SEGURIDAD EN SISTEMAS DE BD

INTRODUCCIÓN

- **Diferencias Seguridad / Integridad:**
  - **Seguridad:**
    - **Protección** de datos contra revelación, alteración o destrucción no autorizados

    ⇒ Asegurar que los usuarios están autorizados para hacer lo que quieren hacer
  - **Integridad:**
    - Exactitud o **validez** de datos (deben reflejar la realidad)

    ⇒ Asegurar que lo que los usuarios tratan de hacer es correcto, y Evitar la pérdida accidental de la consistencia
- **Similitudes Seguridad / Integridad:**
  - El **sistema** debe **conocer** las **restricciones** que los usuarios **no** deben violar
  - Restricciones **especificadas** [por el **DBA** p.ej.] en un **lenguaje apropiado**
  - Las **restricciones** deben almacenarse y **mantenerse** en el **catálogo** del sistema
  - El **SGBD** debe **supervisar** la **interacción** de cada **usuario** con la **BD**, para controlar el **cumplimiento** de las **restricciones**

SEGURIDAD

Aspectos del problema de la Seguridad:

(Hay que adoptar medidas de seguridad en todos estos niveles)

- **Legales, sociales y éticos:** ¿el solicitante tiene el derecho legal de obtener determinada información (*saldo de la cuenta de un cliente*)?
- **Política interna de la empresa:** ¿cómo decide la empresa quién puede acceder a qué? ¿cómo asegurar que no se revelen datos confidenciales a cambio de sobornos y otros favores?
- **Controles Físicos:** ¿cómo proteger físicamente contra intrusos las salas en donde están los sistemas informáticos?
- **Problemas de Operación:** si se usan contraseñas ¿cómo se mantienen en secreto? ¿con qué frecuencia se cambian?
- **Controles de Equipo:** ¿tiene la CPU características de seguridad (claves para protección de áreas de almacenamiento o modo de operación privilegiado)?
- **Seguridad del S.O. :** ¿borra el S.O. el contenido de áreas de almacenamiento y archivos de datos cuando no se necesitan? ¿permite el S.O. acceso directo a los ficheros de la BD?
- **Seguridad de la Red:** la seguridad en el nivel de software de red es fundamental hoy en día, tanto en Internet como en las redes privadas de la empresa.

☆ **Aspectos específicos del Sistema de BD**

¿tiene el Sistema de BD un concepto de *propiedad* de datos?

SEGURIDAD

- La Seguridad es **crucial en Sistemas Multiusuario**, pues
  - Diferentes usuarios usan una misma (y grande) BD integrada
  - Información confidencial (salarios, saldos) debe ocultarse a la mayoría de usuarios
  - » El SGBD proporciona técnicas para que (grupos de) usuarios accedan a partes de la BD **sin** tener acceso al resto
- Es **imposible la Protección Total y Absoluta de la BD** contra mal uso intencionado,
  Pero se puede ELEVAR EL COSTE DE LOS INTENTOS DE ACCESO NO AUTORIZADO lo suficiente como para DISUADIRLOS
- **Merece la pena el ESFUERZO** por conservar la seguridad (y la integridad) de la BD:
  - Grandes BD de nóminas o datos financieros → atractivas para ladrones
  - BD de operaciones empresariales → interesantes para competidores sin escrúpulos
  - La pérdida de datos (accidente o fraude) supone elevados costes y disminución de la capacidad de la empresa para seguir funcionando

» ***Subsistema de Seguridad y Autorización*** (del SGBD)
garantiza la seguridad de (partes de la) BD contra accesos no autorizados

CONTROL DE ACCESO

Objeto de Datos

- ✓ Unidad de datos que requiere protección individual
- ✓ Puede ser la BD completa, o un conjunto de relaciones, ... hasta una posición (fila,columna) dentro de cierta relación

1. CONTROL DISCRECIONAL (Más flexible)

- Un usuario tiene diversos derechos de acceso (privilegios) sobre distintos objetos
- Permite que diferentes **usuarios** tengan **privilegios** distintos **sobre** un mismo **objeto**

2. CONTROL OBLIGATORIO (Más rígido)

- Cada **objeto** de datos etiquetado con un **nivel de seguridad**
- Cada **usuario** se asigna a un **nivel de acreditación**
- Cada **objeto** de datos puede ser **accedido** sólo **por usuarios con acreditación apropiada**

