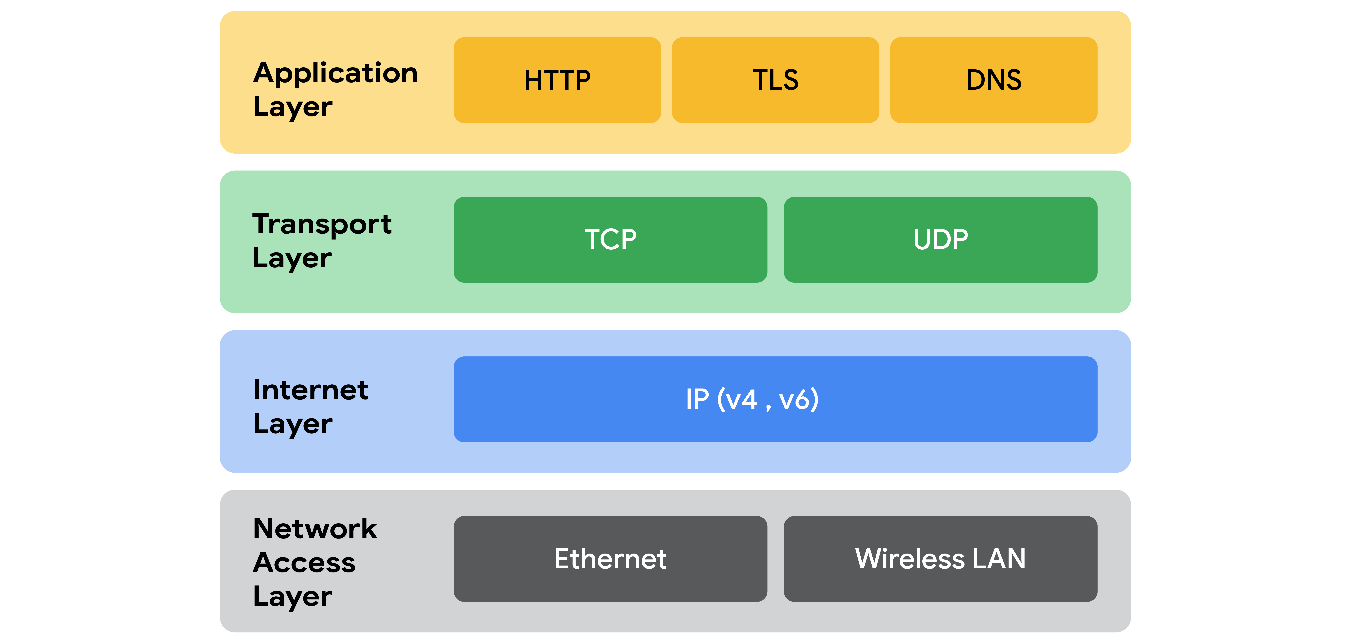
**El Modelo TCP/IP**

El **Modelo TCP/IP** es un framework utilizado para visualizar cómo se organizan y transmiten los datos a través de una red. Este Modelo ayuda a los ingenieros de redes y a los analistas de seguridad de redes a conceptualizar los procesos en la red y a comunicar dónde se producen las interrupciones o las amenazas a la seguridad.

El Modelo TCP/IP tiene cuatro capas: la capa de accesibilidad a la red, la capa de Internet, la capa de transporte y la capa de aplicación. Cuando se solucionan problemas en la red, los profesionales de la Seguridad pueden analizar qué capas se vieron afectadas por un ataque en función de los procesos implicados en un incidente.



**Capa de acceso a la red**

La capa de acceso a la red, a veces denominada capa de vínculo de datos, se ocupa de la creación de paquetes de datos y su transmisión a través de una red. Esta capa corresponde al hardware físico implicado en la transmisión de la red. Concentradores, módems, cables y cableado se consideran parte de esta capa. El protocolo de resolución de direcciones (ARP) forma parte de la capa de accesibilidad a la red. Dado que las direcciones MAC se utilizan para identificar hosts en la misma red física, ARP es necesario para asignar direcciones IP a direcciones MAC para la comunicación de red local.

**Capa de Internet**

La capa de Internet, a veces denominada capa de red es responsable de garantizar la entrega al host de destino, que potencialmente reside en una red diferente. Garantiza que las direcciones IP se adjunten a los paquetes de datos para indicar la ubicación del remitente y el destinatario. La capa de Internet también determina qué protocolo es responsable de entregar los paquetes de datos y garantiza la entrega al host de destino. Estos son algunos de los protocolos comunes que operan en la capa de Internet:

* Protocolo de Internet (IP). IP envía los paquetes de datos al destino correcto y se basa en el Protocolo de control de transmisión/Protocolo de Datagramas de Usuario (TCP/UDP) para entregarlos al servicio correspondiente. Los paquetes IP permiten la comunicación entre dos redes. Se encaminan desde la red emisora hasta la red receptora. El TCP, en particular, retransmite cualquier dato que se pierda o esté corrupto.
* Protocolo de mensajes de control de Internet (ICMP). El ICMP comparte información sobre errores y actualizaciones del estado de los paquetes de datos. Esto resulta útil para detectar y solucionar errores de red. El ICMP transmite información sobre paquetes que se han perdido o que han desaparecido en tránsito, problemas con la conectividad de la red y paquetes redirigidos a otros routers.

