Ingeniería Técnica en Informática
Escuela Universitaria de Informática
Universidad Politécnica de Madrid

Asignatura: **Administración de Bases de Datos**

Tema 3:
Seguridad e Integridad en Bases de Datos

Pedro P. Alarcón Cavero
pedrop.alarcon@eui.upm.es
Juan Garbajosa Sopeña
jgs@eui.upm.es

Febrero 2008

Contenido

1. Introducción

- Seguridad
  - Impedir accesos, alteración o destrucción de los datos con fines indebidos
  - Asegurar que los usuarios están autorizados
- Integridad
  - Controlar la exactitud o validez de los datos almacenados en la BD
  - Asegurar que lo que tratan de hacer los usuarios es correcto

2. Seguridad

- La seguridad es punto esencial de las bases de datos
- La seguridad comprende
  - impedir cualquier ataque deliberado al servicio
  - impedir cualquier acceso no autorizado, modificación, uso y difusión de la información almacenada
  - proteger la integridad lógica y física del SBD
- La seguridad incluye:
  - aspectos lógicos
  - aspectos físicos
- **Catalogo/DD**

2.1 Aspectos de Seguridad/Confidencialidad

- Legales, sociales y éticos
- Humanos o de política interna
- Niveles de seguridad en la organizaciones
  - usuarios
  - datos
- Sistema
  - sistema operativo
  - comunicaciones
  - hardware
  - …

Problemas sobre seguridad y respuestas

- Subsistema de **Control de acceso**
- Subsistema de **Seguridad** y **Autorizaciones**
  - Mecanismos de seguridad discrecionales
  - Mecanismos de seguridad obligatorios
- **Protección** de datos a través de **cifrado** (*encriptación*)
- Seguridad en **bases de datos estadísticas**

Control de acceso

- El acceso se controla por una **cuenta** y una **palabra de paso**
- La conexión y operaciones quedan reflejados en un **diario** (*log*)

CUENTA	PALABRA PASO
CUENTA	OPERACION

DIARIO

- **Auditorías y monitorizaciones**

Papel del administrador

- Autoridad central para gestionar/dirigir la base de datos
- Tiene una **cuenta privilegiada** (cuenta del sistema)
- Acciones
  - **Crear cuentas** asociadas a usuarios y con palabra de paso
  - **Asignar niveles de seguridad** a cuentas
  - **Conceder privilegios** a ciertas cuentas
  - **Eliminar privilegios**

Enfoque de las autorizaciones

- Protagonistas
  - Usuario
  - Objeto
- Utilización de vistas (sub-esquemas)
  - Tabla virtual
  - Múltiples esquemas externos de una BD
  - Permiten ocultar información confidencial
  - No permiten especificar operaciones a realizar con ellas

Mecanismos de seguridad discrecionales Nivel de usuario

- ABD
- Usuario con privilegios de recursos (comandos LDD y LMD)
- Usuario con privilegios de conexión (comandos LMD)
- Utilización de Vistas

Sentencias y ejemplos (Nivel de usuario)

- **GRANT | REVOKE** **dba** **TO** lista_usuarios
  | resource
  | connect
  - Ejemplo:
    - **GRANT** CREATETAB **TO** JUAN (SQL, libre en SQL2)
    - **CREATE SCHEMA** SI **AUTHORIZATION** JUAN (SQL2)
- **CREATE VIEW** nombreVista **AS SELECT** ….
  - Ejemplo:
    - **CREATE VIEW** NomEmpleCom
      AS SELECT E#, Nombre, Apellidos
      FROM Empleados
      WHERE Depto = "Ventas";

Mecanismos de seguridad discrecionales: Nivel de objeto

- Permite establecer autorizaciones sobre los objetos de la base de datos
- Autorizaciones respecto a datos
  - Lectura
  - Inserción
  - Modificación
  - Borrado
- Autorizaciones sobre el esquema de una tabla
  - Índices
  - Alteración
  - Eliminación

Sentencias (Nivel de objeto)

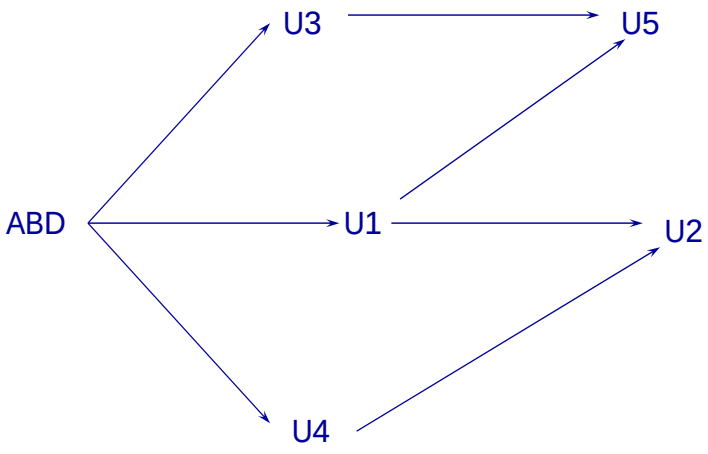
- Concesión de privilegios

  GRANT <privilegios> ON <nombre_de_tabla>
  TO <lista_de_usuarios> | PUBLIC
  [WITH GRANT OPTION]
  <privilegios> ::= SELECT [(<lista de columnas)]
  | DELETE
  | INSERT
  | UPDATE [(<lista de columnas)]
  | ALL
  | INDEX | ALTER | DROP

