**Protocolos de red:** conjunto de reglas que utilizan 2 o mas dispositivos de una red para describir el orden de entrega y la estructura de datos. Antes de acceder a un sitio web, su disp. Establecerá comunicaciones con un servidor web. Esa comunicación usa un protocolo denominado protocolo de control de transmisión o TCP, el cual permite que 2 disp. Establezcan una conexión y transmitan datos (no se limita a 2 dispositivos sino 2 puntos finales). Además de verificar ambos disp. Antes de permitir que se lleve a cabo cualquier otra comunicación, esto se denomina protocolo de enlace. Una vez establecida la comunicación mediante un protocolo de enlace TCP, se realiza una solicitud a la red, como datos de un servidor

A medida que los paquetes de datos se mueven por la red, se mueven entre los disp. De la red como enrutadores. El *protocolo de resolución de direcciones,* o **ARP**, se usa para determinar la dirección MAC del siguiente Router o disp. De la ruta de acceso, lo que garantiza que los datos lleguen al lugar correcto

El *protocolo seguro de transferencia de hipertexto,* o **HTTPS**, es un protocolo de red que proporciona un método seguro de comunicación entre los servidores del cliente y del sitio web. Permite que su navegador envié de forma segura una solicitud de una pagina web al servidor y reciba una pagina web como respuesta. Luego viene el protocolo llamado sistema de nombres de dominio, o **DNS**, que traduce los nombres de dominio de internet en direcciones IP. Envía el nombre de dominio y la dirección web a un servidor que recupera la dirección IP del sitio web al que intentaba acceder. La IP se incluye como dirección de destino para los paquetes de datos que viajan al servidor. Todo esto muestra que con solo visitar un sitio web, el dispositivo utilizara los protocolos TCP, ARP, HTTPS y DNS

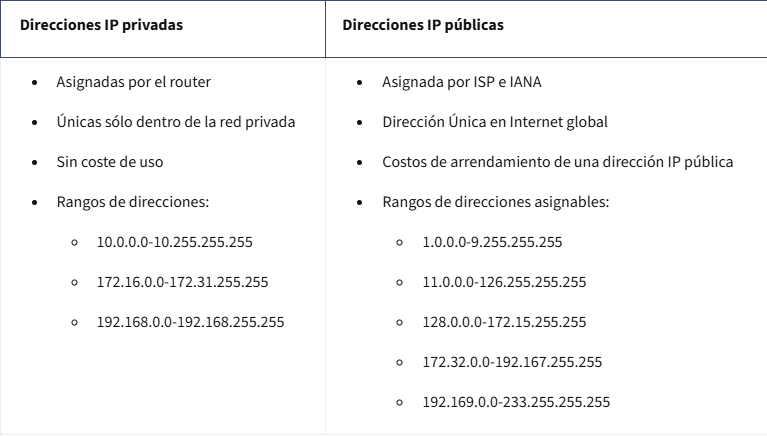
Estos protocolos se relacionan con la seguridad, ya que HTTPS cifra los datos mediante la capa de sockets seguros y la capa de seguridad de transporte, lo que ayuda a proteger la información de los actores malintencionados que buscan robar información. A nivel de protocolos de seguridad también existe el **Protocolo seguro de transferencia de archivos (SFTP)**, utilizado para transferir archivos de un dispositivo a otro a través de una red. Utiliza Secure Shell (SSH), normalmente por el puerto TCP 22. SSH utiliza el *estándar de encriptación avanzada (AES)* y otros tipos de encriptación para garantizar que los destinatarios no deseados no puedan interceptar las transmisiones. En el modelo TPC/IP, SFTP se produce en la capa de aplicación y se utiliza a menudo con el almacenamiento en la nube

También existen **protocolo de gestión** usados para supervisar y gestionar la actividad de una red, vamos a ver 2:

1. **Protocolo simple de administración de red (SNMP):** protocolo de red utilizado para supervisar y gestionar los dispositivos de una red. Puede restablecer una contraseña en un dispositivo de red o cambiar su configuración base, además de enviar solicitudes a los dispositivos de red para obtener un informe sobre la cantidad de ancho de banda de la red que se esta utilizando, en el modelo TCP/IP, se produce en la capa de aplicación
2. **Protocolo de mensajes de control de internet (ICMP):** utilizado en Internet por los dispositivos para informarse mutuamente de los errores de transmisión. Es usado por un dispositivo receptor para enviar un informe al dispositivo emisor sobre la transmisión, se usa como una forma rápida de solucionar problemas de conectividad y latencia de red mediante la emisión del comando ping en un SO operativo Linux. En el modelo TCP/IP, se produce en la capa de internet

**Traducción de direcciones de red**

Los dispositivos de su red local para comunicarse entre si usan una IP privada, pero para la internet publica, utilizan una IP publica que represente a todos los dispositivos ante el publico. Para los mensajes salientes, el Router puede sustituir una IP de origen privada por su dirección IP publica y realizar la inversa para las respuestas, lo que se conoce como *traducciones de direcciones de red (NAT)*y generalmente requiere que un Router o firewall este configurado específicamente para realizar NAT, el cual forma parte de la capa 2 (de internet) y de la capa 3 (de transporte) en el modelo TCP/IP



**Protocolo de configuración dinámica de host (DHCP):** pertenece a la familia de protocolos de red de gestión y a la capa de aplicación que se utiliza en una red para configurar dispositivos. Funciona con el Router para asignar una IP única a cada dispositivo y proporcionar las direcciones del servidor DNS y de la puerta de enlace predeterminada adecuados para cada dispositivo. Los servidores DHCP operan en el puerto UDP 67 mientras que los clientes DHCP lo hacen en el UDP 68

**Protocolo de resolución de direcciones (ARP):** es principalmente un protocolo de la capa de acceso a la red en el modelo TCP/IP que se usa para traducir las IPs que se encuentran en los paquetes de datos a la dirección MAC del disp. De hardware. Cada dispositivo de la red ejecuta ARP y mantiene un registro de las direcciones IP y MAC coincidentes en un caché ARP. ARP no tiene un número de puerto específico ya que es un protocolo de capa 2 y los números de puerto están asociados a la capa de aplicación 7.

**Telnet:** protocolo de capa de aplicación utilizado para conectar con un sistema remoto. Telnet envía toda la información en texto claro y usa la línea de comandos para controlar otro dispositivo de forma similar a SSH, pero no es tan seguro. Puede usarse para conectarse a dispositivos locales o remotos y utiliza el puerto TCP 23

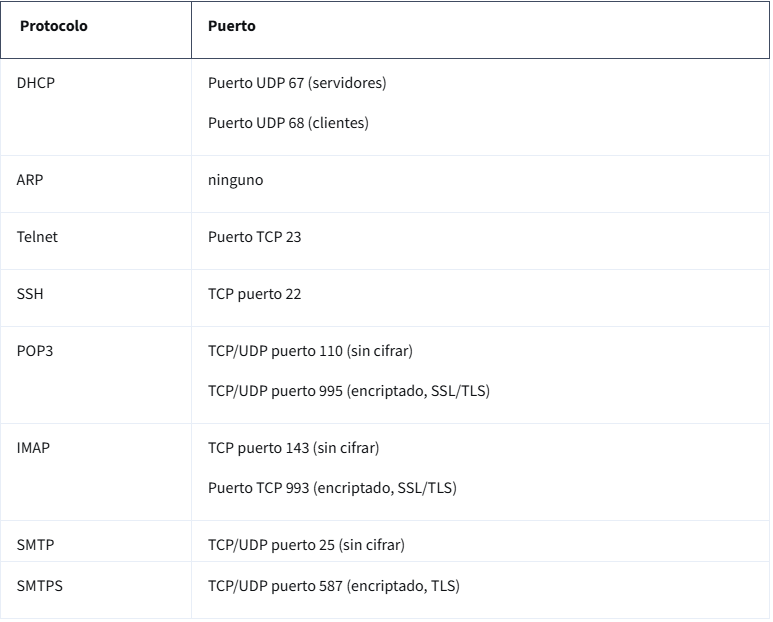
**Secure Shell (SSH):** se utiliza para crear una conexión segura con un sistema remoto. Este protocolo de capa de aplicación proporciona una alternativa para la autenticación segura y la encriptación de la comunicación. SSH funciona a través del puerto TCP 22 y es un sustituto de protocolos menos seguros, como Telnet.

