

Ruben Apablaza Muñoz  
-OzonE-

# Modelos OSI y TCP: relación con **CIBERSEGURIDAD**

## ¿PORQUE DEBES CONOCERLOS Y **APLICARLOS?**



**OzonE**  
CIBERSECURITY

## INTRODUCCIÓN

El presente documento tiene como objetivo mostrar con ejemplos cómo se relacionan los marcos conceptuales **OSI** y **TCP** con Ciberseguridad y en por qué un profesional o estudiante de ciberseguridad debe estar familiarizado con ellos para poder aplicarlos en la defensa de sistemas de información.

Este documento no pretende mostrar información exhaustiva de cada modelo como el origen histórico u otra información que no resulta relevante para el tema que aquí se desea tratar debido a que en internet hay muchas fuentes para quien desee saber más al respecto.

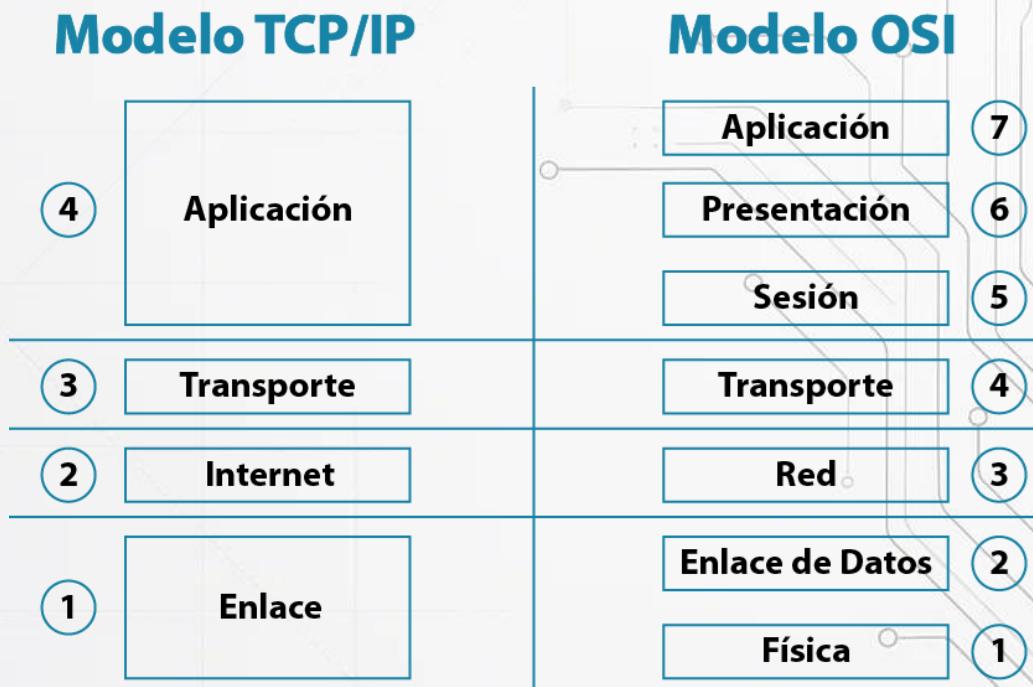
La primera vez que leí sobre estos dos modelos, si bien entendí el sistema de capas, me aprendí los nombres y memorice algunos protocolos, lo cierto es que me quedo la sensación de algo vacío, algo que faltó... la parte de cómo se aplica a ciberseguridad y sobre todo la razón del porqué, como estudiante y futuro profesional de ciberseguridad, debo conocer y saber cómo aplicar esta información.

El conocimiento del modelo OSI y TCP/IP no es un capricho académico. Es como un **mapa mental del funcionamiento de la red**. Un profesional de ciberseguridad:

- No solo reacciona sino que **diagnosticá con precisión**.
- No solo usa herramientas, **las entiende y las aplica inteligentemente**.
- No solo ve los síntomas, **localiza el origen del ataque**.

En lo personal me molesta ser solo alguien que “ocupa herramientas”; así que si eres de los que no se queda con esas explicaciones simples que dicen “porque sí”, te invito a revisar este documento que te puede ayudar como me ayudo a mí para entender la importancia de conocer y saber aplicar el conocimiento de estos modelos en la vía de ciberseguridad.

## MODELOS DE COMUNICACIÓN OSI Y TCP/IP



Ref: <https://platzi.com/clases/2225-redes/35584-modelo-tcip/>

- Son modelos referenciales que ordenan y simplifican la forma como entendemos el funcionamiento de una red.
- El uso de un modelo en capas ayuda en el diseño de protocolos.
- Fomenta la competencia permitiendo que los productos de distintas marcas puedan trabajar conjuntamente.
- Proporciona un lenguaje común a quienes desean explicar y aprender las funciones y capacidades de una red.

## MODELO OSI

Personalmente creo que la imagen a continuación es una de las mejores ilustraciones para explicar el modelo OSI.

