TEMA 4.2: Seguridad y Confidencialidad en la Bases de Datos

a.- Confidencialidad
- Introducción
- Acceso a la base de datos (usuarios)
- Autorización de acceso a datos (permisos y roles)
- Uso de recursos del sistema (perfiles)

b.- Seguridad
- Introducción
- Tipos de Ataques
- Auditorías

4.2.a.- Confidencialidad. Introducción

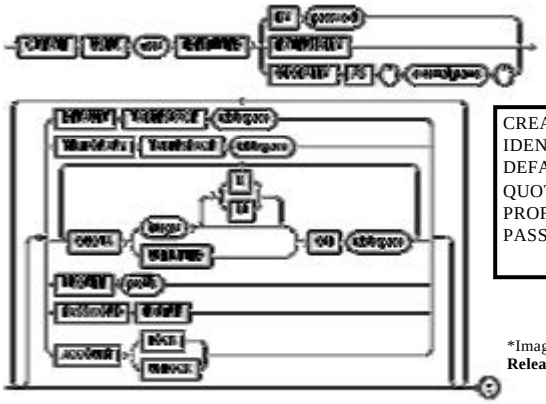
- **Objetivos:**
  - No desvelar/dejar modificar datos a usuarios no autorizados
- **Tipos de Acciones:**
  - **Cuentas de Usuario**: autentican a los usuarios para permitir el acceso a la base de datos.
    - Código y Contraseña (Oracle).
    - Identificación por Hardware
    - Características bioantropométricas (huellas dactilares, voz, retina)
    - Conocimientos, aptitudes y hábitos del usuario
  - **Permisos y Roles**: otorgar/revocar privilegios de acceso a objetos de la base de datos
  - **Perfiles**: controlan el uso de los recursos del sistema

4.2.a.- Confidencialidad. Cuentas de Usuarios

- **Tipos de Usuario (Oracle 9i):**
  - Usuario: nombre definidos en la BD que puede conectarse y acceder a objetos de la BD
  - Usuario externo: usuarios externos al SGBD (p.e.: usuarios de un Sistema Operativo)
  - Usuarios de empresa (global): grupo de usuarios (gestionados en un directorio) con permisos a las mismas BD sin necesidad de crear una cuenta o esquema en cada BD.
- **Usuarios ABD por defecto**: SYS, SYSTEM
- **Definición:**
  - Esquema: colección de objetos (tablas, vistas, clusters, procedimientos, paquetes, etc.)

4.2.a.- Confidencialidad. Cuentas de Usuarios

- **Sintaxis Oracle. Creación de Usuarios (1/2):**
  - Prerrequisitos: Privilegio de sistema *CREATE USER*



EJEMPLO

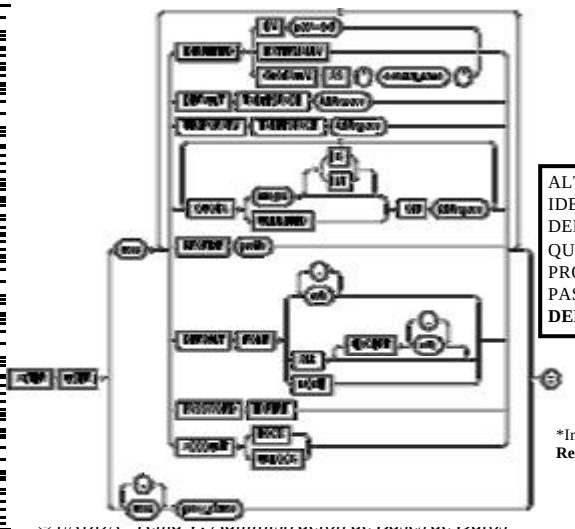
```
CREATE USER user303
IDENTIFIED BY user303
DEFAULT TABLESPACE dbd_tablespace
QUOTA 10M ON dbd_tablespace
PROFILE dbd_perfil
PASSWORD EXPIRE;
```

*Imagen extraída de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Cuentas de Usuarios

