



SEGURIDAD EN BASES DE DATOS



¿Qué es la Seguridad en Bases de Datos?

La seguridad en bases de datos se refiere al conjunto de **políticas, controles técnicos y procedimientos administrativos** diseñados para proteger los sistemas gestores de bases de datos (DBMS) frente a **accesos no autorizados**, modificaciones indebidas, pérdida de información o ataques cibernéticos.

! Principales Amenazas a las Bases de Datos

✓ Inyección SQL

✓ Robo de información

✓ Ataques de ransomware



✓ Escalamiento de privilegios

✓ Accesos no autorizados



Este tipo de seguridad abarca **múltiples capas**, incluyendo la protección física del servidor, la configuración segura del sistema operativo, la **administración de usuarios**, el cifrado de datos y el **monitoreo** continuo de actividades sospechosas.

Muchas **brechas** de seguridad ocurren no por **fallas técnicas complejas**, sino que involucran toda la infraestructura que permite su funcionamiento en caso de controles básicos.

Buenas Prácticas para la Protección de Bases de Datos



Control de Acceso y Principio de Mínimos Privilegios

- ✓ Asignar solo permisos necesarios
- ✓ Implementar autenticación fuerte



Actualizaciones y parches

- ✓ Mantener el motor de base de datos.
- ✓ Aplicar parches de seguridad
- ✓ Revisar boletines de vulnerabilidad



Cifrado de Datos en Tránsito y en Reposo

- ✓ Usar TDE, backups cifrados



Segmentación de Red

- ✓ Ubicar BD en redes internas
- ✓ Utilizar firewalls y listas blancas



Prevención de Inyección SQL

- ✓ Utilizar consultas parametrizadas
- ✓ Validar entradas del usuario
- ✓ Seguir prácticas OWASP



Auditoria, Monitoreo y Registro de Actividades

- ✓ Habilitar logs de accesos
- ✓ Implementar monitoreo continuo.



Respaldo y recuperación

- ✓ Realizar respaldos periódicos
- ✓ Almacenar respaldos en sitios seguros