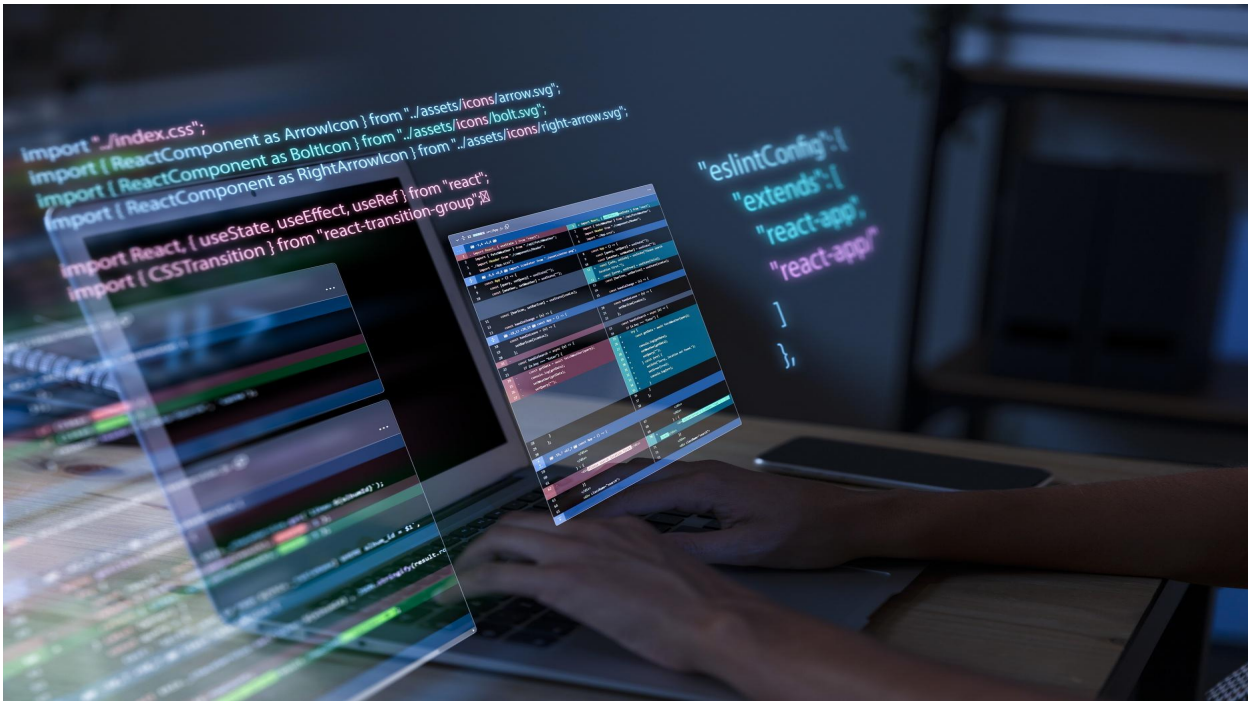
2º ASIR/ASGBD

UNIDAD 2

Gestión de usuarios, roles y seguridad



Autor: Luz María Álvarez Moreno

Fecha: 16/10/2025

Sesión 2: Usuarios, Roles, Perfiles y Contraseñas. Principio de Mínimo Privilegio

1. Introducción

En toda base de datos, la seguridad comienza con una gestión adecuada de quién puede acceder, qué puede hacer y hasta dónde llega su control.

El principio del mínimo privilegio es uno de los pilares fundamentales en la administración de sistemas de información, garantizando que cada usuario disponga solo de los permisos estrictamente necesarios para realizar su trabajo.

2. Elementos Clave en la Seguridad de un SGBD

Concepto	Definición	Ejemplo
Permiso	Acción básica sobre objetos de la base de datos (SELECT, INSERT, UPDATE, DELETE).	GRANT SELECT ON tabla TO analista;
Rol	Agrupación lógica de permisos según	CREATE ROLE rol_marketing;

	funciones o puestos de trabajo.	
Usuario	Identidad que accede al sistema y recibe privilegios del rol asignado.	CREATE USER juan IDENTIFIED BY 'pwd';
Perfil	Conjunto de políticas de seguridad y uso (CPU, contraseñas, sesiones).	CREATE PROFILE perfil_seguridad LIMIT FAILED_LOGIN_ATTEMPTS 3;

3. Jerarquía Lógica de Seguridad

Permisos → Roles → Usuarios → Perfiles

Ejemplo:

SELECT, INSERT → Rol: desarrollador → Usuario: juan.perez → Perfil: perfil_seguridad

4. Principio del Mínimo Privilegio

Cada usuario debe tener solo los permisos estrictamente necesarios para realizar su trabajo.

Este principio reduce drásticamente los errores de configuración, los accesos indebidos y mejora la seguridad general del sistema.

Ejemplo:

- **Rol analista_marketing:** solo lectura de tablas de campañas.
- **Rol cientifico_datos:** lectura y escritura en zonas de staging.
- **Rol soporte_tecnico:** mantenimiento sin acceso a datos sensibles.