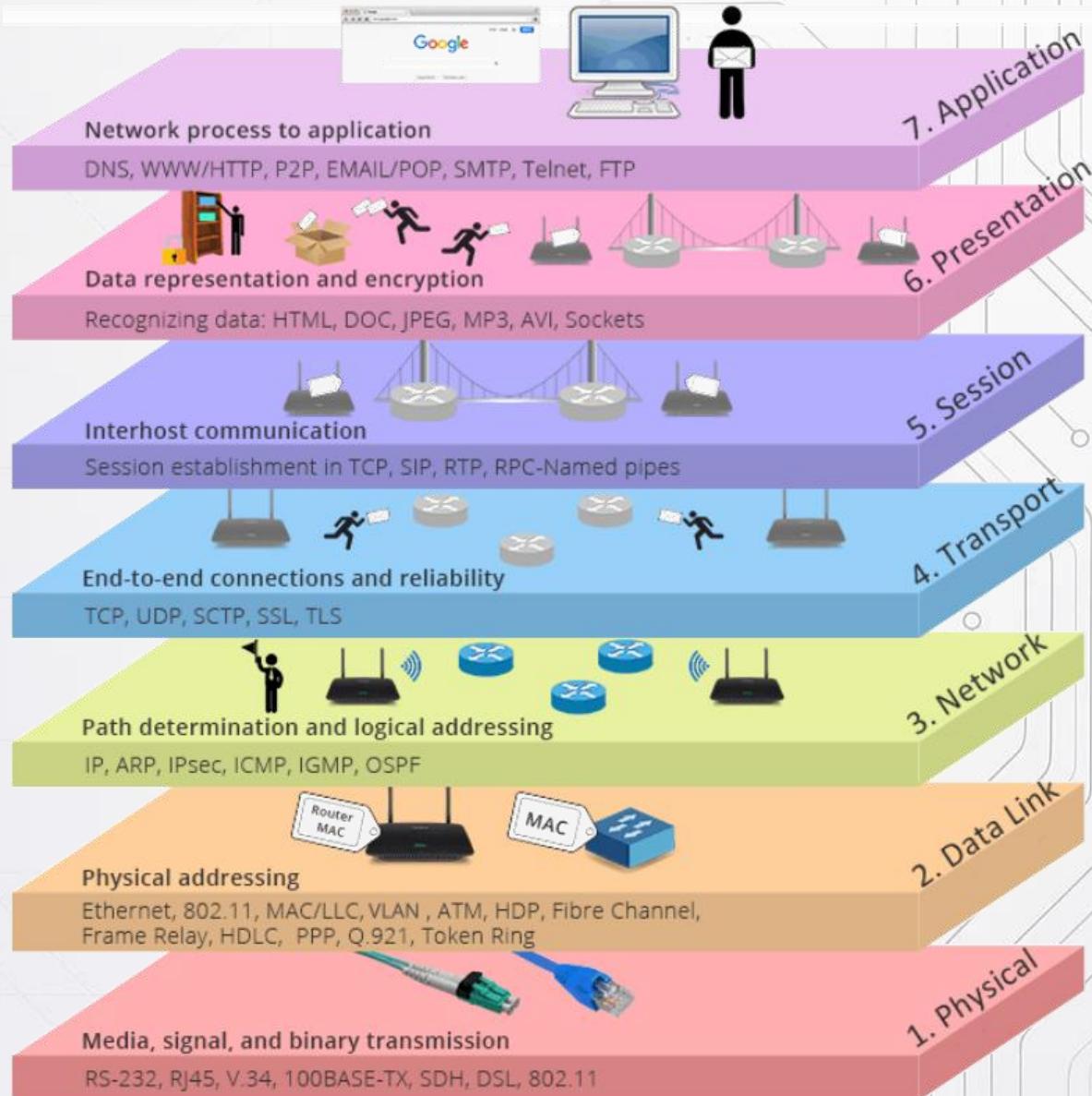


Imagen referencia <https://www.qsfptek.com/es/qt-news/tcp-ip-vs-osi-what-is-the-difference.html?srsltid=AfmBOopN6jLvbgo9Couhm-Ogtw-6gQWFt69Qs8ru-MTlwPmV8awtFN5f>

Respecto de modelo OSI podemos partir describiendo lo siguiente:

- Fue creado en 1980 por la ISO (International Organization for Standardization) cuyas siglas en español es Organización Internacional de Normalización.
- Se utiliza solo para estudio.
- Tiene 7 capas que se utilizan para describir entre otras cosas cómo deben transmitirse y enrutararse los datos.

A continuación, explicaré brevemente el funcionamiento de cada capa.

### **capa 1 – capa física.**

- Define la topología de red y las conexiones físicas.
- Es por donde va a viajar la información, por ejemplo, en un cable de par trenzado, de fibra óptica, los tipos de conectores, la longitud del cableado, etc.



### **OSI capa 2 – capa de enlace de datos.**

- Se encarga como en la capa de red, de transferir datos entre dispositivos, solo que en esta **sobre la misma red**.
- Se crean las **TRAMAS** de red con los paquetes de la capa anterior. Estos paquetes llevan la dirección MAC (física) del equipo emisor y receptor.



## OSI capa 3 – capa de red.

- Se encarga del direccionamiento entre dos redes **diferentes** gracias a las direcciones IP.
- Aquí se le añade un encabezado de red con la IP al segmento, creando lo que se conoce como **PAQUETE DE RED**.
- El encabezado contiene la IP con la que se enrutan los paquetes.