**Capa de transporte**

La capa de transporte es responsable de la entrega de datos entre dos sistemas o redes e incluye protocolos para controlar el flujo de tráfico a través de una red. TCP y UDP son los dos protocolos de transporte que se dan en esta capa.

**Protocolo de control de transmisión**

El Protocolo de control de transmisión (TCP ) es un 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 servicio de destino. TCP contiene el número de puerto del servicio de destino previsto, que reside en el encabezado TCP de un paquete TCP/IP.

**Protocolo de Datagramas de Usuario**

El Protocolo de Datagramas de Usuario (UDP) es un protocolo no orientado a la conexión que no establece una conexión entre dispositivos antes de las transmisiones. Lo utilizan aplicaciones a las que no les preocupa la fiabilidad de la transmisión. Los 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.

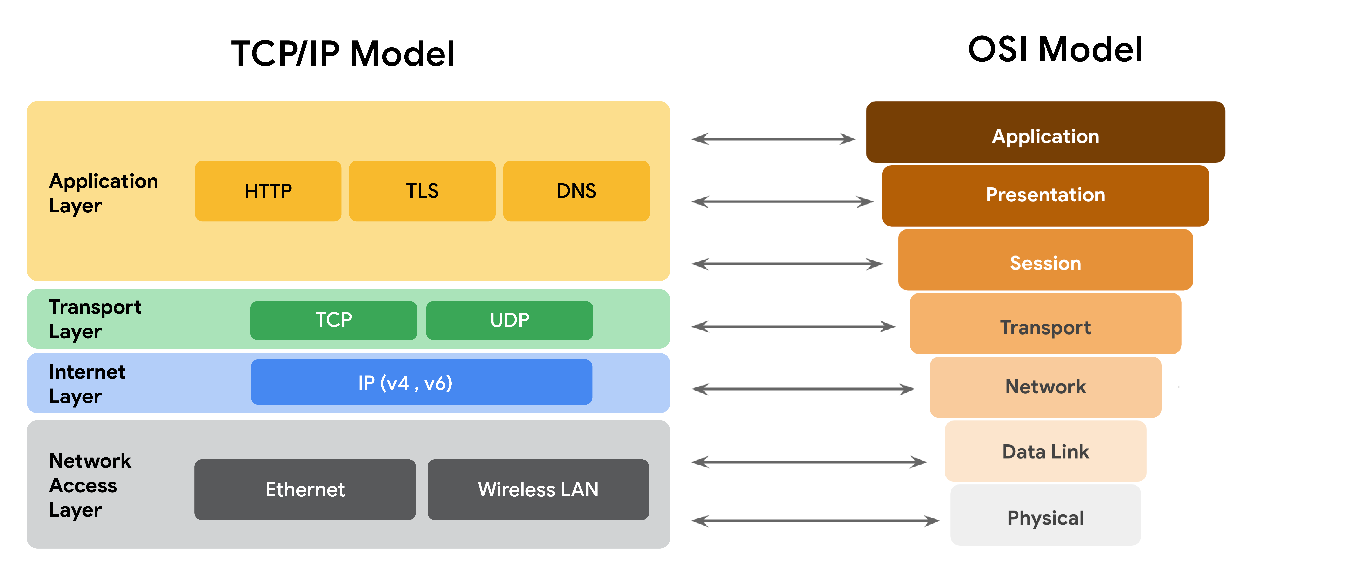
**Capa de aplicación**

La capa de aplicación en el Modelo TCP/IP es similar a las capas de aplicación, presentación y sesión del Modelo OSI. La capa de aplicación es la responsable de realizar las solicitudes de red o de responder a las peticiones. Esta capa define a qué servicios y aplicaciones de Internet puede acceder cualquier usuario. Los protocolos de la capa de aplicación determinan cómo interactuarán los paquetes de datos con los dispositivos receptores. Algunos protocolos comunes utilizados en esta capa 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)

Los protocolos de la capa de aplicación se basan en capas subyacentes para transferir los datos a través de la red.

**Modelo TCP/IP frente al modelo OSI**



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.