5. Herramientas y Buenas Prácticas

Herramienta	Uso Principal	Beneficio
DBEaver / DataGrip / pgAdmin	Auditorías gráficas de roles y permisos	Facilita revisiones y reduce errores
Comandos SQL	Administración de roles y usuarios	Base sólida para políticas de acceso
Autenticación multifactor (MFA)	Añadir capa de seguridad adicional	Previene accesos indebidos

6. Políticas de Contraseñas Robustas

Política	Recomendación
Longitud mínima	12 caracteres
Complejidad	Mezclar letras, números y símbolos
Caducidad	Cada 90 días
Intentos fallidos	Máximo 3 antes de bloqueo
Autenticación multifactor	Activar si el SGBD lo permite

7. Roles Funcionales vs Personales

Tipo de Rol	Ejemplo	Ventajas / Desventajas
Personal	rol_marta, rol_pedro	Difícil reasignación, mantenimiento complejo
Funcional	rol_ventas, rol_rrhh	Reutilizable y escalable según departamentos

9. Flujo de Seguridad en un SGBD

1. El administrador crea roles con permisos específicos.

2. Se asignan a los usuarios según su función.

3. Cada usuario hereda los privilegios de su rol.

4. Se aplica un perfil con políticas de seguridad y uso.

10. Comandos SQL Clave

```
CREATE ROLE analista;
GRANT SELECT ON tabla_marketing TO analista;
CREATE USER juan IDENTIFIED BY 'Password12#';
GRANT analista TO juan;
CREATE PROFILE seguridad LIMIT PASSWORD_LIFE_TIME 90;
ALTER USER juan PROFILE seguridad;
REVOKE UPDATE ON tabla_marketing FROM analista;
```

11. Actividades Propuestas

1. Crear roles y asignarlos a usuarios en un SGBD simulado (Oracle o PostgreSQL).

2. Diseñar una política de contraseñas y roles para una empresa ficticia.

3. Identificar errores de permisos en un escenario mal configurado y proponer correcciones.

Sesión 3: Auditoría, monitorización y buenas prácticas de seguridad (incluyendo RGPD y compliance)

1. Auditoría

- Es el registro histórico de todo lo que ocurre en la base de datos.
- Permite saber quién accede, cuándo y qué hace.
- Es vital para investigar incidentes o cumplir con la normativa (ej. RGPD).

Ejemplo (Oracle):

AUDIT SELECT ON hr.employees BY ACCESS;

Registra todas las lecturas sobre la tabla employees.

Ejemplo (PostgreSQL):

Activar extensión pgaudit:

CREATE EXTENSION pgaudit;

SET pgaudit.log = 'read, write';

Registra operaciones de lectura y escritura para auditorías internas.

2. Monitorización

- Es la observación en tiempo real del sistema.
- Detecta comportamientos anómalos: intentos fallidos, consumo excesivo, accesos fuera de horario, etc.
- Se apoya en herramientas como Zabbix, Checkmk o Prometheus.

Ejemplo práctico:

Un pico repentino en las consultas o en la CPU puede ser un indicador de ataque de fuerza bruta o extracción masiva de datos.

Caso real:

Equifax (2017) no detectó a tiempo accesos anómalos en su base de datos; 147 millones de personas fueron afectadas.

Una simple monitorización activa podría haber alertado de la intrusión antes de que se completara la exfiltración.

3. RGPD y Compliance

El Reglamento General de Protección de Datos (RGPD) exige que cualquier empresa que trate datos personales:

- Controle el acceso a los datos.
- Gestione consentimientos.
- Disponga de registros de auditoría.
- Notifique incidentes de seguridad.

Principios básicos del RGPD aplicados a bases de datos:

Principio	Descripción
Confidencialidad	Solo acceden usuarios autorizados.
Integridad	Los datos no deben alterarse sin control.
Disponibilidad	Los datos deben estar accesibles cuando se necesiten.
Trazabilidad	Todas las acciones deben quedar registradas.

Ejemplos prácticos

Práctica	Descripción	Herramienta / Ejemplo
Auditoría selectiva	Registrar solo tablas críticas para evitar sobrecarga.	AUDIT SELECT, INSERT ON datos_clientes;
Monitorización proactiva	Configurar alertas ante picos de CPU o conexiones.	Zabbix, Prometheus
Protección de logs	Cifrar y guardar en servidor seguro.	openssl enc -aes-256-cbc -in audit.log -out audit.log.enc
Cifrado en tránsito y reposo	Usar SSL/TLS y TDE (Transparent Data Encryption).	Configuración en SGBD Oracle / SQL Server
Revisión periódica de roles	Auditar permisos cada trimestre.	Script SQL + comparación de roles

---

Casos reales y aplicaciones

Caso 1: Sanitas y la protección de datos médicos bajo RGPD

- Implementó auditoría fina (Fine-Grained Auditing) en Oracle.
- Registraba quién accedía, desde dónde y a qué nivel.
- Redujo en un 90% los accesos injustificados.

- Cumplió con los artículos 30 y 32 del RGPD (registro de actividades y seguridad del tratamiento).
- Resultado: mayor confianza y trazabilidad en el sistema sanitario.

Caso 2: LinkedIn (2021)

- Brecha por falta de auditoría sobre los endpoints de su API pública.
- Se extrajeron datos de 700 millones de usuarios.
- Si hubiera existido una monitorización de tráfico anómalo, la fuga se habría detectado antes.

Caso 3: Banco BBVA

- Auditorías automáticas y cifrado TDE en bases de datos de clientes.
- Cumple RGPD y PCI-DSS.
- Genera informes automáticos trimestrales de accesos, modificados y alertas.
- Beneficio: reducción de incidentes de seguridad y cumplimiento garantizado.

Buenas prácticas de seguridad

1. **Aplica parches de seguridad regularmente.**
    - Actualiza el SGBD para evitar exploits conocidos.
2. **Implementa cifrado en tránsito y en reposo.**
    - SSL/TLS + TDE.
3. **Automatiza informes de cumplimiento.**
    - Usa scripts que reporten accesos y cambios.
4. **Revisa trazabilidad de roles y usuarios.**
    - Asegura que permisos antiguos se desactiven.