

TALLER No. 3 – SEGURIDAD PERIMETRAL

1. ¿En qué consiste la seguridad perimetral?

La **seguridad perimetral** consiste en el conjunto de **medidas, dispositivos y estrategias** que se implementan para **proteger los límites de una red informática o de una infraestructura física**.

Su objetivo principal es **evitar el acceso no autorizado** desde el exterior, detectar amenazas, y garantizar la integridad, confidencialidad y disponibilidad de la información.

En el ámbito tecnológico, se centra en:

- Firewalls (cortafuegos)
- Sistemas de detección y prevención de intrusos (IDS/IPS)
- VPN (Redes privadas virtuales)
- Filtrado de contenido
- Segmentación de redes

Ejemplo:

Un firewall que bloquea intentos de conexión sospechosos desde internet hacia los servidores internos de una empresa.

2. Importancia de la seguridad perimetral (según el video y análisis)

La seguridad perimetral es **vital** porque actúa como la **primera línea de defensa** ante los ciberataques.

Sin ella, la red interna estaría totalmente expuesta a:

- Hackeos,
- Robo de datos,
- Ataques de malware,
- Pérdida de información crítica.

Además, **reduce los riesgos operativos**, mejora la **confianza del cliente** y **cumple con normativas de seguridad informática**.

En el video se destaca que permite **monitorear constantemente el tráfico**, detectar anomalías y **bloquear amenazas en tiempo real**.

3. Principales funciones de la seguridad perimetral

1. **Control de acceso:** Permite definir quién puede ingresar y desde dónde.
 2. **Filtrado de tráfico:** Revisa los paquetes de datos que entran o salen para detectar amenazas.
 3. **Prevención de intrusos:** Detecta ataques o comportamientos inusuales (IDS/IPS).
 4. **Cifrado de información:** Protege los datos en tránsito mediante protocolos seguros (SSL, VPN).
 5. **Monitoreo continuo:** Supervisa la red en tiempo real para identificar incidentes.
 6. **Gestión de vulnerabilidades:** Analiza posibles fallas en el sistema y aplica parches o bloqueos.
-

5. ¿Por qué es importante la seguridad perimetral en las aplicaciones de desarrollo?

La seguridad perimetral en aplicaciones de desarrollo es esencial porque:

- **Evita accesos no autorizados** al entorno de desarrollo, pruebas y producción.
- **Protege los servidores** donde se alojan las aplicaciones, bases de datos y API.
- **Asegura la comunicación** entre componentes mediante protocolos cifrados.
- **Previene ataques comunes**, como inyección de código o robo de información del sistema.
- **Cumple estándares de seguridad** exigidos por la industria (ISO 27001, OWASP, GDPR, etc.).

Ejemplo:

Si un desarrollador trabaja en una aplicación web, la seguridad perimetral evita que un hacker acceda al servidor de desarrollo y robe el código fuente o los datos de usuarios.