CONTROL DE ACCESO

- **Decisiones** sobre **seguridad** son **políticas**, no técnicas (**fuera del DBMS**)
- Pero **DBMS refuerza** tales **decisiones** (las impone, OBLIGA a cumplirlas).
  Para ello:

  1. Tales decisiones deben...
  - **a.** Indicarse al sistema, mediante sentencias en DDL (GRANT, REVOKE...)
  - **b.** Ser recordadas por el sistema:
    almacenadas en el catálogo, en forma de
    Reglas (o Restricciones) **de Seguridad y Autorización**

  2. Debe existir una forma de comprobar peticiones de acceso
  (operación solicitada + datos solicitados + usuario solicitante)
  según las restricciones (reglas) de seguridad aplicables
  Chequeo realizado por el **Subsistema** (del SGBD) **de Seguridad y Autorización**

  3. SGBD debe ser capaz de reconocer el **origen** de una petición (**usuario** solicitante)
  para decidir **qué reglas** de seguridad **son aplicables a** cierta **solicitud**
  ⇒ **identificador de usuario (+ contraseña)**

CONTROL DE ACCESO

CONTROL DE ACCESO AL SISTEMA GLOBAL de BD

- Evitar que personal no autorizado acceda al sistema de BD
- Puesto en práctica mediante creación de cuentas de usuario de BD y contraseñas
- DBA
  - ✓ Autoridad central responsable de la Seguridad Global del Sistema de BD, pues
    - Otorga y revoca privilegios a usuarios y
    - Clasifica datos según nivel de seguridad y usuarios según nivel de acreditación
  - ✓ Tiene **cuenta** privilegiada o **de sistema**,
    con capacidades de ADMINISTRADOR DE LA BASE DE DATOS:
    1. Creación de cuentas (y passwords) de usuario para acceder a la BD (CONTROL GLOBAL)
    2. Concesión/Cancelación de privilegios a cuentas (CONTROL DISCRECIONAL)
    3. Asignación de cuentas de usuario a niveles de seguridad (CONTROL OBLIGATORIO)

CONTROL DE ACCESO

- Si una persona necesita acceder a BD, debe solicitar una **cuenta de usuario**
- Cuando el DBA crea una cuenta, le da un **nombre** y una **contraseña** (password)

Nota: Programa de aplicación = Usuario (puede exigírsele contraseña)

CONTROL DE USUARIOS DE LA BD. CUENTAS Y CONTRASEÑAS

- **Tabla** (archivo) **cifrada**, con dos atributos (campos): cuenta, contraseña
- Almacenada en el catálogo del sistema

- Para entrar al SGBD, el usuario indica (al SGBD) su cuenta y su password
- Si el SGBD valida esos datos, el usuario puede usar el SGBD y acceder a la BD

- SGBD controla toda operación de todo usuario en cada sesión de trabajo en la BD:
  - Cuando el usuario entra, el SGBD asocia su cuenta al terminal desde el que accede
  - Toda operación desde ese terminal se atribuye a la cuenta del usuario

  » Si la BD se altera incorrectamente, el DBA podrá saber quién lo hizo ⇒ Auditoría

CONTROL DE ACCESO

- **SEGUIMIENTO DE AUDITORÍA**
  - Necesario si los datos son muy delicados, o el procesamiento realizado con ellos es crítico
  - Consiste en mantener un archivo especial donde el sistema registra de forma automática, toda interacción de los usuarios con la BD
  - Permite
    - Verificar que todo está en orden
    - Si alguien ha accedido o ha realizado operaciones sin autorizaci ón, descubrirlo

  - Una entrada en dicho fichero podr ía contener:
    - operación (por ejemplo UPDATE)
    - terminal desde la que se invocó la operación
    - usuario que solicitó la operación
    - fecha y hora de la operación
    - base de datos, tablas (ficheros), tuplas (registro) y atributos (campos) afectados
    - valor anterior de los datos
    - nuevo valor de los datos

  - En muchos casos, el hecho de mantener un seguimiento de auditor ía basta para desanimar a posibles *espías*

CONTROL DE ACCESO DISCRECIONAL

- Basado en **privilegios** o autorizaciones
- Soportado por la mayoría de los SGBD comerciales (Oracle)
- Privilegios a nivel de Cuenta y a nivel de Objeto

