sustantiva
CON•SENTIDO

Energiza!

Estrategias de Segmentación y Seguridad de Redes de Datos

Introducción

Introducción

- Las redes de datos son esenciales para la operación de cualquier organización moderna.
- El aumento de amenazas cibernéticas exige estrategias robustas de seguridad.
- Esta presentación cubre la **seguridad en redes**, **segmentación**, **protocolos seguros**, y **auditorías de seguridad**.

Reconocimiento de Amenazas y Vulnerabilidades Comunes

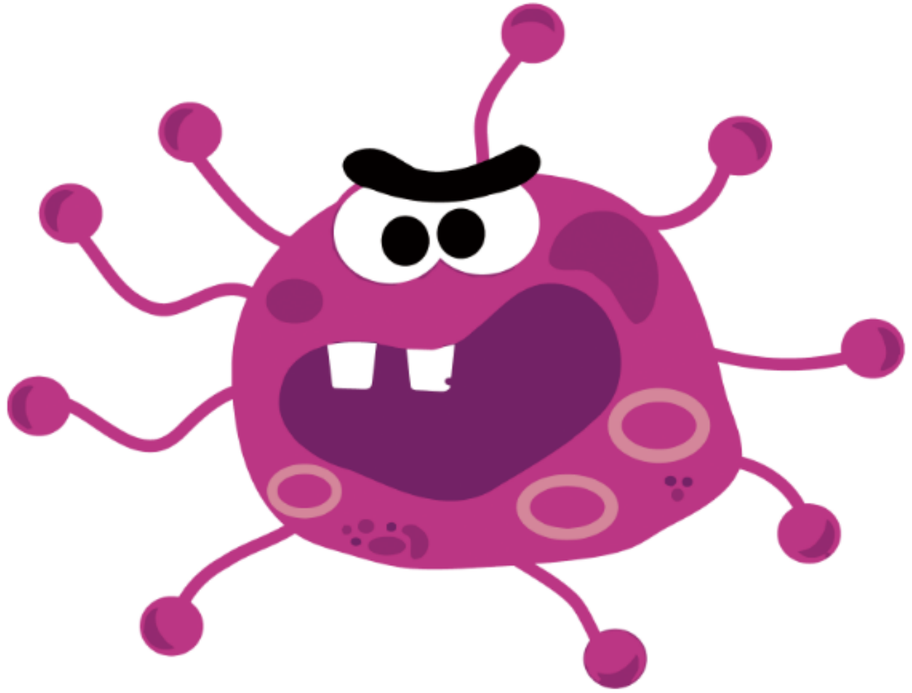
Reconocimiento de Amenazas y Vulnerabilidades Comunes

1.1 Amenazas comunes:

- Malware: Virus, ransomware, spyware que afectan la confidencialidad, integridad y disponibilidad de los datos.
- Phishing: Engaño para obtener credenciales o información confidencial.
- DoS/DDoS: Ataques que saturan los recursos de servidores y redes.

1.2 Vulnerabilidades recurrentes:

- Contraseñas débiles.
- Software desactualizado.
- Configuraciones inseguras de dispositivos.

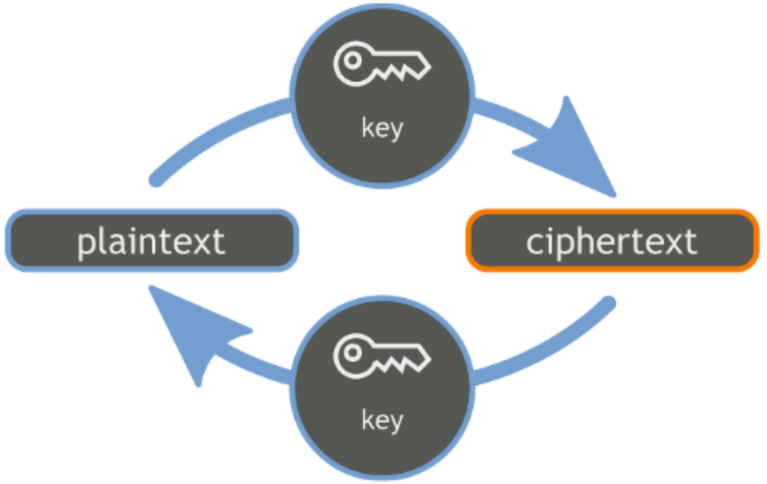


Protocolos de Comunicación Seguros

Protocolos de Comunicación Seguros

2.1 Protocolos recomendados:

- **HTTPS:** Protege la información mediante SSL/TLS.
- **VPN (Red Privada Virtual):** Cifra conexiones entre usuarios y redes.
- **SSH (Secure Shell):** Conexiones seguras de administración a servidores.