**Protocolo de oficina de correos (POP):** protocolo de capa de aplicación (capa 4 del Modelo TCP/IP) utilizado para gestionar y recuperar correo electrónico de un servidor de correo. POP3 es la versión más utilizada de POP. Muchas organizaciones tienen un servidor de correo dedicado en la red que gestiona el correo entrante y saliente para los usuarios de la red. Los dispositivos de los usuarios enviarán solicitudes al servidor de correo remoto y descargarán los mensajes de correo electrónico localmente. La autenticación en texto plano sin cifrar utiliza el puerto TCP/UDP 110 y los correos electrónicos cifrados utilizan la Capa de sockets seguros/Seguridad de la capa de transporte (SSL/TLS) a través del puerto TCP/UDP 995. Cuando se utiliza POP, el correo tiene que terminar de descargarse en un dispositivo local antes de poder ser leído. Después de descargarse, el correo puede o no borrarse del servidor de correo, por lo que no garantiza que un usuario pueda sincronizar el mismo correo electrónico en varios dispositivos.

**Protocolo de acceso a mensajes de Internet (IMAP):** se utiliza para el correo electrónico entrante. Descarga las cabeceras de los correos electrónicos y el contenido del mensaje. El contenido también permanece en el servidor de correo electrónico, lo que permite a los usuarios acceder a su correo electrónico desde múltiples dispositivos. IMAP utiliza el puerto TCP 143 para el correo electrónico no cifrado y el puerto TCP 993 a través del protocolo TLS. El uso de IMAP permite a los usuarios leer parcialmente el correo electrónico antes de que termine de descargarse. Dado que el correo se guarda en el servidor de correo, permite al usuario sincronizar los correos electrónicos de varios dispositivos.

**Protocolo simple de transmisión de correo (SMTP):** se usa para transmitir y encaminar el correo electrónico del remitente a la dirección del destinatario. Funciona con el software de agente de transferencia de mensajes (MTA) que busca en los servidores de DNS para resolver las direcciones de correo electrónico en direcciones IP, para garantizar que los correos lleguen a su destino previsto. SMTP utiliza el puerto TCP/UDP 25 para los correos electrónicos no cifrados y el puerto TCP/UDP 587 que utiliza TLS para los correos electrónicos cifrados. El puerto TCP 25 suele ser utilizado por el spam de gran volumen. SMTP ayuda a filtrar el spam regulando cuántos correos electrónicos puede enviar una fuente a la vez.

- Los números de puerto son utilizados por los dispositivos de red para determinar qué debe hacerse con la información contenida en cada paquete de datos una vez que llegan a su destino. Los firewalls pueden filtrar el Tráfico no deseado basándose en los números de puerto. Por ejemplo, una organización puede configurar un firewall para que sólo permita la accesibilidad al puerto TCP 995 (POP3) a las direcciones IP pertenecientes a la organización.