## OSI capa 4 - capa de transporte.

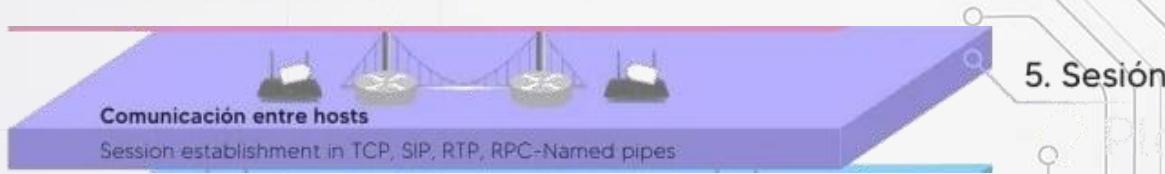
- Encargada del transporte de la información de un equipo a otro.
- Garantiza que los paquetes de red se envíen de manera **fiable** y sin errores.
- En esta capa, se fragmenta la información enviada en trozos llamados **SEGMENTOS**. El equipo de destino se encargará de unirlos.
- Si se utiliza un protocolo TCP en esta capa, se van a ir comprobando que los segmentos lleguen a su destino. En cambio, si utilizamos UDP, no se va a comprobar. Si se pierden datos, se pierden.
  - **TCP** (protocolo de control de transmisiones)
    - Tenemos conexiones fiables, pero más lentas que con UDP. Útil con archivos los cuales vamos a necesitar todos los segmentos. Por ejemplo, si te descargas un PDF, si se pierden algunos segmentos, no se va a poder reconstruir correctamente y de nada te va a servir ese archivo corrupto.

- **UDP** (protocolo de datagramas de usuario)
  - Tenemos conexiones menos fiables, pero más rápidas al no comprobar si se pierden o no los segmentos. Un ejemplo de uso, son los streams, puesto que es en directo, si se corta parte del stream, no interesa que se recupere esa parte, interesa que se siga viendo el directo lo más fluidamente posible.



### OSI capa 5 - capa de sesión.

Se encarga de abrir y cerrar la comunicación entre dos dispositivos.



### OSI capa 6 - capa de presentación.

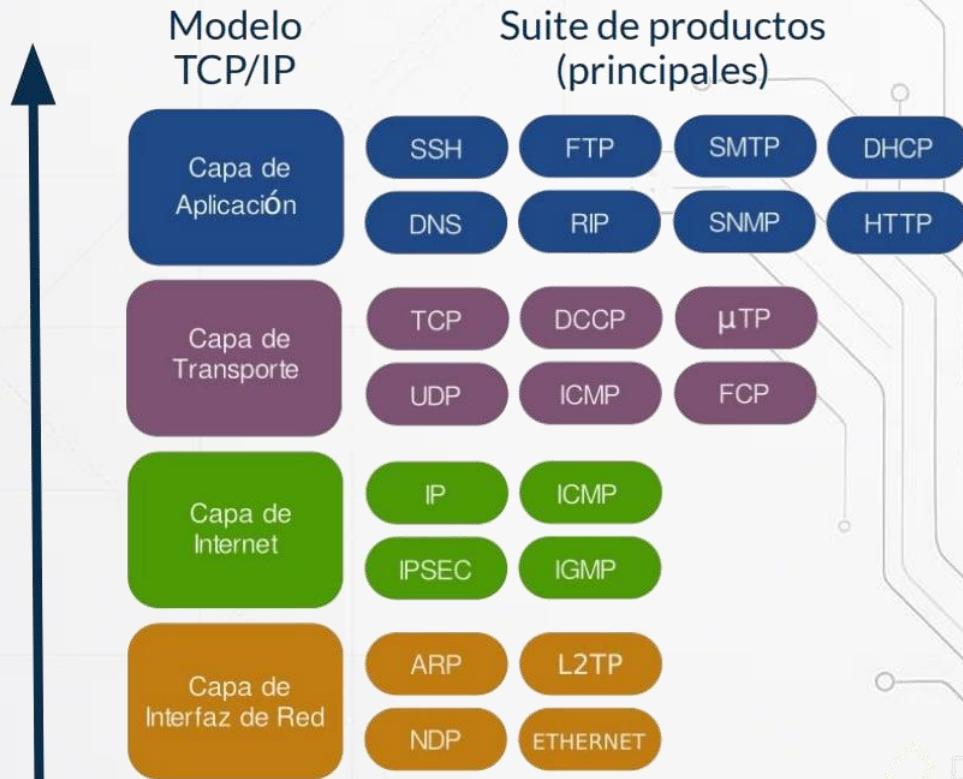
Esta capa se encarga de preparar los datos para que los pueda usar la capa 7. Aquí se maneja la conversión entre codificaciones, la compresión, el cifrado, etc.



**OSI capa 7 - capa de aplicación.** Esta es la capa correspondiente a los protocolos de red que necesitan las aplicaciones finales que ve el usuario. Un ejemplo es el protocolo HTTP en navegador web.



