23/10/25

# Redes De Computadoras II

## Técnicas de seguridad en redes


Alumno: Jared López Toledo
Profesor: Carlos Mijangos Jiménez

# Contenido

# Técnicas de seguridad de redes

## Control de acceso

Todos hemos utilizado una contraseña para iniciar sesión en un equipo, red o aplicación, a esto lo llamamos control de acceso. Se divide en cuatro partes: identificación, autenticación, autorización y responsabilidad (IAAR).

El sistema inicia confirmando la identidad del usuario a través de un identificador único como su ID (abreviatura del inglés «Identification»), nombre de usuario o número de cuenta. Después, autentifica la identidad mediante la verificación de las credenciales del ID y la contraseña para luego concederle la autorización y acceder. Y por último, la responsabilidad, que consta de hacer un seguimiento de la actividad del usuario para que se hagan responsables de sus acciones en un sistema.

## Segmentación de la red

Se encarga de separar una red en partes lógicas más pequeñas para que se puedan agregar controles entre ellas, favoreciendo el rendimiento y la seguridad.

Un método común de segmentación de la red son las redes de área local virtual (VLAN o Virtual Local Area Network) y cuando son utilizadas para una infraestructura en la nube, se denominan nubes privadas virtuales (VPC o Virtual Private Cloud).

## Seguridad perimetral

Las redes tradicionales cumplen sus funciones en un datacenter físico con un perímetro definido conectado con el mundo exterior. Es fundamental que cuando se define un perímetro, se determinen qué datos, voz y vídeo pueden pasar para configurar los mecanismos de control de acuerdo a ellos.

Por ejemplo, están los firewalls (FW), el sistema de detección de intrusiones (IDS o Intrusion Detection System) y el sistema de prevención de intrusiones (IPS o Intrusion Prevention System).

## Cifrado de datos

La confidencialidad y la integridad están garantizadas con el cifrado de datos, ya que los datos en tránsito o en reposo se cifran y utilizan una clave. Existen dos tipos esenciales de cifrado: la encriptación simétrica y la asimétrica.

- La simétrica consta de una única clave que se comparte entre el remitente y el receptor, siendo descifrada en menor tiempo que la asimétrica, la cual emplea dos claves, una pública y una privada para descifrar la información, haciéndola menos vulnerable.

  En trámites bancarios necesitamos que el ingreso de la sesión sea confidencial, por lo que se usa un cifrado simétrico y para asegurar la autenticidad de la página web, se emplea un cifrado asimétrico para que se intercambie de manera segura las claves del cifrado simétrico de esa sesión.

## Seguridad Física

A menudo olvidada, esta técnica protege el acceso físico a los componentes de la red.

- Salas de servidores (Data Centers) cerradas con llave.
- Control de acceso con tarjetas o biométricos para áreas restringidas.
- Videovigilancia (CCTV).
- Protección de puertos de red no utilizados en oficinas para evitar que alguien conecte un dispositivo no autorizado

## Concienciación y Capacitación del Usuario (El Factor Humano)

Esta técnica se enfoca en educar a los usuarios y al personal para que reconozcan las amenazas y sigan las mejores prácticas de seguridad.

Capacitación contra la Ingeniería Social: Enseñar a los empleados a reconocer tácticas de manipulación psicológica. Esto incluye:

- Phishing y Spear Phishing: Identificar correos electrónicos, mensajes de texto (smishing) o llamadas (vishing) fraudulentas que intentan robar credenciales o instalar malware.
- Pretexting: Reconocer cuando un atacante inventa un escenario (ej. "Soy de soporte técnico y necesito tu clave para una actualización urgente") para obtener información.
- Políticas de Uso Aceptable (AUP): Reglas claras sobre lo que los empleados pueden y no pueden hacer con los recursos de la red (ej. prohibir la instalación de software no autorizado, no conectar dispositivos USB personales o desconocidos).
- Gestión de Contraseñas Seguras: Fomentar el uso de contraseñas largas y complejas, no reutilizarlas, y promover el uso de gestores de contraseñas.
- Procedimientos de Reporte de Incidentes: Asegurarse de que cada empleado sepa exactamente qué hacer y a quién contactar inmediatamente si sospecha de una brecha de seguridad o un correo malicioso.
- Simulacros de Phishing: Realizar pruebas controladas enviando correos de phishing falsos (pero seguros) a los empleados para evaluar su nivel de concienciación y ofrecer formación adicional a quienes caigan en la trampa.