2.2 Criptografía y Autenticación:

- **Criptografía AES, RSA.**
- **Autenticación multifactor (MFA).**

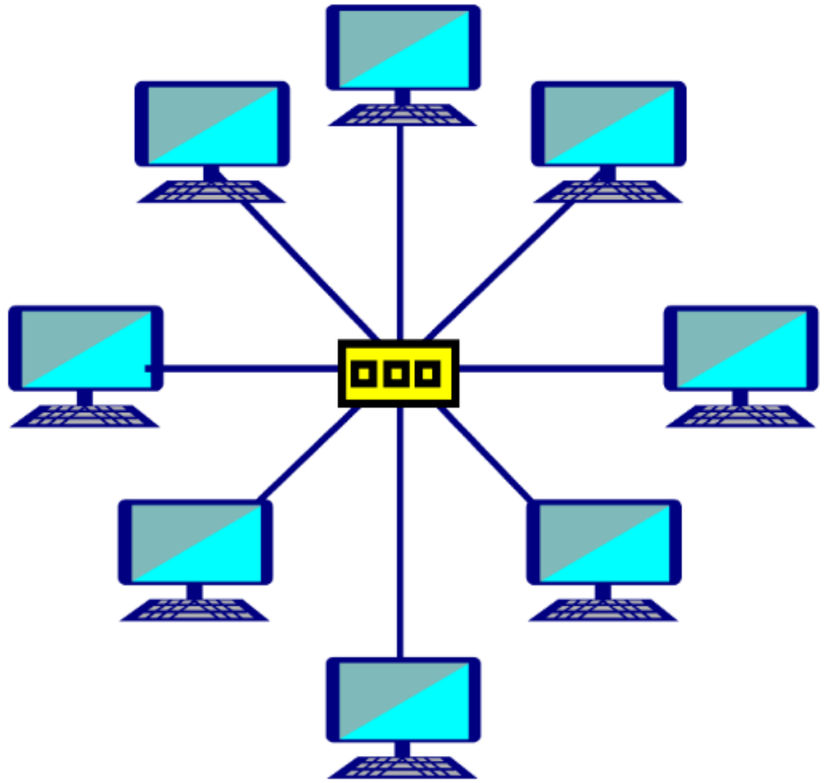
Arquitectura Defensiva de Redes

3.1 Segmentación de Red:

- Dividir redes en segmentos basados en función o nivel de acceso.
- **VLANs:** Aislar tráfico entre departamentos.

3.2 Firewalls:

- **Firewalls de filtrado de paquetes:** Analizan y bloquean tráfico según reglas.
- **Firewalls de inspección profunda:** Analizan el contenido de las tramas.



Sistemas de Detección y Prevención de Intrusiones

Sistemas de Detección y Prevención de Intrusiones (IDS/IPS)

- **IDS (Intrusion Detection System):** Detecta intrusiones y genera alertas.
- **IPS (Intrusion Prevention System):** Bloquea intrusiones activamente.
- **Monitoreo constante** del tráfico para identificar comportamientos anómalos.

VPN y Acceso Remoto Seguro

VPN y Acceso Remoto Seguro

- **VPNs:** Protegen las conexiones remotas cifrando el tráfico de datos.
- **Protocolos VPN recomendados:**
  - **IPsec**
  - **OpenVPN**
  - **WireGuard**

Evaluación Continua de Medidas de Seguridad

Evaluación Continua de Medidas de Seguridad

4.1 Auditorías de Seguridad:

- Evaluación periódica de políticas, configuraciones y cumplimiento normativo.
- Estándares: **ISO 27001**, **NIST**.

4.2 Pruebas de Penetración (Pentesting):

- Simulación de ataques reales para identificar vulnerabilidades.
- **Evaluación interna y externa** de posibles brechas de seguridad.

Gestión de Incidentes y Riesgos

Gestión de Incidentes y Riesgos

- **Evaluación de riesgos:** Determina amenazas, impacto y probabilidad.
- **Planes de respuesta a incidentes (IRP):** Define roles y procedimientos de respuesta rápida.

Conclusión

Conclusión

- **La seguridad en redes** debe ser un enfoque **proactivo** y **multicapa**.
- **Segmentación de red** y **uso de protocolos seguros** son esenciales para proteger los datos.
- La **evaluación continua** mediante auditorías y pruebas de penetración garantiza redes **resilientes** frente a amenazas.


Energiza!