## MODELO TCP/IP



En líneas generales acerca del modelo TCP/IP podemos describir lo siguiente:

- Fue creado en la década de los 70's (anterior a OSI) y fue implantado en la red ARPANET, que sería la primera red WAN.
- La sigla TCP/IP significa *Transmission Control Protocol / Internet Protocol*.
- A diferencia del modelo OSI que se utiliza solo como referencia, el protocolo TCP/IP se emplea en la transmisión de datos a través de internet.
- Tiene 4 capas.

A continuación, explicare brevemente el funcionamiento de cada capa:

### **Capa 1: capa física de enlace de red.**

- Nivel más bajo de comunicación compuesto por pulsaciones eléctricas o transporte físico.
- Este protocolo no establece comunicación entre dos puntos, solo transmite en el medio físico.
- Equivalente a las capas 1 y 2 del modelo OSI.

Tiene protocolos como:

- ARP: *Address Resolution Protocol*. Encuentra la MAC de las IP.
- Ethernet: tecnología tradicional para conectar dispositivos en una red LAN.

### **Capa 2: capa de internet.**

- Se encarga de comunicar dos hosts para transmitir los datos y establecer la ruta para que la información llegue al destino deseado.
- Equivalente a la capa 3 del modelo OSI.

Tiene protocolos como:

- IP: *Internet Protocol*. Para identificación y comunicación.
- ICMP: *Internet Control Message Protocol*.
- IPSEC: *Internet Protocol security*. Son varios protocolos que autentican la IP y cifran los paquetes.
- IGMP: *Internet Group Management Protocol*. Multidifusión.

### **Capa 3: capa de transporte.**

- Equivalente a la capa 4 del modelo OSI.
- Sus protocolos principales son: TCP y UDP.
- Otros protocolos son:
  - DCCP: *Datagram Congestion Control Protocol*. Transporte de mensajes.
  - MTP: *Micro Transport Protocol*. Conexiones peer to peer.
  - ICMP: *Internet Control Message Protocol*. Mensajes de error e información operativa.
  - FCP: *Fibre Channel protocol*. Carga el S.O y verificación.

### **Capa 4: capa de aplicación.**

- Ofrece a las aplicaciones la capacidad de acceder a los servicios de las demás capas y define los protocolos utilizados para el intercambio de datos, como el correo electrónico (POP y SMTP), gestores de bases de datos y protocolos de transferencia de archivos (FTP). Equivalente a las capas 5, 6 y 7 del modelo OSI.

Tiene protocolos como:

- FTP: *File Transfer Protocol*. Transferencia de archivos.
- SSH: *Secure Shell*. Para conexiones seguras.
- SMTP: *Simple Mail Transfer Protocol*.
- DHCP: *Dynamic Host Configuration Protocol*.
- DNS: *Domain Name System*.
- RIP: *Routing Information Protocol*.
- SNMP: *Simple Network Management Protocol*.
- HTTP: *Hypertext Transfer Protocol*.

## ¿Y COMO SE APLICA TODO ESTO?

Los modelos OSI y TCP/IP con su sistema de capas tienen una influencia clara en la *búsqueda de soluciones cuando existe un problema de red*.

A continuación se dan 2 ejemplos prácticos de cómo estos modelos influyen en la comunicación de datos en una red empresarial y su implicancia en ciberseguridad.

### Ejemplo 1:

**Comunicación fallida entre dos computadores (A y B) en red interna**

#### 1. Capa Física (OSI capa 1 / TCP-IP parte de la capa Link)

##### Acción:

- Se verifica si los dispositivos están físicamente conectados.
- Revisión de: cables, conectores RJ-45, puertos del switch, NIC del PC, estado de los LEDs de red, etc.

##### Ejemplo concreto del caso:

"*¿Están conectados los dispositivos a la red?*". En muchos casos, el error era simplemente un cable mal conectado o dañado.

##### Herramientas posibles:

- Verificación visual
- Tester de red
- Reemplazo de cables
- LED del puerto encendido.

## **2. Capa de Enlace de Datos (OSI capa 2 / TCP-IP capa Link)**

### **Acción:**

- Comprobar si hay comunicación entre tarjetas de red y el switch.
- Validar direcciones MAC, si hay colisiones, errores de trama, o problemas con VLANs.

### **Ejemplo concreto del caso:**

Se revisa que las tarjetas de red funcionen, estén activadas, no tengan conflictos y estén en la VLAN correcta si aplica.

### **Herramientas posibles:**

- ipconfig /all o ifconfig para ver dirección MAC.
- Logs del switch o consola de administración.
- Ping a la puerta de enlace.

## **3. Capa de Red (OSI capa 3 / TCP-IP capa Internet)**

### **Acción:**

- Verificar direcciones IP, máscara de subred, puerta de enlace y rutas.
- Confirmar que los dos dispositivos estén en la misma red o segmento, o que el enrutamiento sea correcto si están en diferentes redes.

### **Ejemplo concreto del caso:**

Si el computador A tiene IP 192.168.**1**.10 y el B tiene 192.168.**2**.10 sin un router que los conecte, no se podrán comunicar.