**Puntos clave**

Tanto el modelo TCP/IP como el OSI son modelos conceptuales que ayudan a los profesionales de las redes a visualizar los procesos y protocolos de red en lo que respecta a la transmisión de datos entre dos o más sistemas. El Modelo TCP/IP contiene cuatro capas y el modelo OSI, siete.

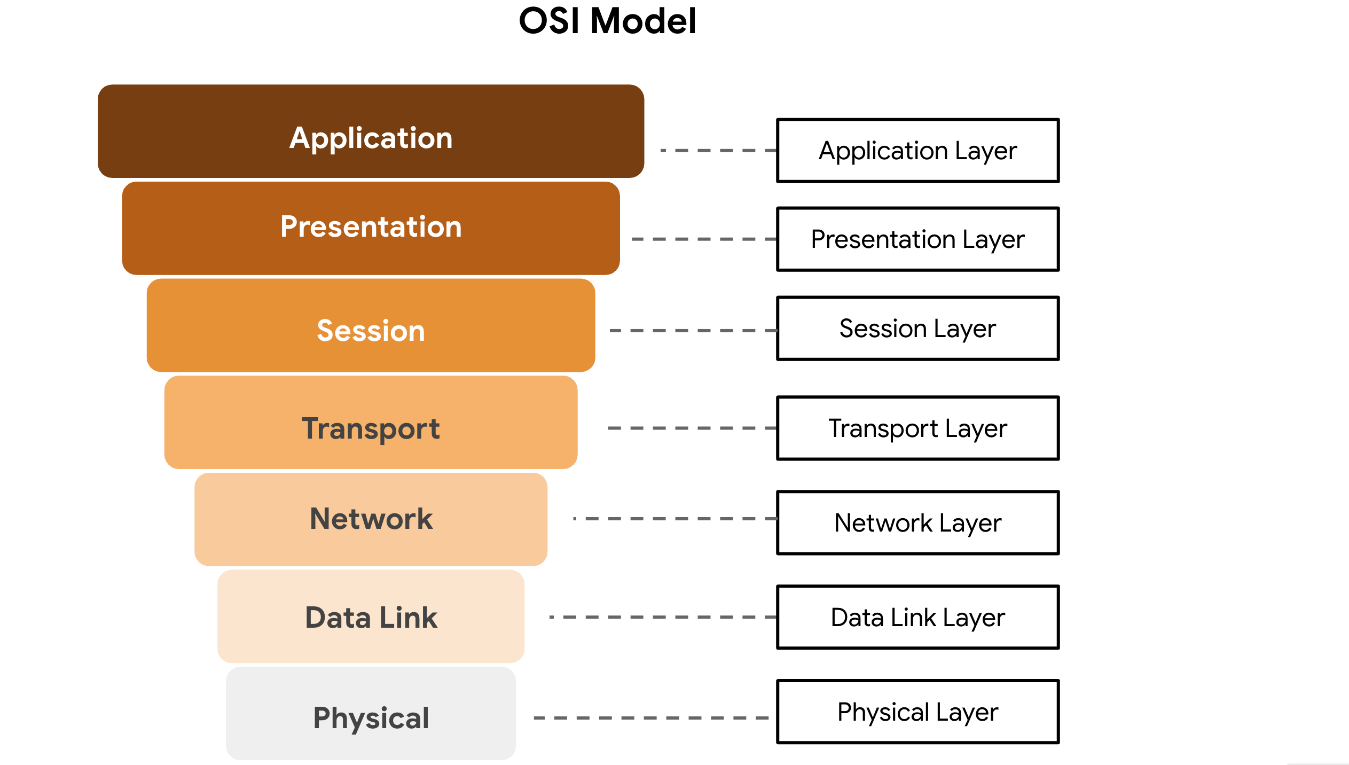
**El Modelo OSI**

**El Modelo TCP/IP frente al modelo OSI**

El **Modelo TCP/IP** es un framework utilizado para visualizar cómo se organizan y transmiten los datos a través de una red. Este Modelo ayuda a los ingenieros de redes y a los analistas de seguridad a conceptualizar los procesos en la red y a comunicar dónde se producen las interrupciones o las amenazas a la seguridad.

El Modelo TCP/IP tiene cuatro capas: la capa de accesibilidad a la red, la capa de Internet, la capa de transporte y la capa de aplicación. Al analizar los incidentes de red, los profesionales de la seguridad pueden determinar en qué capa o capas se produjo un ataque en función de los procesos que intervinieron en el incidente.

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. Los profesionales de las redes y la seguridad suelen utilizar este Modelo para comunicarse entre sí sobre las posibles fuentes de problemas o amenazas a la seguridad cuando se producen.



