🔐 Tema 72

Seguridad en Sistemas en Red

Servicios, Técnicas, Estándares

1. Fundamentos de la seguridad en red

1.1 Importancia

- Las redes son vectores constantes de ataque.
- Afecta a **disponibilidad**, **integridad** y **confidencialidad**.

1.2 Protección imprescindible

- La ciberseguridad comienza **en la red**.
- Control del **canal de datos** = clave.

2. Servicios de seguridad

2.1 Autenticación y autorización

- Métodos: Contraseñas, MFA, biometría
- Protocolos: **Kerberos**, **OAuth2**, **SSO**

2.2 Control de acceso

- Modelos: **RBAC**, **ABAC**
- Tecnologías: VLANs, **NAC**, **ACL**

2. Servicios de seguridad (II)

2.3 Cifrado y no repudio

- Herramientas: HTTPS, VPN, cifrado disco, **firmas digitales**

2.4 Auditoría y SIEM

- **SIEM** = análisis + gestión de eventos
- Ejemplos: **Wazuh**, **Splunk**

3. Técnicas de protección

3.1 Segmentación de red

- VLANs
- Microsegmentación
- SDN (redes definidas por software)

3.2 Bastionado (hardening)

- Eliminar servicios innecesarios
- Refuerzo de configuraciones
- Automatización: **Ansible**

3. Técnicas de protección (II)

3.3 Prevención de amenazas

- **EDR** (Endpoint Detection and Response)
- **DNSSEC**
- Bloqueo de IPs maliciosas

4. Defensa en profundidad

4.1 Firewalls de nueva generación (NGFW)

- Inspección profunda
- Filtro por aplicación
- Bloqueo en tiempo real

4.2 IDS e IPS

- IDS = detección
- IPS = prevención activa

4.3 Copias de seguridad

- Regla **3-2-1**
  3 copias, 2 medios, 1 externa

5. Normativa y estándares

5.1 Estándares técnicos

- ISO 27001, NIST SP 800-53, COBIT, MITRE ATT&CK

5.2 Legislación vigente

- RGPD, LOPDGDD, ENS, NIS2

5.3 Evaluación de riesgos

- MAGERIT y PILAR

6. Amenazas actuales

- **Man-in-the-Middle (MITM)**
- **Ransomware**
- Fallos de configuración en **cloud**
- **DDoS**: tráfico masivo → caída del servicio

7. Concienciación y formación

- El usuario = **primera línea de defensa**
- Campañas: phishing, ingeniería social, ransomware
- Actividades: **CyberCamp**, **CTFs**, tests de impacto

✅ Conclusión

- La seguridad en red es **multicapa**, proactiva y normativa.
- Implica herramientas, **cultura de seguridad** y actualizaciones continuas.
- ¡Una red protegida = usuarios y datos protegidos!