### **Herramientas posibles:**

- ping, tracert o traceroute.
- ipconfig, route print.
- Revisión de tabla de rutas y configuración de Gateway.

## **4. Capa de Transporte (OSI capa 4 / TCP-IP capa Transporte)**

### **Acción:**

- Verificar si la comunicación es confiable o no.
- Revisar si hay bloqueo de puertos TCP o UDP por parte de un firewall o error en la apertura de sockets.

### **Ejemplo concreto del caso:**

Puede haber un firewall bloqueando el puerto 445 (SMB) y eso impide compartir archivos entre los equipos.

### **Herramientas posibles:**

- netstat, telnet, nc (netcat).
- Logs de firewall o antivirus.
- Desactivación temporal de firewall para probar.

## **5. Capa de Aplicación (OSI capa 7 / TCP-IP capa Aplicación)**

### **Acción:**

- Verificar si el servicio final funciona correctamente (compartición de archivos, acceso remoto, impresión, etc.).
- Validar credenciales, permisos, configuraciones de red compartida, etc.

## **Ejemplo concreto del caso:**

El recurso compartido está bien configurado pero el usuario no tiene permisos para acceder a la carpeta en el otro equipo.

## **Herramientas posibles:**

- Revisar configuración de servicios (SMB, HTTP, FTP, etc.)
- Logs del sistema operativo
- Revisión de políticas de grupo o permisos NTFS

## **Resultado Final**

Gracias al enfoque estructurado por capas del modelo OSI/TCP-IP, se puede diagnosticar la causa exacta del problema y solucionarlo de forma ordenada, desde lo más básico (capa física) hasta lo más complejo (servicio o aplicación).

## Ejemplo 2

**Un empleado envía un correo electrónico desde la oficina.**

### Contexto

- Empresa con red interna.
- El empleado usa Outlook para enviar un correo a un cliente externo.
- La red pasa por firewall, proxy, switch, router y usa servicios como DNS y SMTP.

### 1. Capa Aplicación (OSI capa 7 / TCP-IP capa 4: Aplicación)

- El empleado escribe el correo en Outlook (aplicación).
- Outlook usa el protocolo SMTP para enviar el mensaje y DNS para resolver el dominio del destinatario (cliente@empresa.com → IP).
- Se manejan protocolos nivel usuario: SMTP, DNS, HTTP, FTP, etc.

### 2. Capa de Transporte (OSI capa 4 / TCP-IP capa 3: Transport)

- Se usa TCP, que divide el correo en segmentos y asegura que se entreguen de forma confiable.
- Si un segmento se pierde, TCP lo reenvía automáticamente (control de errores y flujo).
- Puerto usado: 25 (SMTP) para salida.

### 3. Capa de Red (OSI capa 3 / TCP-IP capa 2: Internet)

- El sistema consulta al servidor DNS para obtener la IP del destinatario.
- Se crea un paquete IP con la dirección IP de origen (empresa) y destino (servidor externo).
- Este paquete es enrutado por routers a través de Internet.

#### **4. Capa de Enlace de Datos (OSI capa 2 / TCP-IP capa 1: Network Access o Link)**

- El paquete IP es encapsulado en tramas Ethernet.
- Estas tramas incluyen la MAC de origen y destino (por ejemplo, del PC al switch o del switch al router).
- Aquí actúan switches, tarjetas de red (NIC), y se aplican reglas como VLAN, filtrado MAC, etc.

#### **5. Capa Física (OSI capa 1 / TCP-IP parte de la capa Link)**

- Las tramas se convierten en señales eléctricas, ópticas o inalámbricas y viajan por el cableado de red, fibra óptica o WiFi.
- Aquí están los cables, conectores, interfaces, repetidores, etc.

#### **Resultado:**

El correo viaja desde Outlook en la red local de la empresa hasta el servidor de correo del cliente externo, pasando por todas las capas. Cada capa agrega o interpreta información específica y permite que la comunicación sea estructurada, segura y eficiente.

#### **¿Por qué es importante entender esto en ciberseguridad?**

*Porque cuando hay un problema (ataque, pérdida de conexión, tráfico sospechoso), debes saber en qué capa ocurre, qué protocolo está implicado, y cómo solucionarlo o protegerlo (firewall en capa 4, IPS en capa 3, WAF en capa 7, etc.).*

## Resumen de ejemplos presentados

*Comunicación fallida entre dos computadores (A y B) en red interna*

Modelo OSI	Modelo TCP/IP	Acción de diagnóstico y solución (PC A y PC B)
Capa 1: Física	Capa 1: Link (Acceso red)	Verificar cables, puertos, conectores, tarjetas de red. ¿Están bien conectados? ¿Hay luz en el puerto de red?
Capa 2: Enlace de Datos	Capa 1: Link (Acceso red)	Revisar funcionamiento de las tarjetas de red, direcciones MAC, colisiones, pertenencia a VLANs.
Capa 3: Red	Capa 2: Internet	Comprobar direcciones IP, máscara de subred, puerta de enlace. ¿Están en el mismo segmento de red?
Capa 4: Transporte	Capa 3: Transporte	Verificar puertos abiertos, bloqueo de firewall, conectividad TCP/UDP. ¿Hay puertos bloqueados?
Capa 5: Sesión	Incluida en Aplicación	Validar que se pueda establecer sesión entre los equipos, por ejemplo, para compartir archivos.
Capa 6: Presentación	Incluida en Aplicación	Confirmar que los formatos de datos se interpretan correctamente si se usa alguna aplicación entre los equipos.
Capa 7: Aplicación	Capa 4: Aplicación	Verificar que el servicio que se intenta usar (impresora compartida, acceso remoto, etc.) funcione correctamente