- Revocación de privilegios

  REVOKE [WITH GRANT OPTION] <privilegios>
  ON <nombre de objeto> FROM <lista de usuarios> | PUBLIC

Grafo de autorización de permisos



Ejemplo 1

```
ABD:    GRANT CREATETAB TO Pedro
Pedro:  CREATE TABLE Empleados
Pedro:  CREATE TABLE Departamentos
Pedro:  GRANT INSERT, DELETE ON Empleados, Departamento
                                        TO Luis
Pedro:  GRANT SELECT ON Empleados, Departamento TO Paco
                                        WITH GRANT OPTION
Paco:   GRANT SELECT ON Empleados TO Lucas
Pedro:  REVOKE SELECT ON Empleados FROM Paco

Pedro:  CREATE VIEW PacoEmpleados AS
        SELECT Nombre, Fecha FROM Empleados
                WHERE  Dni = 25
Pedro:  GRANT SELECT ON PacoEmpleados TO Paco
                WITH GRANT OPTION
```


Ejemplo 2

Empleados: Nombre, Departamento
Departam: Código, Sección, Número

1. Hay que autorizar a U1 para crear tablas
2. U1 crea las tablas Emplados y Departam
3. U1 autoriza a U2 a realizar todo tipo de operaciones con ambas tablas
4. U2 autoriza a U3 a ver Código y Sección
5. U2 autoriza a U4 a modificar la tabla Departam
6. U2 autoriza a U5 a modificar Departamento y a conceder privilegios
7. U2 retira el privilegio a U4

Control de acceso obligatorio para seguridad multinivel

- Necesario para ciertos tipos de clientes
- Utiliza clases de seguridad. Por ejemplo:

  alto secreto > secreto > confidencial > no clasificado

- **S**ujetos: usuario, cuenta, programa...
- **O**bjeto: relación, tupla, columna, vista, operación
- Cada sujeto y objeto tiene una clase

1. S no puede acceder en lectura a O a menos que clase (S) >= clase(O)
2. S no puede acceder en escritura a O a menos que clase (S) <= clase (O)

2.2. Auditorías

- Concepto
- Rastreo de diarios (integrados o no con recuperación)
- Indispensable si
  - los datos son muy delicados
  - el procesamiento realizado con ellos es crítico
  - existe sospecha de alteración indebida de los datos
- La auditoría puede servir para
  - examinar lo sucedido
  - verificar el estado de la cosas
  - ayudar a descubrir problemas o atacante
  - desanimar a posibles atacantes

Campos de un fichero diario para seguridad

- Operación (por ejemplo, UPDATE)
- Terminal desde el que se invocó la operación
- Usuario que la invocó
- Fecha y hora de la operación
- Base de datos, tabla, registro y campos afectados
- Valor anterior del campo
- Valor nuevo del campo

2.3. Bases de Datos Estadísticas

- Concepto
- Importancia de la privacidad de los datos individuales
- Consultas: funciones agregadas (totalizadoras)
- Interrogaciones anómalas: con respuestas referidas a un individuo

C1: ¿Cuántos clientes del banco, de sexo femenino, con edad comprendida entre los 25 y 35 años residen en Alpedrete?

C2: ¿ Cuál es el saldo medio de los clientes del banco, de sexo femenino, con edad entre los 25 y los 35 años que residen en Alpedrete?

3. Integridad

- Integridad de una BD
  - Exactitud, validez o consistencia de los datos almacenados en la BD, de acuerdo a un conjunto de restricciones semánticas
- Restricción de integridad
  - Condiciones que deben cumplir los datos
- BD coherente
  - Los datos cumplen el conjunto de restricciones de integridad

3.1 Tipos de restricciones de integridad

- Dominio de variación
- Rango del valor
- No valores nulos
- Unicidad (claves principales y secundarias)
- Referencial (claves foráneas)
- Dependencias funcionales y dmv
- Aritméticas
- Temporales

3.1. Tipos de restricciones de integridad

- En SQL2:
  - NOT NULL, UNIQUE, PRIMARY KEY, FOREIGN KEY
  - CREATE DOMAIN
  - CHECK
  - CREATE ASSERTION <nombre> CHECK (<condicion>)

3.2. Control de Integridad

- El control lo ejerce el Subsistema de integridad de un SGBD
- Pueden almacenarse en el catálogo
  - Formando parte integrante de la descripción de los datos
  - No han de incluirse en los programas
  - Ventajas:
    - reglas de integridad más sencillas
    - mejor detección de inconsistencias

3.3. Inconsistencias

- Pérdida de integridad de una BD
- Pueden provenir de:
  - Operaciones semánticamente inconsistentes (errores lógicos)
  - Interferencias por accesos concurrentes
  - Caídas durante el procesamiento de transacciones