






Tema 44

Técnicas y Procedimientos para la Seguridad de los Datos

1.1 Contexto y Principios Fundamentales

- La **pérdida de datos** implica riesgos económicos, legales y de reputación.
- Principios clave de la seguridad:
 -  Confidencialidad
 -  Integridad
 -  Disponibilidad
 -  Autenticidad
 -  No repudio

Líneas de defensa

- **Seguridad activa:** prevención, detección (firewalls, antivirus, alertas)
- **Seguridad pasiva:** respuesta, recuperación (backups, auditorías)

1.2 Servicios Clave de Seguridad

Confidencialidad

- Cifrado en tránsito (TLS/SSL) y reposo (AES, RSA)
- Clasificación de datos
- Control de acceso (RBAC, Zero Trust)



Integridad

- Hashes seguros (SHA-256)
- Firmas digitales
- Herramientas de integridad: Tripwire
- Restricciones de integridad en BD: `CHECK` , `UNIQUE`

Disponibilidad

- Estrategia de copias 3-2-1
- Clústeres, failover, replicación
- DRP: Planes de recuperación ante desastres

Autenticidad y No repudio

- Autenticación robusta (MFA, biometría)
- Timestamps + firma digital para garantizar trazabilidad



1.3 Técnicas Avanzadas de Protección

- Cifrado en la nube:
 - BYOK (Bring Your Own Key)
 - HSM (Hardware Security Module)
- Bases de datos:
 - TDE (Transparent Data Encryption)
 - Always Encrypted (Microsoft SQL)
- Enmascaramiento / pseudonimización
- Prevención de fugas (DLP)

1.4 Sistemas de Protección de Datos

- **Backups:** completos, incrementales, snapshots
- **Monitorización:** Wazuh, Splunk
- **Base de datos:**
 - ACID
 - Consultas parametrizadas
 - Protección frente a SQLi y XSS
- **Sistemas de ficheros:**
 - BitLocker, snapshots, ACLs
- **Replicación:**
 - Síncrona: alta consistencia
 - Asíncrona: mayor rendimiento

1.5 Marcos Normativos y Estándares

- ISO/IEC 27001 / 27002
- NIST 800-53 / 800-207
- Legislación:
 - RGPD
 - LOPDGDD
 - ENS (España)
- Análisis de riesgos: MAGERIT, PILAR

1.6 Amenazas Habituales

- Ransomware y malware
- Empleados desleales
- Errores humanos
- Shadow IT

Técnicas comunes:

- SQL Injection (SQLi)
- Cross-site scripting (XSS)
- Ataques Man-in-the-middle (MITM)

1.7 Seguridad en entornos Cloud

- **Riesgos comunes:**
 - Buckets públicos mal configurados
 - Claves expuestas en código
- **Controles eficaces:**
 - CloudTrail (auditoría)
 - IAM (gestión de identidades)
 - Cifrado lado cliente
 - CSPM: Prisma Cloud, Lacework

Conclusión

- La seguridad de los datos es responsabilidad continua.
- Requiere enfoque técnico, organizativo y legal.
- Es vital en contextos de administración pública, empresas y servicios cloud.