- **Sintaxis Oracle. Creación de Usuarios (2/2):**
  - NOTA: Después de crear el usuario, hay que darle permisos para que pueda acceder a los recursos de la BD.
    - Es necesario el permiso CREATE SESSION para permitir la conexión a la BD
      - GRANT CONNECT, RESOURCE TO user303;
      - (o al menos GRANT CREATE SESSION TO user303)
  - EJERCICIOS:
    1. Usuario 'Pepe' identificado de forma externa cuya cuenta no expire y cuyo tablespace temporal sea 'espacio_temporal'.
    2. Usuario 'María' identificado por la pwd 'Maria' con tablespace por defecto 'espacio_infinito' y espacio en este tablespace ilimitado.
    3. Usuario 'Juan' identificado de forma global como 'Juanillo' y cuya cuenta está inicialmente bloqueada.

4.2.a.- Confidencialidad. Cuentas de Usuarios



xis Oracle. Modificación
uarios (1/2):

EJEMPLO

```
ALTER USER user303
IDENTIFIED BY user303
DEFAULT TABLESPACE dbd_tablespace
QUOTA 10M ON dbd_tablespace
PROFILE dbd_perfil
PASSWORD EXPIRE
DEFAULT ROLE rol_user303;
```

*Imagen extraída de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Cuentas de Usuarios

- **Sintaxis Oracle. Modificación de Usuarios (2/2):**
  - NOTA: Mismos parámetros que la sentencia CREATE USER + gestión de roles.
  - EJERCICIOS:
    1. Modificar el usuario 'Pepe' identificado de forma interna por la pwd 'pepito' cuya cuenta expire.
    2. Modificar el usuario 'María' identificado de forma externa con tablespace por defecto 'espacio_infinito' y espacio en este tablespace limitado a 30 Megas. Además, este usuario ha de tener el rol por defecto llamado 'rol_usuarios_habituales'.

4.2.a.- Confidencialidad. Cuentas de Usuarios

- **Sintaxis Oracle. Borrado de Usuarios:**

*Imagen extraída de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

- **NOTA:** Se borran automáticamente TODOS los objetos del que el usuario es propietario

EJEMPLO

```
DROP USER user303 CASCADE;
```

4.2.a.- Confidencialidad. Permisos y Roles

- **Objetivo:**
  - Proporcionar a los usuarios privilegios de acceso a objetos de la BD
- **Definición:**
  - Permiso: privilegio de acceso a objetos de la BD
  - Rol: conjunto de privilegios (agrupados).
    - Simplificación en la gestión de privilegios
- **¿Quién tiene privilegios para asignar privilegios?:**
  - El ABD (privilegios de cuenta, sistema y objetos de esquemas).
  - Otros usuarios a los que le hayan dado privilegios de forma específica.
  - El propietario del esquema tiene todos los privilegios sobre sus objetos.

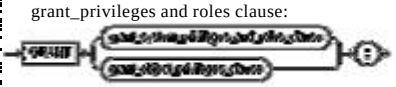
4.2.a.- Confidencialidad. Permisos y Roles

- **Tipos de privilegios de ORACLE**
  - Del sistema: ejecutar una acción en **cualquier** esquema
    - Conexión a una base de datos (create session)
    - Crear Tablespaces, borrar filas de cualquier tabla, etc.
      - Crear un esquema o relación base. *CREATE SCHEMA, CREATE TABLE*
      - Crear una vista. *CREATE VIEW*
      - Agregar o eliminar atributos de relaciones. *ALTER*
      - Eliminar relaciones o vistas. *DROP*
      - Insertar, eliminar o modificar tuplas. *MODIFY*
      - Obtener información de la BD. *SELECT*
      - …
    - Clusters, índices, disparadores, enlaces a BD, etc.
  - De objetos del esquema: ejecutar una acción en un **objeto de un esquema específico**
    - Tablas, vistas, secuencias, procedimientos, funciones y paquetes
      - Privilegio SELECT, para obtener tuplas de la relación.
      - Privilegio MODIFY, para modificar tuplas de la relación.
        - UPDATE, actualización (también a atributos)
        - DELETE, borrado
        - INSERT, insertar (también a atributos)
      - Privilegio REFERENCES, que confiere a la cuenta la capacidad de hacer referencia a la relación al especificar restricciones de integridad.
      - …