1. Privilegios a Nivel de Cuenta

- DBA especifica privilegios particulares de cada usuario independientemente de las relaciones en la BD

- Tipos de **Privilegios**:
  - CREATE SCHEMA, DROP SCHEMA
  - CREATE TABLE, ALTER TABLE, DROP TABLE
  - CREATE VIEW, DROP VIEW
  - CREATE DOMAIN, ALTER DOMAIN, DROP DOMAIN
  - CREATE ASSERTION, DROP ASSERTION
  - INSERT, UPDATE, DELETE (tuplas)
  - SELECT

- NO están definidos en el estándar SQL2: debe definirlos el implementador del SGBD

CONTROL DE ACCESO DISCRECIONAL

2. Privilegios a Nivel de Objeto (Relación, Dominio...)

- Aplicados a **objetos individuales** (relaciones base o virtuales (vistas), dominios)
- Sí están **definidos en el estándar SQL2**

GRANT <privilegios> **ON** <objetos> **TO** <sujetos> [**WITH GRANT OPTION**]

- Se especifica para cada usuario a qué objetos puede aplicar qué operaciones
- En SQL2 existen privilegios a nivel de **relación** (tabla o vista), **atributo** y **dominio**

- Cada objeto tiene una **cuenta propietario** (en la que fue creado)
- El propietario del objeto posee **todos** los **privilegios** sobre él (incluso el de conceder esos derechos a otros usuarios: GRANT OPTION)

- Tipos de **Privilegios:**
  - USAGE (uso de **dominios**)
  - ALL PRIVILEGES (todos los que posee -sobre el objeto- aquel que los concede)
  - SELECT (todos los atributos de una relación, incluidos los añadidos después)
  - UPDATE, INSERT (ambos con opción de sólo ciertos atributos)
  - DELETE (tuplas)
  - REFERENCES (permite hacer referencia a -ciertos atributos- de una relación mediante *Restricciones de Integridad de cualquier tipo*, no sólo *RI Referencial*)

CONTROL DE ACCESO DISCRECIONAL

- Modelo de autorización para privilegios discrecionales: **Modelo Matriz de Acceso**

	Objeto1	Objeto2	Objeto3 ...
User1	NONE	SELECT	ALL
User2	SELECT	UPDATE	SELECT DELETE UPDATE
User3	NONE	NONE	SELECT
User4	ALL	ALL	ALL

M(u,o) : conjunto de autorizaciones o privilegios del usuario **u** sobre el objeto **o**

La fila **u** es el **perfil del usuario u**

- **CANCELACIÓN (revocación) DE PRIVILEGIOS** (privilegios temporales)

REVOKE [**GRANT OPTION FOR**] <privilegios>
ON <objetos>
FROM <sujetos> { **RESTRICT** | **CASCADE** }

```
REVOKE SELECT ON FOTOGRAFO FROM julia;
REVOKE UPDATE(cuota) ON EDITORIAL FROM ruben;
```


CONTROL DE ACCESO DISCRECIONAL

- **USO DE VISTAS COMO MECANISMO DE SEGURIDAD DISCRECIONAL**

Sea el usuario A, propietario de la relación R(a1,a2,a3,a4,a5)

✓ Si A desea que otro usuario B pueda leer sólo algunos atributos a1,a2,a3 de R
» A crea vista V de R con sólo esos atributos y da a B el privilegio SELECT sobre V

```
CREATE VIEW V AS SELECT a1, a2, a3 FROM R;
GRANT SELECT ON V TO B;
```

✓ Si A desea que B lea sólo algunas tuplas de R, que satisfacen cierta condición Q
» A crea vista W de R, definida con una consulta que selecciona sólo las tuplas de R que puede ver B, y otorga a B el privilegio SELECT sobre W

```
CREATE VIEW W AS SELECT * FROM R WHERE Q;
GRANT SELECT ON W TO B;
```

◗ Para crear una vista, la cuenta debe poseer privilegio SELECT sobre cada una de las tablas base de la vista

CONTROL DE ACCESO DISCRECIONAL

PROPAGACIÓN DE PRIVILEGIOS

- Cuando **A propietario de** una relación **R**, concede privilegios (SELECT por ejemplo) sobre R a otro usuario B, también **puede** darle la **opción de otorgar** dichos privilegios (cláusula **WITH GRANT OPTION**)