*Un empleado envía un correo electrónico desde la oficina*

Modelo OSI	Modelo TCP/IP	Función en el ejemplo (correo saliente)
Capa 7: Aplicación	Capa 4: Aplicación	El usuario usa Outlook para redactar y enviar un correo. Se usa SMTP para enviar y DNS para resolver la IP.
Capa 6: Presentación	Incluida en Aplicación	Outlook codifica el contenido del mensaje (texto, adjuntos) para que sea interpretado correctamente.
Capa 5: Sesión	Incluida en Aplicación	Outlook establece y mantiene una sesión con el servidor de correo.
Capa 4: Transporte	Capa 3: Transporte	Se usa <b>TCP</b> para dividir el mensaje en segmentos y garantizar su entrega sin errores.
Capa 3: Red	Capa 2: Internet	Se construye un <b>paquete IP</b> con IP de origen y destino. Router enruta el paquete hacia su destino.
Capa 2: Enlace de Datos	Capa 1: Link (Acceso red)	Se crean tramas con dirección MAC de origen y destino. Se usan switches para el envío dentro de la LAN.
Capa 1: Física	Capa 1: Link (Acceso red)	El mensaje viaja como señales eléctricas por cables Ethernet o como señales ópticas por fibra.

## Equipos de comunicación y protocolos asociados

### Modelo OSI

Nº	Capa OSI	Dispositivos asociados	Protocolos / Tecnologías	Relación con Ciberseguridad
7	Aplicación	Software (Outlook, navegador, cliente FTP, etc.)	HTTP/S, FTP, DNS, SMTP, SNMP, Telnet, SSH	Donde ocurren muchos ataques: phishing, inyecciones, XSS, malware. Se protegen con <b>WAF</b> , filtros DNS, antivirus.
6	Presentación	Software intermedio (códecs, cifrado)	SSL/TLS, JPEG, ASCII, JSON, XML	Criptografía y cifrado de datos (TLS/SSL). <b>Cifrado débil = vulnerabilidad.</b>
5	Sesión	Software de control de sesión (servidores, autenticadores)	NetBIOS, RPC, PPTP	Establecimiento/control de sesiones. Vulnerable a secuestro de sesión o ataques MITM.
4	Transporte	Firewalls, balanceadores de carga	TCP, UDP, SCTP	Ataques DDoS, escaneo de puertos, secuestro de sesión TCP. Control de tráfico por <b>firewalls</b> .
3	Red	Routers, Firewalls, IPS/IDS	IP, ICMP, IPSec, OSPF, BGP	Suplantación IP (IP spoofing), ICMP flooding. Defensas: <b>IPSec, ACLs, IDS/IPS</b> .
2	Enlace de Datos	Switches, bridges, NIC	Ethernet, ARP, PPP, STP, VLAN	Ataques: ARP spoofing, MAC flooding. Defensa con <b>port security, VLANs, NAC</b> .
1	Física	Cables, conectores, hubs, repetidores, interfaces físicas	No hay protocolos, solo medios: UTP, fibra, radio, etc.	Corte de cables, interferencias, espionaje físico. Protección física y control de acceso.

### Modelo TCP/IP

Nº	Capa TCP/IP	Equivalencia OSI	Dispositivos / Protocolos	Relación con Ciberseguridad
4	Aplicación	Capas 5-7 (Aplicación, Sesión, Presentación)	HTTP/S, DNS, FTP, SSH, SNMP, SMTP, etc.	Protecciones: <b>WAF, autenticación multifactor, antivirus, TLS, antiphishing</b> .
3	Transporte	Capa 4 (Transporte)	TCP, UDP, SCTP	Escaneo de puertos, manipulación de paquetes, <b>firewall a nivel de puertos, control de tráfico</b> .
2	Internet	Capa 3 (Red)	IP, ICMP, ARP, IGMP, IPSec	Ataques: IP spoofing, sniffing, routing attacks. Defensa: <b>IPSec, filtrado IP, IDS/IPS</b> .
1	Acceso a Red (Link)	Capas 1-2 (Física y Enlace)	Ethernet, WiFi, PPP, Frame Relay, VLAN	ARP spoofing, sniffing, acceso físico no autorizado. Protección: <b>ACLs, VLAN, NAC, segmentación</b> .

