UNIVERSIDAD MARIANO GÁLVEZ

INGENIERÍA EN SISTEMAS DE

INFORMACIÓN Y CIENCIAS DE LA COMPUTACIÓN

SEGURIDAD Y AUDITORÍA DE SISTEMAS

SECCIÓN B

COMPARATIVA MODELO TCP/IP Y MODELO OSI

MARIO ROBERTO MANZO ESTRADA **5190 05 3915**

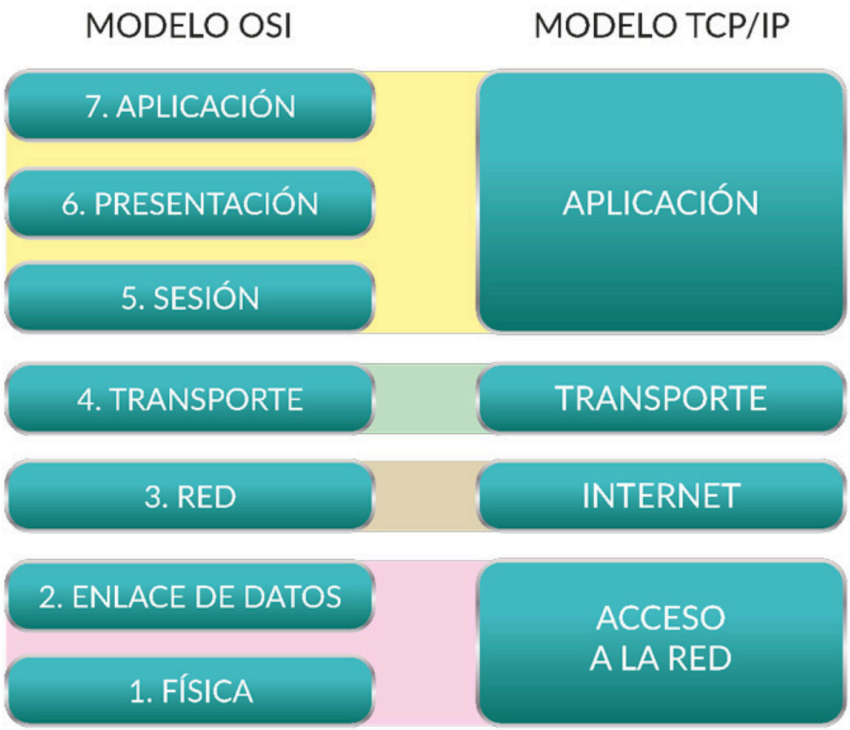
VILLA NUEVA, GUATEMALA, AGOSTO 2021

Modelo TCP/IP

Las siglas de TPC/IP significan transmisión control protocol/internet protocol, que en su traducción al español es protocolo de control de transmisión/protocolo de internet, estas reglas permiten la comunicación de equipos a través de una red. Este modelo es muy aceptado, mas aun cuando se toma como referencia el de cuatro capas: Aplicación, Transporte, Internet y Acceso a la red, aun que algunos otros como Tanembaum prefieren una capa adicional que es la física.

Modelo OSI

El modelo osi es un estándar busca conseguir la conexión de diferentes sistemas para que estos lleguen a poder intercambiar información sin ningún tipo de dificultad, el modelo osi a diferencia del modelo tcp/ip, maneja siete capas, cada una de estas capas realiza sus propias tareas, para que es conjunto consigan el mismo objetivo, las capas que comprende el modelo osi son: física, enlace de datos, red, transporte sesión, presentación y aplicación. El objetico de poder mantener las capas separadas, es hacer posible la comunicación de diferentes protocolos.



A continuación mostraremos una comparación entre ambos modelos, así como las posibles vulnerabilidades.

MODELO OSI		***MODELO TCP IP***		
Capa	***Definición***	***Capa***	***Definición***	***Vulnerabilidades***
Aplicación	*Igual la capa TCP/IP, es la encargada de conceder a los usuarios la ejecución de acciones o comandos en sus propias aplicaciones.*	*Aplicación*	*Esta provee de las funciones hacia los usuario, como los programas, también provee de un control de las conexiones entre aplicativos.*	*Consideramos que uno de los pundos debiles esta definido por el protocolo http, y esta dado a las malas practicas por parte de los desarrolladores ya que por medio de un link determinado pueden llegar obtener informacion de accesos si se envian datos confidenciales por metodos GET, o dejando sessiones activas durante su interaccion a sistemas web.*
Presentación	*Esta capa se encarga de mostrar toda la data que sea trasmitida, asi como asegurarse que los datos enviados sean entendibles sin importar los protocolos por los cuales sean enviados*			
Sesión	*Este permite manejar la comunicación entre los diferentes equipos, impide que se desactive la comunicación entre equipos que esten transmitiendo datos.*			
Transporte	*Este es el encagado del envio de los paquetes desde un punto origen hacia el punto destino*	*Transporte*	*es la capacidad que se tiene de transferencia de un punto hacia otro punto de los mensajes, independiente de la red subyacente*	*Las vulneravilidades detectadas en esta capa estan tomadas en base a la autenticacion de integración, y autenticación de confidencialida*

				relacionados con el acceso a los protocolos dentre las diferentes capas
Red	*Este permite poder determinar el enrutamiento de dos o mas redes*	*Internet*	*esta es la encargada del ruteo de los mensajes por medio del internet*	*Creemos que es la capa mas critica, lo primordial es poder tener un accesos a los paquetes que pasan por la red, los cuales pueden ser capturados por algun software espia utilizando procesos conocidos como Sniffing*
Enlace de datos	*Permite proporcionar los elementos necesarios para realizar una comunicación entre los elementos físicos*	*Acceso a la red*	*esta capa incluye los protocolos cuyo equipo necesita para proporcionar datos hacia otros equipos que estén conectados a una red*	*Este capa pudiera presentar problemas si no se tiene un control de las personas que tienen accceso a nuestros centros de datos, mas que todo se trata de de la confidencialidad accesos que maneja cada persona.*
Física	*Este se encarga esplicitamente de los componentes físiscos de una conexión.*			