FACULTAD DE CIENCIAS EXACTAS
UNIVERSIDAD NACIONAL DEL CENTRO DE LA PROVINCIA DE BUENOS AIRES

Tecnicatura Universitaria en Desarrollo de Aplicaciones Informáticas (TUDAI)

Base de Datos

Tema 9.1: Seguridad y Control de Acceso

2025

SEGURIDAD DE LA INFORMACIÓN

Seguridad: protección de los datos contra accesos no autorizados

Hay muchos *aspectos* relativos a la seguridad de la información:

Cuestiones éticas y legales

Controles físicos de los equipos

Políticas de la organización

Problemas operacionales

Controles de Hardware

Soporte del Sistema Operativo

SEGURIDAD EN BASES DE DATOS

¿Cuáles son las implicaciones de los cambios o destrucciones de datos?

El costo de la pérdida de los datos determinará el tipo de seguridad requerida

¿Cuánto costarían los accesos ilegales a los datos?

Si una porción de los datos tiene mucho valor para la organización, el acceso ilegal puede ser muy costoso

¿Las medidas de seguridad afecta a los usuarios de la BD?

No serán útiles los sistemas de seguridad que impidan el acceso a los datos a un usuario legítimo

SEGURIDAD EN BASES DE DATOS

El SGBD provee un **subsistema de seguridad y autorización** de la BD. Para acceder a la BD se requiere una cuenta de usuario y contraseña

El **Administrador de la Base de Datos (DBA)** -posee cuenta privilegiada- debe asegurar una política de acceso clara y consistente:

¿Quiénes?
(cuáles usuarios?)

¿Qué datos?
(restringir filas/columnas?)

¿Qué operaciones?
(sólo consulta o modificación?)

SEGURIDAD A CARGO DEL SGBD

Otros mecanismos para garantizar seguridad sobre la información:

SEGUIMIENTO DEL 'RASTRO' (*Audit Trail*):

- El SGBD puede registrar quién entra en la BD, a qué datos accedió y qué operaciones hizo sobre ellos (*LOG o bitácora del sistema*)

CIFRADO o ENCRIPTACIÓN de datos:

- Los datos se codifican mediante algoritmos particulares, en función de una clave (*privada*) o dos claves (*privada-pública*)
- los datos resultan ilegibles a menos que se tenga conocimiento del código usado y la clave correspondiente

CONTROL DE ACCESO A LA BD

Granularidad: La protección de los **objetos de la BD** depende de su tamaño o extensión (ej: registro, tabla, columna, elemento de la BD (vistas, procedimientos, funciones). Tenemos que considerar 3 aspectos:

(S)ujeto: usuario que requiere acceso a un objeto

(O)bjeto: lo que necesita ser accedida por un sujeto (registro, tabla, columna, elemento de la BD)

(P)rivilegio: derecho de acceso, cómo un **sujeto** puede acceder o manipular un **objeto** (consulta/modificación/borrado/inserción)

MÉTODOS DE CONTROL DE ACCESO

Control de Acceso Discrecional:

garantiza privilegios a usuarios, incluyendo la capacidad para acceder tablas, registros o campos para operar de una manera determinada (select, insert, delete, update, otras…).

Control de Acceso basado en Roles:

establece grupos de privilegios encapsulados en un rol que se otorgan a usuarios

Control de Acceso Mandatorio:

clasifica usuarios y datos en múltiples niveles de seguridad y luego fuerza determinadas reglas acordes a cada nivel

CONTROL DE ACCESO DISCRECIONAL

Se basa en **dar y/o quitar privilegios** sobre los objetos de la BD de manera selectivo a otros usuarios (a discreción)

GRANT privilegio/s **ON** objeto/s
TO usuario/s **[WITH GRANT OPTION]**

REVOKE [GRANT OPTION FOR] privilegio/s **ON** objeto/s
FROM usuario/s **{CASCADE | RESTRICT}**

privilegio/s: derecho/s para acceder o ejecutar un procedimiento SQL - operación/es de acceso a los datos (puede ser uno o varios)
objeto/s: tablas, vistas, índices, etc. (uno o varios)
usuario/s: nombre de usuario que la BD reconoce o PUBLIC (=todos los usuarios)