**Protocolos de comunicación IEEE802.11:** conocido comúnmente como Wi-Fi, es un conjunto de estándares que definen las comunicaciones para las LAN inalámbricas. IEEE son las siglas de Instituto de Ingenieros Eléctricos y Electrónicos, que es una organización que mantiene los estándares Wi-Fi, y 802.11 es un conjunto de protocolos usados en las comunicaciones inalámbricas. En 2004 se introdujo un protocolo llamado Acceso Wi-Fi protegido, o WPA, el cual es un protocolo de seguridad inalámbrico para que los dispositivos se conecten a Internet, actualmente a ido evolucionando para incluir mas seguridad (como una encriptación mas avanzada)

Los protocolos de comunicación inalámbrica (Wi-Fi), basados en la familia IEEE 802.11, han evolucionado para mejorar la **seguridad** en redes inalámbricas:

* **WEP (1999):** Primer protocolo de seguridad inalámbrica; buscaba ofrecer la misma privacidad que las redes cableadas, pero resultó inseguro y fácil de romper.
* **WPA (2003):** Sustituyó a WEP, usando TKIP y comprobaciones de integridad, pero vulnerable a ataques KRACK.
* **WPA2 (2004):** Incorporó AES y CCMP para mayor seguridad; estándar actual, disponible en modo *Personal* (para hogares, clave compartida) y *Enterprise* (control centralizado para empresas). Aún vulnerable a KRACK.
* **WPA3 (2018):** Soluciona fallos de WPA2, añade SAE para evitar ataques de descifrado offline, mejora cifrado (128/192 bits) y ofrece mayor protección.

En general, la seguridad Wi-Fi ha evolucionado desde WEP hasta WPA3 para responder a vulnerabilidades y ofrecer cifrado y autenticación más sólidos.

**Firewall:** dispositivo de seguridad de red que monitorea el trafico hacia y desde su red. Permite el trafico o lo bloquea basándose en un conjunto definido de reglas de seguridad. Este puede utilizar el filtrado de puertos, que bloquea o permite ciertos números de puertos para limitar la comunicación no deseada, las configuraciones vienen determinadas por la política de seguridad de la organización

Hay varios tipos de cortafuegos:

* **Cortafuegos de hardware:** se considera la forma mas básica de defenderse contra las amenazas de una red, inspecciona cada paquete de datos antes de que se le permita entrar en la red
* **Cortafuegos por software:** realiza las mismas funciones que el anterior pero no es un dispositivo físico sino un programa instalado en una computadora o un servidor. Si se instala en una computadora, analizara todo el trafico recibido por esa computadora, en cambio, si es en un servidor, protegerá todos los dispositivos conectados al mismo. Suele costar menos que adquirir un dispositivo físico independiente, además no ocupa espacio adicional, aunque añadirá cierta carga de proceso
* **Cortafuegos basado en la nube:** son ofrecidos por proveedores de servicios como servicio, o FaaS, para organizaciones. Las mismas pueden configurar las reglas del firewall en la interfaz del proveedor, y el firewall realizara operaciones de seguridad en todo el trafico entrante antes de que llegue a la red in situ de la organización, también protegen cualquier recurso o proceso que una organización pueda estar usando en la nube

Todos estos firewalls pueden tener 2 características:

1. *Con estado:*una clase de cortafuegos que realiza un seguimiento de la información que pasa a través de él y filtra proactivamente las amenazas, analiza el trafico de red en busca de características y comportamientos que parezcan sospechosos e impide que entre a la red
2. *Sin estado:* clase de cortafuegos que funciona basándose en reglas predefinidas y no lleva un registro de la información de los paquetes de datos. Solo actúa según reglas establecidas por el administrador del cortafuegos, las cuales le dicen que aceptar y rechazar. No almacena información analizada ni descubre tendencias sospechosas, por lo que es considerado menos seguro

Los cortafuegos de nueva generación (**NFGW**), proporcionan más seguridad que un cortafuegos con estado, ya que no solo inspecciona el estado del trafico que entra y sale, sino que también inspecciona profundamente los paquetes y protege contra intrusos. Algunos de estos se conectan a servicios de inteligencia sobre amenazas basados en la nube, por lo que se pueden actualizar más rápido

