere a conjuntos de software operados por el CSP que una empresa puede utilizar de forma remota sin alojar el software
2. **Infraestructura como servicio (Iaas):** se refiere al uso de componentes informáticos virtuales ofrecidos por el CSP, incluyen contenedores virtuales y almacenamiento que se configuran de forma remota a través de la API o la consola web
3. **La plataforma como servicio (Paas):** hace referencia a las herramientas que los desarrolladores de aplicaciones pueden utilizar para diseñar aplicaciones personalizadas para su empresa



**Entornos de nube hibrida:** Cuando las organizaciones utilizan los servicios de un CSP además de sus ordenadores, redes y almacenamiento locales, se habla de un entorno de nube híbrida. Cuando las organizaciones utilizan más de un CSP, se denomina entorno de nubes múltiples. La gran mayoría de las organizaciones utilizan entornos de nube híbrida para reducir costes y mantener el control sobre los recursos de red.

**Redes definidas por software:** están formadas por dispositivos y servicios de red virtuales

La computación en la nube y las redes definidas por software, ofrecen 3 benificios destacados:

1. **Confiabilidad:** la computación en la nube permite a los empleados y clientes a acceder a los recursos que necesitan de forma constante y con una interrupción mínima
2. **Costes:** como los CSP disponen de centros de datos tan grandes, pueden ofrecer dispositivos y servicios virtuales a una fracción del coste que suponen para las empresas instalar, parchear, actualizar y gestionar ellas mismas los componentes y el software
3. **Escalabilidad:** los cambios que necesita la empresa en caso de aumentar sus necesidades empresariales o disminuirse, son mucho mas rápidos gracias a esto

La comunicación a través de una red se produce cuando los datos se transfieren de un punto a otro. Los fragmentos de datos suelen denominarse **paquetes de datos**.

Un paquete de datoses una unidad básica de información que viaja de un dispositivo a otro dentro de una red. Cuando los datos se envían de un disp. A otro a través de una red, se envían como un paquete que contiene información sobre a donde va el paquete, de donde viene y el contenido de mensaje. Contiene un encabezado que incluye la dirección del protocolo de Internet la dirección IP y la dirección MAC (media acces control) del dispositivo de destino. También incluye el numero de protocolo que indica al dispositivo receptor que hacer con la información del paquete. Luego esta el cuerpo del paquete que contiene el mensaje y por último un pie de pagina que indica al receptor que el paquete ha finalizado

El rendimiento de una red puede medirse por el **ancho de banda** que se refiere a la cantidad de datos que recibe un dispositivo por segundo, este mismo se puede calcular dividiendo la cantidad de datos por el tiempo en segundos. La *velocidad* se refiere a la velocidad que se reciben o descargan los paquetes de datos

**Sniffing:** practica de capturar e inspeccionar paquetes de datos a través de la red

**Modelo TCP/IP:** protocolos de comunicación y disp. Utilizados para comunicarse entre si a través de Internet. TCP/IP son las siglas de Protocolo de control de transmisión y Protocolo de Internet. TCP/IP es el modelo estándar utilizado para la comunicación en red. TCP es un protocolo de comunicación de Internet que permite a 2 disp. Formar una conexión y transmitir datos. El protocolo incluye un conjunto de instrucciones para organizar los datos, de forma que puedan enviarse a través de una red, también establece una conexión entre 2 disp. Y se asegura que los paquetes lleguen a su destino apropiado. El IP significa protocolo de internet. IP tiene un conjunto de estándares utilizados para enrutar y direccionar paquetes de datos a medida que viajan entre dispositivos de una red. Incluida en el protocolo de internet esta la dirección IP un poco mas adelante. Cuando se envían y reciben paquetes de datos a través de una red, se les asigna un puerto. Dentro del sistema operativo de un dispositivo de red, un puerto es una ubicación basada en software que organiza el envío y recepción de datos entre dispositivos de una red. Los puertos dividen el Tráfico de red en segmentos basados en el servicio que realizarán entre dos dispositivos. Las computadoras que envían y reciben estos segmentos de datos saben cómo priorizar y procesar estos segmentos basándose en su número de puerto. Esto es como enviar una carta a un amigo que vive en un edificio de apartamentos. El repartidor de correo no sólo sabe cómo encontrar el edificio, sino que también sabe exactamente dónde ir en el edificio para encontrar el número de apartamento donde vive su amigo. Los paquetes de datos incluyen instrucciones que indican al dispositivo receptor qué hacer con la información. Estas instrucciones vienen en forma de número de puerto. Los números de puerto permiten a las computadoras dividir el Tráfico de red y priorizar las operaciones que realizarán con los datos. Algunos números de puerto comunes son: el puerto 25, que se utiliza para el correo electrónico, el puerto 443, que se utiliza para la comunicación segura en Internet , y el puerto 20, para las transferencias de archivos de gran tamaño. Como ha aprendido en este vídeo, una gran cantidad de información e instrucciones están contenidas en paquetes de datos mientras viajan a través de una red. Este modelo cuenta con 4 capas:

1. **Capa de acceso a la red:** se ocupa de la creación de paquetes de datos y su transmisión a través de la red, lo que incluye los disp. De hardware conectados a cables físicos y conmutadores que dirigen los datos a su destino
2. **Capa de Internet:** donde se adjuntan las direcciones IP a los paquetes de datos para indicar la ubicación del emisor y el receptor, también se centra en como se conectan las redes entre si
3. **Capa de transporte:** incluye protocolos para controlar el flujo de tráfico a través de una red, estos permiten o deniegan la comunicación con otros dispositivos e incluyen información sobre el estado de conexión. Se utilizan 2 protocolos de transporte:

* *Protocolo de transmisión (TCP):* protocolo de comunicación de internet que permite que dos dispositivos formen una conexión y transmitan datos. Garantiza que los datos se transmitan de forma fiable al destino, contiene el numero de puerto del servicio de destino
* *Protocolo de Datagramas de Usuario (UDP):* protocolo no orientado a la conexión que no establece una conexión entre disp. Antes de las transmisiones. Lo utilizan aplicaciones a las que no les preocupa la fiabilidad de transmisión. os Datos enviados a través de UDP no son objeto de un seguimiento tan exhaustivo como los enviados mediante TCP. Dado que UDP no establece conexiones de red, se utiliza sobre todo para aplicaciones sensibles al rendimiento que funcionan en tiempo real, como la transmisión de vídeo.

1. **Capa de aplicación:** los protocolos determinan como los paquetes de datos interactuaran con los dispositivos receptores. Las funciones que se organizan en la capa de aplicación incluyen la transferencia de archivos y los servicios de correo electrónico. Los protocolos de la capa de aplicación determinan como interactuaran los paquetes de datos con los disp. Receptores, algunos más comunes son:

* Protocolo de transferencia de hipertexto (HTTP)
* Protocolo simple de transmisión de correo (SMTP)
* Secure Shell (SSH)
* Protocolo de transferencia de archivos (FTP)
* Sistema de nombres de dominio (DNS)

El OSI organiza visualmente los protocolos de redes en diferentes capas. Los profesionales de las redes suelen utilizar este modelo para comunicarse entre sí sobre posibles fuentes de problemas o amenazas a la seguridad cuando se producen.

El Modelo TCP/IP combina varias capas del modelo OSI. Existen muchas similitudes entre ambos Modelos. Ambos Modelos definen Estándares para las redes y dividen el proceso de comunicación de la red en diferentes capas. El Modelo TCP/IP es una versión simplificada del modelo OSI.