WITH GRANT OPTION permite que el sujeto poseedor de privilegios pueda transmitirlos a otros usuarios

CONTROL DE ACCESO DISCRECIONAL

NIVELES DE ASIGNACIÓN DE PRIVILEGIOS

A nivel de cuenta: se pueden especificar privilegios particulares a cada usuario, independientemente de las relaciones de la BD

Ejemplos

CREATE SCHEMA,

CREATE TABLE,

CREATE VIEW,

ALTER,

DROP

CONTROL DE ACCESO DISCRECIONAL

NIVELES DE ASIGNACIÓN DE PRIVILEGIOS

Nivel de tabla: se puede controlar el privilegio para acceder a cada tabla o vista de manera individual

SELECT

DELETE

INSERT

UPDATE

REFERENCES (columna/s) – definir FK referidas a esa/s columna/s

CONTROL DE ACCESO DISCRECIONAL

PROPAGAR PRIVILEGIOS: Por ejemplo si el propietario A de un objeto R desea otorgar a otra cuenta B un cierto privilegio para R (o si posee ese privilegio), puede hacerlo con la opción de **propagar** ese privilegio (WITH GRANT OPTION=GO) o **sin ella**

GRANT privilegio/s ON objeto/s
TO usuario/s [WITH GRANT OPTION]

- Se puede propagar un mismo privilegio a más de un usuario
- Se puede recibir un mismo privilegio de más de un usuario

CONTROL DE ACCESO DISCRECIONAL

QUITAR PRIVILEGIOS: es posible quitarle los privilegios otorgados a un usuario/s o rol o la posibilidad de propagarlos

REVOKE [GRANT OPTION FOR] privilegio/s ON objeto/s
FROM usuario/s {CASCADE | RESTRICT}

- **GRANT OPTION FOR** le quita la posibilidad de propagar el privilegio
- **REVOKE** con opción **CASCADE**, el efecto es revocar el privilegio al usuario y a todos los que lo recibieron a través de él. Con opción **RESTRICT**, se rechazará si el efecto de revocación de privilegios provocaría privilegios *colgados*

CONTROL DE ACCESO DISCRECIONAL

Ejemplos

GRANT INSERT, SELECT, DELETE ON Hotel TO U1;

→ U1 puede insertar, borrar y seleccionar tuplas de la tabla Hotel

GRANT DELETE, INSERT ON Hotel TO U2 WITH GRANT OPTION;

→ U2 puede insertar y borrar tuplas de la tabla Hotel (y propagar los privilegios a otros)

GRANT UPDATE (nro_estrellas) ON Hotel TO U3;

→ U3 puede actualizar solamente el campo nro_estrellas de las tuplas de Hotel

GRANT SELECT ON VistaHoteles3Estrellas TO U4;

→ U4 pueden consultar los datos sobre hoteles 3 estrellas de la vista (pero NO pueden consultar directamente la tabla Hotel)

✓ Se puede generar un **Grafo de Autorizaciones** con los privilegios concedidos:

- **Nodos → usuarios**
- **Arcos (dirigidos) → concesión de privilegio** (sobre qué objeto), y si tiene GO

CONTROL DE ACCESO DISCRECIONAL

Ejemplos

A es propietario del esquema BD_EJ y crea en él las tablas T1 y T2 (privilegio de cuenta) - (El DBA antes hizo: CREATE SCHEMA BD_EJ AUTHORIZATION A;)

A: GRANT SELECT ON T1, T2 TO **B**;
→ B puede seleccionar tuplas de T1 y T2 (sin posibilidad de propagarlo)

A: GRANT SELECT ON T1, T2 TO **C** WITH GRANT OPTION;
→ C puede seleccionar tuplas de T1 y T2 (y puede propagar ese privilegio)

C: GRANT SELECT ON T1 TO **B, D**;
→ B y D reciben el priv. de seleccionar tuplas de T1 (pero no de propagar el privilegio)

A: REVOKE GRANT OPTION ON T2 FROM **C**;
→ C ya no puede ceder el privilegio de selección sobre T2 (pero lo conserva)

A: REVOKE SELECT ON T1 FROM **C** CASCADE;
→ C pierde el privilegio de selección sobre T1
y esto se propaga en cascada a B y D
pero B había recibido también el privilegio directamente de A (lo sigue conservando)