**Red privada virtual (VPN):** servicio de seguridad de red que cambia tu IP publica y oculta tu ubicación virtual para que puedas mantener la privacidad de tus datos cuando utilices una red pública. También cifran tus datos mientras viajan para preservar la confidencialidad y realiza la encapsulación de los datos en tráfico, lo que consiste en proteger los datos empaquetando lo confidencial en otros paquetes de datos. Además, permite que los enrutadores puedan acceder a la IP de forma segura porque sino no podríamos acceder a distintos servicios webs. La VPN también utiliza un túnel cifrado entre el dispositivo y el servidor VPN, la cual no se puede hackear sin una clave criptográfica

**Zonas de seguridad:** segmento de una red que protege la red interna de Internet. Forman parte de una técnica de seguridad denominada segmentación de red. Cada segmento tiene sus propios permisos de acceso y reglas de seguridad. Las zonas de seguridad controlan quien puede acceder a los diferentes segmentos y actúan como una barrera para las redes internas, mantienen la privacidad dentro de un grupo corporativo y evitan que los problemas se propaguen a toda la red. Un ejemplo podría ser ofrecer un Wi-Fi gratis para los huéspedes de un hotel, pero que los empleados tengan uno propio

La red de una organización también se puede dividir en subredes para mantener la privacidad de cada departamento de la organización. Estas subredes más pequeñas se forman en función de las direcciones IP y la máscara de red de los dispositivos de la red. La división en subredes crea una red de dispositivos para que funcionen como su propia red. Esto hace que la red sea más eficiente y también puede utilizarse para crear zonas de seguridad. Si los dispositivos de una misma subred se comunican entre sí, el Switch cambia las transmisiones para que permanezcan en la misma subred, lo que mejora la velocidad y la eficacia de las comunicaciones. Es clasificada en 2 zonas de seguridad:

1. Zona descontrolada: cualquier red fuera del control de la organización
2. Red controlada: subred que protege la red interna de la zona no controlada. Entre las redes que se encuentran en su interior están:

* Capa exterior: se encuentra la zona desmilitarizada (DMZ), que contiene servicios públicos que pueden acceder a internet, como servidores webs, proxys que alojan sitios web para el publico y servidores DNS, actúa como perímetro de red para la red interna
* Zona restringida: protege la información altamente confidencial a la que solo pueden acceder los empleados con ciertos privilegios

Lo ideal es que la DMZ este entre 2 firewalls, el cual uno filtra el trafico fuera de la DMZ y el otro el que ingresa a la red interna. En caso de haber una zona restringida, también estaría protegida con otro firewall, para que, si un ataque penetra la red DMZ, no pueda propagarse a la red interna

**Direccionamiento entre dominios sin clase (CIDR):** método de asignación de mascaras de subred a IPs para crear una subred, sustituye al direccionamiento con clase que se utilizó en la década de 1980 como sistema de agrupación de direcciones IP en clases (A-E). Cada una incluía un numero limitado de direcciones IP, que se fueron agotando a medida que el número de disp. Que se conectaban a internet superaba el rango de clases en la década de 1990. El CIDR amplio el numero de direcciones IPv4 disponibles

Permite a los profesionales segmentar las redes con clase en trozos mas pequeños. Las IP CIDR tienen el mismo formato que las IPv4, pero incluyen una barra (“/”) seguida de un numero al final de la dirección, denominado prefijo de red IP, por ejemplo: el formato normal sería 198.51.100.0. en cambio, la dirección CIDR seria 198.51.100.0/24. Esta dirección CIDR engloba todas las direcciones IP entre 198.51.100.0 y 198.51.100.255. El sistema de direccionamiento CIDR reduce el número de entradas en las tablas de enrutamiento y proporciona más direcciones IP disponibles dentro de las redes.

La división en subredes permite a los profesionales y analistas de redes crear una red dentro de su propia red sin solicitar otra dirección IP de red a su proveedor de servicios de Internet. Este proceso utiliza el ancho de banda de la red de forma más eficiente y mejora el rendimiento de la red. La división en subredes es uno de los componentes de la creación de subredes aisladas mediante el aislamiento físico, la configuración del enrutamiento y los firewalls.