Algunas organizaciones se basan en gran medida en el Modelo TCP/IP, mientras que otras prefieren utilizar el Modelo OSI. Como analista de Seguridad, es importante estar familiarizado con ambos Modelos. Tanto el modelo TCP/IP como el OSI son útiles para comprender cómo funcionan las redes.

**Capa 7: Capa de aplicación**

La 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.

Un ejemplo de un tipo de comunicación que se produce en la capa de aplicación es el uso de un navegador de Internet. El navegador de Internet utiliza HTTP o HTTPS para enviar y recibir información del servidor del sitio web. La aplicación de correo electrónico utiliza el Protocolo simple de transmisión de correo (SMTP) para enviar y recibir información por correo electrónico. Además, los navegadores web utilizan el protocolo del sistema de nombres de dominio (DNS) para traducir los nombres de dominio de los sitios web en direcciones IP que identifican el servidor web que aloja la información del sitio web.

**Capa 6: Capa de presentación**

Las funciones de la capa de presentación implican la traducción y encriptación de datos para la red. Esta capa añade y sustituye Datos por formatos que puedan ser entendidos por las aplicaciones (capa 7) tanto en los sistemas emisores como en los receptores. Los formatos en el extremo del usuario pueden ser diferentes de los del sistema receptor. Los procesos en la capa de presentación requieren el uso de un formato estandarizado.

Algunas funciones de formateo que tienen lugar en la capa 6 incluyen la encriptación, la compresión y la confirmación de que el conjunto de códigos de caracteres puede ser interpretado en el sistema receptor. Un ejemplo de encriptación que tiene lugar en esta capa es SSL, que encripta los datos entre los servidores web y los navegadores como parte de los sitios web con HTTPS.

**Capa 5: Capa de sesión**

Una Sesión describe el momento en que se establece una conexión entre dos dispositivos. Una sesión abierta permite que los dispositivos se comuniquen entre sí. Los protocolos de la capa de sesión mantienen la sesión abierta mientras se transfieren los datos y la terminan una vez finalizada la transmisión.

La capa de sesión también es responsable de actividades como la autenticación, la reconexión y el establecimiento de puntos de control durante una transferencia de datos. Si se interrumpe una sesión, los puntos de control garantizan que la transmisión se retome en el último punto de control de la sesión cuando se reanude la conexión. Las Sesiones incluyen una solicitud y una respuesta entre aplicaciones. Las funciones de la capa de sesión responden a las solicitudes de servicio de los procesos de la capa de presentación (capa 6) y envían solicitudes de servicios a la capa de transporte (capa 4).

**Capa 4: Capa de transporte**

La 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 más pequeños para facilitar su transporte. Segmentación es el proceso de dividir una gran transmisión de Datos en trozos más 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 (capa 5). La velocidad y el ritmo de la transmisión también tienen que coincidir con la velocidad de conexión del sistema de destino. TCP y UDP son protocolos de capa de transporte.

**Capa 3: Capa de red**

La capa de red supervisa la recepción de las tramas desde la capa de enlace de datos (capa 2) y las entrega al destino previsto. El destino previsto puede encontrarse basándose en la dirección que reside en la trama de los paquetes de datos. Los paquetes de datos permiten la comunicación entre dos redes. Estos paquetes incluyen direcciones IP que indican a los routers dónde enviarlos. Se encaminan desde la red emisora hasta la red receptora.

**Capa 2: Capa de vínculo de datos**

La capa de enlace de datos organiza el envío y la recepción de paquetes de datos dentro de una misma red. En la capa de vínculo de datos se encuentran los conmutadores de la red local y las tarjetas de interfaz de red de los dispositivos locales.

En la capa de enlace de datos 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 control de enlace de datos síncrono (SDLC).

**Capa 1: Capa física**

Como su nombre indica, la capa física corresponde al hardware físico que interviene en la transmisión de la red. Los concentradores, los módems y los cables y el cableado que los conectan se consideran parte de la capa física. Para viajar a través de un cable ethernet o coaxial, un paquete de datos necesita ser traducido a un flujo de 0s y 1s. El flujo de 0s y 1s se envía a través del cableado físico y los cables, se recibe y, a continuación, pasa a niveles superiores del Modelo OSI.

**Claves**

Tanto el modelo TCP/IP como el OSI son modelos conceptuales que ayudan a los profesionales de las redes a diseñar procesos y protocolos de red en relación con la transmisión de datos entre dos o más sistemas. El Modelo OSI contiene siete capas de Comunicación. Los profesionales de las redes y la seguridad utilizan el modelo OSI para comunicarse entre sí sobre las posibles fuentes de problemas o amenazas a la seguridad cuando se producen. Los ingenieros de redes y los analistas de seguridad de redes utilizan los modelos TCP/IP y OSI para conceptualizar los procesos de red y comunicar la ubicación de las interrupciones o amenazas.