¿Qué privilegios conserva cada usuario entonces? (*analizar grafo*)

CONTROL DE ACCESO DISCRECIONAL

GRANT/REVOKE EN VISTAS:

- El creador de una vista tiene privilegios sobre la vista si los tiene sobre todas las tablas subyacentes
- Si el creador de una vista pierde el privilegio SELECT sobre alguna de las tablas subyacentes, la vista es removida!
- Si el creador de una vista pierde un privilegio obtenido con WITH GRANT OPTION sobre una tabla subyacente, también pierde el privilegio sobre la vista (lo mismo ocurre con los demás usuarios que hayan obtenido el privilegio sobre la vista)

Asignar derechos para ejecutar programas compilados:

- GRANT EXCECUTE ON <procedimiento> TO <usuario>
- Problema: los procedimientos(stored procedures) podrían acceder a recursos para los cuales el usuario no tiene permisos de acceso

CONTROL DE ACCESO
BASADO EN ROLES

Un **ROL** es el conjunto de privilegios o derechos de acceso que se le pueden otorgar a usuarios (encapsulan un conjunto de privilegios)

```
CREATE ROLE <nom_rol> [ WITH option ] ;

GRANT nom_rol [{,<nom_rol> }] TO <a_quien> [{,<a_quien>}]
      [ WITH ADMIN OPTION ] ;
```

a_quien indica usuario/s u otros roles o PUBLIC (todos)

WITH ADMIN OPTION indica que se puede conceder el rol a otros usuarios/roles

Ej: CREATE ROL RR; GRANT CREATE TABLE TO RR; GRANT RR TO user1;

Nota: un usuario puede tener asignado a uno o más roles y siempre existe u rol especial: **ADMIN** (tiene privilegios como: *create role* y *drop role*)

CONTROL DE ACCESO
BASADO EN ROLES

Para quitarle la pertenencia a uno o más roles de uno o más usuarios/roles

REVOKE [ADMIN OPTION FOR] nom_rol [{, nom_rol}]
FROM <*a_quien*> [{,<*a_quien*>}] ;

No se pueden quitar los privilegios del propietario de un objeto

Ejemplos

REVOKE CREATE TABLE FROM RR;

REVOKE ADMIN OPTION FROM RR;

CONTROL DE ACCESO MANDATORIO

Cada **objeto** de la BD tiene asignada una **clase de seguridad** (*seguridad multinivel)*

Cada **sujeto** (usuario o programa) tiene asignado **un permiso** para una clase de seguridad

- Basado en estrategias de la organización, no pueden ser modificados por los usuarios individualmente
- Existen reglas que habilitan/prohíben lecturas/escrituras en la BD, según combinaciones específicas de clases de seguridad y permisos

La mayoría de los DBMSs actuales **NO** soportan este control Algunas versiones lo hacen para aplicaciones específicas (*ej. Defensa, Espionaje, …*)

GUÍAS DE SEGURIDAD PARA EL SGBD

Funcionalidad

- Usar la menor cantidad de protocolos de comunicación posible
- Eliminar del sistema procedimientos innecesarios o inútiles
- Desabilitar login por defecto y usuarios invitados hasta donde sea posible
- No permitir a todos los usuarios que se logueen interactivamente (consola), a menos que se requiera

Planeamiento

- Desarrollar un plan de seguridad para prevenir y detectar problemas
- Crear procedimientos/protocolos para emergencias de seguridad y practicarlos

GUÍAS DE SEGURIDAD PARA EL SGBD

Es aconsejable:

- Ejecutar el SGBD detrás de un *firewall*
- Proteger el/los equipo/s sobre el/los que corre el SGBD
  - Ubicar los equipos con el SGBD en ambientes físicamente seguros
  - No permitir que los usuarios “no-DBA” lo utilicen
  - Se debería registrar el acceso en un log (diario o bitácora del sistema)
- Manejar cuentas y passwords
  - Usuarios con privilegios adecuados para el servicio del SGBD
  - Proteger las cuentas de la BD con passwords **MUY** seguras
  - Llevar auditoría de intentos fallidos a la BD (log)
  - Chequeo de usuarios y grupos o roles
  - Limitar los privilegios para la cuenta del DBA y asignar a los otros usuarios/roles la menor cantidad posible de privilegios