

Tema-7.pdf



ozzyosbourne



Tecnología de bases de datos



3º Grado en Ingeniería Informática



**Escuela Técnica Superior de Ingeniería Informática
Universidad Politécnica de Valencia**



Estamos de
Aniversario

De la universidad al
mercado laboral:
especialízate con los posgrados
de EOI y marca la diferencia.



EOI Escuela de
organización
industrial



saber más

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato
→ Planes pro: más coins

pierdo espacio



Necesito concentración

ali ali oohh
esto con 1 coin me
lo quito yo...

WUOLAH

TEMA 7 – Seguridad de bases de datos

1. Concepto de seguridad en bases de datos

A la base de datos solo pueden **acceder** las **personas autorizadas** y en la **forma autorizada**.

- Los usuarios deben **estar autorizados** para conectarse al SGBD.
- Los usuarios deben **tener privilegios (permisos)** para crear objetos de BD y realizar operaciones sobre ellos.

2. Control de acceso

Se realiza por medio de la definición de **usuarios del sistema**.

- El **administrador de la base de datos (ABD)** debe crear un usuario y contraseña para cada usuario al que se le autorice la conexión al sistema.
- Para llevar el control de usuarios el SGBD dispone de una tabla cifrada con registros:
<usuario, contraseña>
- Para controlar la actividad de los usuarios, el SGBD asocia a cada operación el id del usuario que la ejecutó. Se puede hacer de dos formas:
 - Extendiendo el formato de las entradas del fichero de diario, incluyendo el id.
 - Manteniendo una tabla con entradas de la forma **<transacción, usuario>**

3. Mecanismos de concesión de privilegios: discrecional y fijo

Los **privilegios (permisos)** concedidos a un usuario restringen el tipo de objetos de BD que el usuario puede crear, y el conjunto de objetos a los que puede acceder y realizar operaciones.

Privilegios discrecionales

Consisten en permisos concedidos específicamente a cada usuario.

Genéricos: independientes de objetos concretos de BD (a nivel de usuario):

- Definición de esquemas **CREATE SCHEMA**
- Definición de tablas **CREATE TABLE**
- Definición de vistas **CREATE VIEW**
- Modificación de la definición de objetos de BD **ALTER**
- Eliminación de objetos de BD **DROP**
- Consulta de tablas **SELECT**
- Modificación de tablas **UPDATE, DELETE, INSERT**

De objeto: sobre objetos concretos de BD (a nivel de objeto):

- Consulta **SELECT**
- Modificación **UPDATE, DELETE, INSERT**
- Referencia

Privilegios fijos

Este mecanismo se basa en el uso de **niveles de seguridad**. Cada usuario y objeto de BD se clasifica en uno de estos niveles. A la clasificación de un usuario U se denomina **clase(U)** y a la de un objeto O **clase(O)**.

$$\text{TS (Top Secret)} \geq \text{S (Secret)} \geq \text{C (Confidential)} \geq \text{U (Unclassified)}$$

Reglas de acceso en un sistema con seguridad multinivel:

- Un usuario U no puede tener acceso de lectura a un objeto O a menos que $\text{clase(U)} \geq \text{clase(O)}$ (**propiedad de seguridad simple**).
- Un usuario U no puede tener acceso de escritura a un objeto O a menos que $\text{clase(U)} \leq \text{clase(O)}$ (**propiedad estrella**).

4. Seguridad en SQL

En SQL sólo se pueden conceder **privilegios discrecionales a nivel de objeto**:

```
concesión_privilegio ::=
GRANT {ALL|SELECT| INSERT [nom-atributo1, nom-atributo2, ... ]
      |DELETE | UPDATE [nom-atributo1, nom-atributo2, ... ] }
ON objeto TO {PUBLIC | usuario1, usuario2, ...}
[WITH GRANT OPTION]

revocación_privilegio ::=
REVOKE [GRANT OPTION FOR ]
{ALL | SELECT | INSERT [nom-atributo1, nom-atributo2, ... ]
 |DELETE | UPDATE [nom-atributo1, nom-atributo2, ... ] }
ON objeto TO {PUBLIC | usuario1, usuario2, ...}
{RESTRICT | CASCADE}
```

En la cláusula **REVOKE**, la opción **RESTRICT** impide revocar un privilegio concedido a un usuario (con opción **WITH GRANT OPTION**), si éste lo ha transferido a su vez a otro usuario.

La opción **CASCADE** realiza la revocación transitivamente.