El *Modelo OSI* es un concepto estandarizado que describe las siete capas que utilizan los ordenadores para comunicarse y enviar datos a través de la red

**7- Capa de aplicación:** incluye procesos que implican directamente al usuario cotidiano. Esta capa incluye todos los protocolos de redes que las aplicaciones de software utilizan para conectar a un usuario a Internet. Esta característica es el rasgo identificativo de la capa de aplicación: la conexión del usuario a Internet a través de aplicaciones y solicitudes

6- **Capa de presentación:** implica la traducción y encriptación de datos para la red, añade y sustituye datos por formatos que puedan ser entendidos por las aplicaciones tanto en los sistemas emisores como en los receptores. Algunas funciones de formateo que tienen lugar en la capa 6 incluyen la encriptación, compresión y la confirmación de que el conjunto de códigos de caracteres puede ser interpretado en el sistema receptor

5- **Capa de sesión:** describe el momento en que se establece una conexión entre 2 dispositivos. Una sesión abierta permite que los dispositivos se comuniquen entre sí, los protocolos mantienen la sesión abierta mientras se transfieren los datos y la terminan una vez finalizada la transmisión. Esta capa también es responsable de actividades como la autenticación, la reconexión y el establecimiento de puntos de control durante una transferencia de datos

4- **Capa de transporte:** es responsable de la entrega de datos entre dispositivos. Esta capa también se encarga de la velocidad de transferencia de datos, del flujo de la transferencia y de dividir los datos en segmentos mas pequeños para facilitar su transporte. *Segmentación* es el proceso de dividir una gran transmisión de datos en trozos mas pequeños que puedan ser procesados por el sistema receptor. Estos segmentos tienen que volver a ensamblarse en su destino para que puedan ser procesados en la capa de sesión

3- **Capa de red:** supervisa la recepción de las tramas desde la capa de enlace de datos y las entrega al destino previsto, el cual puede encontrarse basándose en la dirección que reside en la trama de los paquetes de datos

2- **Capa de vinculo de datos:** organiza el envió y la recepción de paquetes de datos dentro de una misma red, se encuentran los conmutadores de la red local y las tarjetas de interfaz de red de los disp. Locales. Se utilizan protocolos como el protocolo de control de red (NCP), el control de enlace de datos de alto nivel (HDLC) y el protocolo de enlace de datos síncrono (SDLC)

1- **Capa física:** corresponde al hardware físico que interviene en la transmisión de red. Los concentradores, los módems y los cables y el cableado que los conectan se consideran parte de la capa física

IP son las siglas de protocolo de internet, que es una cadena única de caracteres que identifica la ubicación de un dispositivo de internet. Cada disp. En Internet tiene una IP única

Hay dos tipos de IP:

* IP Versión 4: se escriben como números de 4,1, 2 o 3 dígitos separados por un punto decimal. Estas eran utilizadas en los primeros días de Internet, pero a medida que crecía el uso, empezaron a agotarse por lo que se desarrollo IPv6. El formato del Encabezado IPv4 viene determinado por el protocolo IPv4 e incluye la información de enrutamiento IP que los dispositivos utilizan para dirigir el Paquete. El tamaño del encabezado IPv4 oscila entre 20 y 60 bytes. Los primeros 20 bytes son un conjunto fijo de información que contiene datos como la dirección IP de origen y destino, la longitud de la cabecera y la longitud total del paquete. El último conjunto de bytes puede oscilar entre 0 y 40 y está formado por el campo de opciones.  
  La longitud de la sección de Datos de un paquete IPv4 puede variar mucho en tamaño. Sin embargo, el tamaño máximo posible de un paquete IPv4 es de 65.535 bytes. Contiene el mensaje que se transfiere por Internet, como la información de un sitio web o el texto de un correo electrónico.  
  Hay 13 campos dentro del encabezado de un paquete IPv4:

1. **Version (VER):** este componente de 4 bits indica a los dispositivos receptores que protocolo esta utilizando el paquete
2. **Longitud del encabezado IP (HLEN o IHL):** es la longitud del encabezado del paquete. Este valor indica donde termina el encabezado del paquete y donde comienza la segmentación de datos
3. **Tipo de servicio (TOS):** los routers priorizan la entrega de paquetes para mantener la calidad del servicio en la red, ToS proporciona al Router esta información
4. **Longitud total:** comunica la longitud total de todo el paquete IP, en IPv4 el tamaño máximo es de 65535 bytes
5. **Identificacion:** los paquetes IPv4 pueden tener hasta 65535 bytes, pero las redes suelen tener un limite menor, por lo que los paquetes se dividen, o fragmentan en paquetes IP mas pequeño. El campo de identificación proporcioa un identificador único para todos los fragmentos del paquete original, para que puedan ser reemsamblados luego
6. **Banderas:** este campo proporciona al dispositivo de enrutamiento mas información sobre si el paquete original fue fragmentado y si hay mas fragmentos en transito
7. **Desplazamiento de fragmentación:** el campo de offset de fragmentación indica a los dispositivos de encaminamiento a que parte del paquete original pertenece el fragmento
8. **Tiempo de vida (TTL):** impide que los paquetes de datos sean reenviados por los routers indefinidamente. Contiene un contador que establece la fuente, el cual decrementa en uno a medida que pasa por cada Router a lo largo de su ruta de acceso, cuando llega a cero, el Router que tiene el paquete en ese momento lo descarta y devuelve al remitente un mensaje de error ICMP Time Exceeded
9. **Protocolo:** el campo de protocolo indica al dispositivo receptor que protocolo utilizara para la parte de datos del paquete
10. **Suma de comprobación del encabezado:** contiene una suma de comprobación que puede utilizarse para detectar la corrupción del encabezado IP en tránsito, si esta corrupto se descarta
11. **Direccion IP de origen:** la dirección del dispositivo emisor
12. **Direccion IP de destino:** dirección del dispositivo destino
13. **Opciones:** permite aplicar opciones de seguridad al paquete si el valor HLEN es superior a cinco

* IP versión 6: se componen de 32 caracteres, debito a esto, permitirá que mas dispositivos se conecten a Internet sin quedarse sin direcciones tan rápido como en IPv4

Las direcciones IP pueden ser publicas o privadas, el proveedor de Internet asigna una dirección IP publica linkeada a su ubicación geográfica. Cuando se interrumpe la comunicación de red desde tu dispositivo en Internet, todos tienen la misma dirección pública. Las IPs privadas solo las ven los otros dispositivos de la misma red local, lo que significa que todos los dispositivos de su red domestica pueden comunicarse entre si mediante direcciones IP únicas que el resto de internet no puede ver. Otro tipo de dirección utilizada se denomina dirección MAC, la cual es un identificador alfanumérico único que se asigna a cada dispositivo físico de una red. Cuando un conmutador recibe un paquete de datos lee la dirección MAC del dispositivo de destino y le asigna a un puerto

Algunas de las principales diferencias entre IPv4 e IPv6 son la longitud y el formato de las direcciones. Las direcciones IPv4 se componen de cuatro números decimales separados por puntos, cada número va de 0 a 255. Juntos, los números abarcan 4 bytes y permiten hasta 4.300 millones de direcciones posibles. Un ejemplo de dirección IPv4 sería: 198.51.100.0. Las direcciones IPv6 están formadas por ocho números hexadecimales separados por dos puntos, cada número consta de hasta cuatro dígitos hexadecimales. Juntos, todos los números abarcan 16 bytes y permiten hasta 340 undecilillones de direcciones (340 seguidos de 36 ceros). Un ejemplo de dirección IPv6 sería: 2002:0db8:0000:0000:0000:ff21:0023:1234.

Nota: para representar uno o más conjuntos consecutivos de todos ceros, puede sustituir los ceros por dos puntos dobles "::", por lo que la dirección IPv6 anterior sería "2002:0db8::ff21:0023:1234"

También existen algunas diferencias en el diseño del Encabezado de un Paquete IPv6. El formato del Encabezado IPv6 es mucho más sencillo que el de IPv4. Por ejemplo, el Encabezado IPv4 incluye los campos IHL, Identificación y Banderas, mientras que el IPv6 no. El encabezado IPv6 sólo introduce el campo de etiqueta de flujo, donde la etiqueta de flujo identifica un paquete como que requiere un manejo especial por parte de otros routers IPv6.