  GRANT SELECT ON R TO B WITH GRANT OPTION;

- De este modo **B podrá otorgar privilegios sobre R a otras cuentas** de usuario (PROPAGACIÓN DE PRIVILEGIOS)

- Revocar la opción de GRANT no cancela ningún privilegio, pero evita su propagación

  REVOKE GRANT OPTION FOR SELECT ON R FROM B;

- Pero, si A revoca el privilegio dado a B, *¿qué ocurre con los que B propagó a partir de éste?*

  ⇒ **Privilegios Abandonados** (no válidos)

- Y si el propietario de una vista V pierde el privilegio SELECT sobre alguna de las tablas base de V

  ⇒ **Vista Abandonada** (no válida)

CONTROL DE ACCESO DISCRECIONAL

- Cuando un usuario A revoca privilegios, indica una opción...
  - CASCADE
    - ✓ el sistema revocará automáticamente todos los privilegios que quedarían abandonados y
    - ✓ eliminará las vistas que quedarían abandonadas
  - RESTRICT
    - ✓ el sistema no dejará revocar un privilegio si ello dejara privilegios o vistas abandonados
    - ✓ Sólo lo revocaría si no dejara otros privilegios ni vistas abandonados

- Un SGBD que permite propagación, debe seguir la pista de la concesión y propagación de privilegios, para conseguir una revocación completa y correcta.

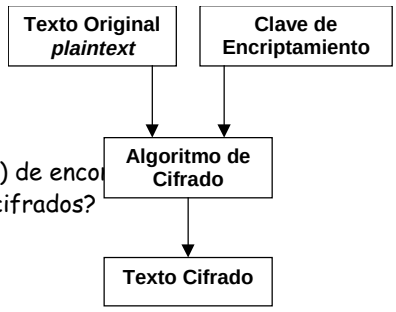
- Un usuario puede recibir un mismo privilegio desde 2 o más usuarios. Sólo lo perderá si lo revocan todos ellos.
- Eliminar un objeto (dominio, tabla base, columna o vista), revoca automáticamente todo privilegio (en todos los usuarios) sobre tal objeto eliminado

CONTROL DE ACCESO OBLIGATORIO

- Para establecer una **seguridad multinivel**
- Política que **clasifica datos** y **usuarios** en **niveles (clases) de seguridad**
- Se combina con el control de acceso discrecional
- Aunque la mayoría de los SGBD sólo ofrecen el control discrecional
- Existe la necesidad de esta seguridad multinivel en aplicaciones gubernamentales, militares, de espionaje, de algunas industrias...
- **Niveles de seguridad**
  - TS (top secret) secreto máximo o alto secreto
  - S (secret) secreto
  - C (confidential) confidencial
  - U (unclassified) no clasificado
- **Modelo de seguridad Multinivel**
  - Asigna a cada sujeto (usuario, cuenta o programa) y a cada objeto (relación, tupla, columna, vista) un nivel de seguridad (TS, S, C, U)
  - **Reglas (restricciones) de acceso**:
    1. Un sujeto P puede *leer* el objeto O si nivel(P) ≥ nivel(O)
    2. Un sujeto P puede *escribir* el objeto O si nivel(P) = nivel(O)

CIFRADO DE LOS DATOS

- Para proteger **datos confidenciales**...
  - **transmitidos** por **satélite** o cualquier tipo de **red** de comunicaciones
  - **almacenados** en la **BD** (» protección de áreas de la BD)



- ✓ **Clave de cifrado secreta**
- ✓ **Algoritmo** de Cifrado **público o secreto**
- ✓ **Es el texto cifrado el que se transmite** o almacena ininteligible para quien no dispone de la clave

- ¿Cuál es la dificultad (para un infiltrado o intruso) de encontrar la clave, comparando *plaintexts* y sus textos cifrados?
- Precaución: variar la clave periódicamente
- Punto débil: ¿dónde almacenar la clave?

- ENCRIPTACIÓN DE CLAVE PÚBLICA
  - Esquema con dos claves: Clave de encriptación y Clave de descifrado ("desencriptación")
  - Ninguna puede deducirse de la otra
  - Incluso el que encripta puede ser incapaz de recuperar el *plaintext* si desconoce la clave de descifrado