## Resumen de la relación con Ciberseguridad por capas

- **Capa 7 (Aplicación):** Ataques como inyección SQL, XSS, y explotación de APIs o servicios web.
  - Defensa: WAF, autenticación, validación de entrada.
- **Capas 6-5 (Presentación/Sesión):** Se asegura la integridad y confidencialidad de la información, evitando intercepciones.
  - Defensa: SSL/TLS, gestión de sesiones seguras.
- **Capa 4 (Transporte):** Se puede hacer escaneo de puertos o ataques de denegación de servicio (DoS).
  - Defensa: Firewalls, IDS/IPS, rate limiting.
- **Capa 3 (Red):** Se atacan rutas o direcciones IP, como el IP spoofing o ICMP flooding.
  - Defensa: VPN, IPSec, reglas de firewall de capa 3.
- **Capa 2 (Enlace):** Riesgo de ataques internos como ARP Spoofing, suplantación de MAC o sniffing.
  - Defensa: Port security, ARP inspection, VLANs.
- **Capa 1 (Física):** Ataques físicos o interrupciones.
  - Defensa: Control de acceso físico, monitoreo, blindaje de cable.

## ENTONCES...

### ¿Por qué es importante conocer el modelo OSI y TCP/IP en ciberseguridad?

Porque todo ataque, defensa, monitoreo o análisis forense en ciberseguridad ocurre en alguna capa de red. Entender cómo se estructura y comunica una red permite:

- Detectar dónde ocurre una intrusión.
- Elegir el control de seguridad adecuado.
- Analizar el tráfico y las vulnerabilidades con mayor precisión.

### ¿Por qué son clave para un profesional de ciberseguridad?

Porque cada ataque o defensa ocurre en una o más capas. Saber en qué capa ocurre un ataque te dice:

- Qué **herramienta o técnica usar**
- Dónde **poner controles**
- Cómo **reaccionar o prevenir**

### 3 ejemplos concretos de aplicación profesional

**Ejemplo 1:** Análisis de tráfico con Wireshark.

#### Situación real:

Un servidor interno comienza a responder lento. Sospechas de una intrusión o de tráfico anómalo y decides capturar paquetes con Wireshark.

#### ¿Qué verás?

Miles de líneas con columnas como: "Frame", "Ethernet II", "IP", "TCP", "HTTP", etc.

Esto corresponde directamente a las capas OSI:

Protocolo	Capa OSI	Qué puedes detectar
Ethernet II	Capa 2 - Enlace de datos	Ataques como ARP Spoofing o cambios de MAC
IP	Capa 3 - Red	IP spoofing, rutas maliciosas
TCP	Capa 4 - Transporte	Conexiones sospechosas, escaneo de puertos, SYN flood
HTTP	Capa 7 - Aplicación	Exfiltración de datos, malware comunicándose con el atacante

#### ¿Por qué necesitas conocer el modelo OSI?

- Porque Wireshark no te explica qué significa cada protocolo. Lo hace visible, pero si tú no sabes que TCP está en la capa 4 y HTTP en la 7, te vas a perder.
- Por ejemplo: Si ves que alguien está usando el puerto 80, ¿significa que es HTTP? No necesariamente. Pero si entiendes que la capa 4 maneja puertos y la capa 7 el protocolo, sabes qué buscar.

**Conclusión:** Puedes usar Wireshark sin saber OSI, pero no sabrás interpretar lo que ves ni sabrás qué parte de la red proteger. Estarás a ciegas.

## **Ejemplo 2:** Configuración de un firewall de nueva generación (NGFW).

### **Situación real:**

Tu empresa sufre un ataque desde Internet. El firewall actual solo filtra IPs y puertos. El jefe de TI quiere instalar un “firewall más inteligente”, que detecte ataques a la aplicación web.

### **¿Qué hace un NGFW?**

- Bloquea tráfico según IP (capa 3).
- Bloquea tráfico según puertos y protocolos como TCP/UDP (capa 4).
- Analiza contenido de protocolos como HTTP, HTTPS, DNS (capa 7).
- Tiene funciones de IDS/IPS para detectar comportamientos maliciosos

### **¿Por qué es vital el modelo OSI/TCP-IP?**

- Para configurar un WAF (Web Application Firewall), debes saber que trabaja en capa 7.
- Para bloquear un ataque DoS por TCP SYN Flood, debes aplicar reglas en capa 4.
- Si ves ataques desde IPs sospechosas, puedes aplicar bloqueos en capa 3.

**Conclusión:** Sin saber qué hace cada capa, puedes bloquear donde no corresponde o dejar abierta una puerta crítica.

### Ejemplo 3: Ataque ARP Spoofing dentro de la red local.

#### Situación real:

Un atacante conectado a la red WiFi en una empresa ejecuta un ataque ARP spoofing para interceptar tráfico entre los empleados y el router.

#### ¿Qué es ARP?

Es un protocolo que vive en la capa 2 del modelo OSI. Asocia direcciones IP con direcciones MAC.

#### ¿Qué hace el atacante?

- Envía respuestas ARP falsas, diciendo: "Yo soy el router".
- Las víctimas envían su tráfico al atacante, sin saberlo (*Man-in-the-Middle*).
- Si no está cifrado, puede ver contraseñas, correos, etc.

#### ¿Cómo se defiende un profesional?

- Conoce que esto ocurre en capa 2, así que no busca soluciones en firewall (capa 4), ni en IPtables (capa 3), ni en antivirus (capa 7).
- Aplica: Dynamic ARP Inspection, segmentación de VLANs, o implementa sniffers para confirmar el ataque.