**Servidor proxy:** servidor que cumple con la solicitud de un cliente reenviándola a otros servidores. Es un servidor dedicado que se encuentra entre internet y el resto de la red. Cuando llega una solicitud de conexión a la red, el servidor determinara si la solicitud es segura. El proxy es una dirección IP publica que es diferente del resto de la red privada, lo que oculta la IP de la red privada de los actores malintencionados y añade una capa de seguridad. Por ejemplo, cuando un cliente recibe una respuesta HTTPS, notara una dirección IP distorsionada o ninguna IP en lugar de la dirección real del servidor web de la organización. También se puede usar un servidor proxy para bloquear sitios web no seguros a los que los usuarios no pueden acceder en la red de una organización. Este servidor usa memoria temporal para almacenar los datos que solicitan regularmente los servidores externos, por lo que no tiene que buscar datos en los servidores internos de una organización en todo momento. Esto mejora la seguridad ya que reduce el contacto con el servidor interno. Hay diferentes tipos de servidores proxy que admiten la seguridad de la red. Esto es importante para los analistas de Seguridad que supervisan el tráfico de varios servidores proxy y es posible que necesiten saber para qué sirven. Exploremos algunos tipos diferentes de servidores proxy. Un servidor proxy directo regula y restringe el acceso de una persona a Internet. El objetivo es ocultar la dirección IP del usuario y aprobar todas las solicitudes salientes. En el contexto de una organización, un servidor proxy de reenvío recibe el tráfico saliente de un empleado, lo aprueba y, a continuación, lo reenvía al destino en Internet. Un servidor proxy inverso regula y restringe el acceso a Internet a un servidor interno. El objetivo es aceptar el tráfico de terceros, aprobarlo y reenviarlo a los servidores internos. Esta configuración es útil para proteger los servidores web internos que contienen datos confidenciales para que no expongan su dirección IP a terceros. Un servidor proxy de correo electrónico es otra valiosa herramienta de Seguridad. Filtra el correo no deseado verificando si la dirección del remitente fue falsificada. Esto reduce el riesgo de ataques de suplantación de identidad en los que se hacen pasar por personas conocidas por la organización.

**VPN de acceso remoto:** son utilizadas por los usuarios para establecer una conexión entre un dispositivo personal y un servidor VPN. Encriptan los datos enviados o recibidos a través de un dispositivo personal y la conexión entre el usuario y la VPN se establece a través de internet

**VPN de sitio a sitio:** las utilizan las empresas en gran medida para extender su red a otras redes y ubicaciones, lo que es especialmente útil para las organizaciones que tienen muchas oficinas en todo el mundo. IPSec se utiliza habitualmente en las VPN de sitio a sitio para crear un túnel cifrado entre la red principal y la remota. Una desventaja es lo complejas que pueden ser para configurar y gestionar al lado de las VPN remotas

**VPN WireGuard:** protocolo de alta velocidad, con una encriptación avanzada para proteger a los usuarios cuando acceden a internet. Esta diseñado para ser sencillo de configurar y mantener. Puede usarse tanto para conexiones de sitio a sitio como para las de cliente-servidor. Este es mas reciente que IPSec y se utiliza por muchas personas debido a que su velocidad de descarga aumenta al utilizar menos líneas de programación, además, es de código abierto lo que facilita su implementación y depuración. Este protocolo es útil para procesos que requieren velocidades de descarga ams rápidas, como la transmisión de contenidos de video o la descarga de archivos de gran tamaño

**VPN IPSec:** protocolo que puede utilizarse para configurar la VPN. La mayoría de los proveedores de VPN lo utilizan para encriptar y autenticar los paquetes de datos con el fin de establecer conexiones seguras y encriptadas. Como es uno los primeros protocolos, muchos SO son compatibles con IPSec