**Conclusión:** Sin saber que **ARP opera en capa 2**, podrías perder días buscando el problema en un firewall o en el servidor web.



**OOPS...**

En este punto, talvez por mi formación académica anterior o mi estructura mental de no soltar hasta que estoy fuera de toda duda, una parte de mi sigue reticente a aceptar de forma plena las razones sobre él porque alguien que se dedica a ciberseguridad DEBE tener conocimiento de los modelos OSI y TCP, hasta que lei el siguiente ejemplo con ayuda de la ia:

## **ESCENARIO:**

### **Tráfico anómalo en la red – análisis con Wireshark**

#### **Situación real:**

Una empresa nota que un servidor de archivos (por ejemplo, 192.168.1.10) *responde lento* y que *hay picos de uso de ancho de banda*. Sospechan que alguien está sacando información sin autorización.

Te entregan un archivo .pcap (captura de red hecha con Wireshark) y te dicen:

*"Revisa si hay algo raro en el tráfico de este servidor. Algo está pasando."*

#### **Paso a paso sin saber modelo OSI (ni TCP/IP)**

*Tú sabes abrir Wireshark, pero no sabes lo que significa cada protocolo ni a qué nivel opera.*

1. Abres el archivo .pcap.
2. Ves muchas líneas con columnas como:  
No. | Time | Source | Destination | Protocol | Info
3. Ves protocolos como TCP, ARP, HTTP, DNS, TLSv1.2...  
→ Pero no sabes qué hace cada uno ni qué importancia tienen.
4. Filtras por  
`ip.addr == 192.168.1.10`  
→ Ves cientos de conexiones hacia direcciones externas, muchas por HTTP.
5. Te preguntas:  
"¿Está bien que use HTTP?"  
"¿Por qué hay tantas conexiones?"  
"¿Esto es tráfico normal o es un ataque?"  
"¿Dónde empiezo a mirar?"

## Mismo paso a paso **sabiendo** modelo OSI (y TCP/IP)

Tú sabes cómo fluye el tráfico por capas y qué significan los protocolos según la capa.

### PASO 1. Sabes qué ver en cada capa.

Tienes esto en mente:

Capa OSI	Qué revisas
2 - Enlace	¿Quién está enviando paquetes? ¿Hay duplicación de MAC? ¿Spoofing?
3 - Red	¿Hay direcciones IP desconocidas? ¿IP spoofing?
4 - Transporte	¿Qué puertos se están usando? ¿Hay puertos sospechosos?
7 - Aplicación	¿Qué protocolos de aplicación se usan? ¿Se exfiltran datos por HTTP, DNS?

### PASO 2. Filtras por dirección del servidor.

ip.addr == 192.168.1.10

### PASO 3 – Analizas capa por capa

- **Capa 2 (Enlace de datos)**

Ves que el servidor responde siempre con la misma MAC. No hay duplicación ni ARP falsos.

→ No parece un ataque en capa 2 (descartas ARP spoofing).

- **Capa 3 (Red)**

Todas las conexiones salen desde su IP hacia IPs públicas (por ejemplo, 34.104.18.90, 142.250.190.78).

→ Verificas si esas IPs son legítimas con `whois/dns`. Si son sospechosas, podría estar enviando datos a un C2 (comando y control).

- **Capa 4 (Transporte)**

Filtras por puerto:

tcp.port == 80

→ Ves que hay tráfico HTTP no cifrado.

- **Capa 7 (Aplicación)**

Sigues el flujo:

Click derecho en paquete HTTP → Follow → HTTP stream

→ Descubres que está enviando logs internos del servidor por HTTP

a una IP de EEUU. **iExfiltración de datos!**

## ¿Qué hizo la diferencia?

<b>Sin modelo OSI</b>	<b>Con modelo OSI</b>
No sabes dónde mirar	Sabes por dónde empezar (capa 2 a capa 7)
No sabes qué protocolos ver	Identificas qué capa usa cada protocolo
No sabes si algo es normal	Reconoces patrones por capa y protocolo
Solo ves datos	Entiendes comportamiento (por qué ocurre)

## Conocimiento aplicado

Debido a que conoces OSI y TCP/IP:

- Sabes que HTTP (capa 7) no debe usarse en tráfico sensible.
- Sabes que IPs raras (capa 3) deben investigarse.
- Sabes que el servidor no usa cifrado (capa 6), y eso es un riesgo.

Puedes levantar un informe con fundamentos técnicos sólidos:

*"Se detectó exfiltración de datos mediante protocolo HTTP (capa 7) desde IP 192.168.1.10 a IP pública no autorizada. El tráfico no está cifrado, lo que expone información sensible. Se recomienda bloquear conexiones salientes por puerto 80 en capa 4 y revisar el proceso que genera esta conexión."*

## Conclusión

Si no entiendes el modelo OSI y TCP/IP, estás adivinando cuando haces análisis.

Con ese conocimiento, pasas de ser "el que mira Wireshark" a ser **el que realmente investiga, detecta y mitiga amenazas**.