4.2.a.- Confidencialidad. Permisos y Roles

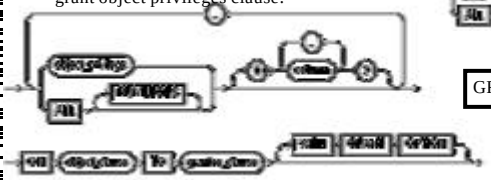
- **Sintaxis Oracle. Otorgar Privilegios: GRANT (1/3)**

grant_privileges and roles clause:



grant system_privileges and roles clause:

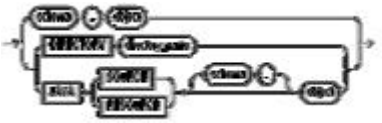
grant object privileges clause:



EJEMPLO

```
GRANT connect, resorce, create user TO user303;
```

object clause:



grantee clause

*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Permisos y Roles

- **Sintaxis Oracle. Otorgar Privilegios: GRANT (2/3)**
  - **System_privileges:** ALTER DATABASE, AUDIT SYSTEM, CREATE TABLE, DROP ANY TABLE, DELETE ANY TABLE, LOCK ANY TABLE, UPDATE ANY TABLE, SELECT ANY TABLE, CREATE VIEW, CREATE ROLE, ALTER ANY ROLE, DROP ANY ROLE, ALTER SESSION, CREATE SEQUENCE, CREATE PROCEDURE, CREATE TRIGGER, CREATE TYPE, CREATE ROLLBACK SEGMENT, CREATE USER, etc.
  - **Object_privileges:** LDD (ALTER, REFERENCES, INDEX); LMD (INSERT, DELETE, UPDATE, SELECT); READ, EXECUTE, etc.
  - **Roles predefinidos:** CONNECT, RESOURCE, DBA, EXP_FULL_DATABASE, IMP_FULL_DATABASE, etc.

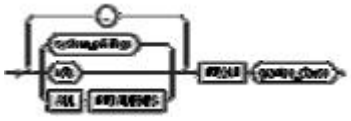
4.2.a.- Confidencialidad. Permisos y Roles

- **Sintaxis Oracle. Otorgar Privilegios: GRANT (3/3). Ejercicios**
  - **Dar permisos de crear sesión (CREATE SESSION) al usuario *user303***
  - **Dar permisos de creación de tablas (CREATE TABLE) al rol *dbd_role***
  - **Dar el rol *dbd_role* al usuario *user303* con permisos de administración**
  - **Dar todos los permisos (ALL) sobre la tabla *tabla1* del usuario *user302* al usuario *user303***
  - **Dar permisos de selección (SELECT) y modificación (UPDATE) sobre la tabla *tabla1* a todos los usuarios**

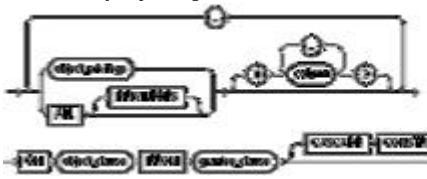
4.2.a.- Confidencialidad. Permisos y Roles

- **Sintaxis Oracle. Revocar Privilegios: REVOKE (1/2)**

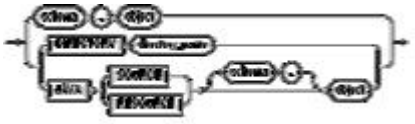
revoke_system privileges and roles clause:



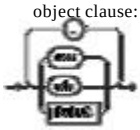
revoke object privileges clause:



grantee clause:



object clause:



*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Permisos y Roles

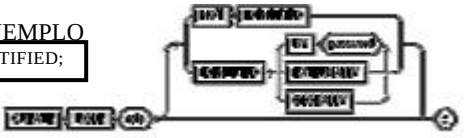
- **Sintaxis Oracle. Revocar Privilegios: REVOKE (2/2). Ejercicios**
  - **Quita el permiso de conexión (CREATE SESSION) al usuario *user303***
  - **Quita el permiso de crear tablas (CREATE TABLE) al role *dbd_role***
  - **Quita el role *dbd_role* al usuario *user303***
  - **Quita todo los permisos (ALL) sobre la tabla *tabla1* del usuario *user302* al usuario *user303***
  - **Impide seleccionar (SELECT) y modificar (UPDATE) la tabla *tabla1* a todos los usuarios (PUBLIC)**
  - **Impide borrar cualquier tabla (DROP ANY TABLE) al usuario *user303* y al role *dbd_role***

4.2.a.- Confidencialidad. Permisos y Roles

- **Sintaxis Oracle. Roles.**
  - Crear

EJEMPLO

```
CREATE ROLE usuario_dbd NOT IDENTIFIED;
```



  - Borrar

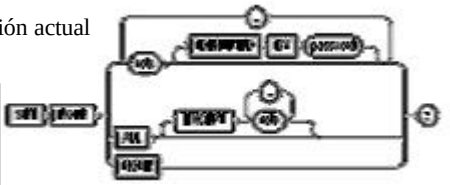
EJEMPLO

```
DROP ROLE usuario_dbd;
```

  - Activar/Desactivar roles para la sesión actual

EJEMPLOS

```
SET ROLE usuario_dbd  IDENTIFIED BY
pwd_usuario_dbd;
SET ROLE ALL;
SET ROLE ALL EXCEPT usuario_dbd;
SET ROLE NONE;
```



*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Perfiles

- **Objetivo:** gestionar el uso de los recursos de la BD
  - Establecer recursos cuando se crea el usuario: un tablespace por defecto, temporal, cuotas de espacio y uso.
  - Limitar recursos:
    - A nivel de sesión: a cada sesión un determinado tiempo de CPU, determinada cantidad de memoria
    - A nivel de llamadas: ordenes SQL.

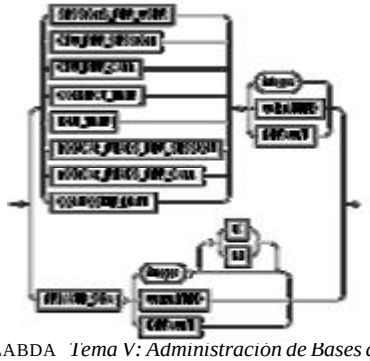
4.2.a.- Confidencialidad. Perfiles

- **Sintaxis Oracle. Perfiles (1/2):**

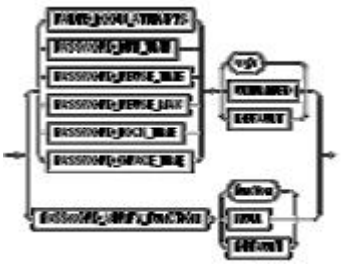
EJEMPLO

```
CREATE PROFILE perfil1 LIMIT
CPU_PER_CALL UNLIMITED
```

Resource parameters:



Pwd parameters:



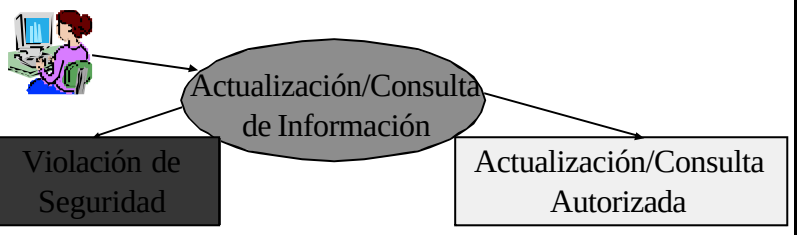
*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

4.2.a.- Confidencialidad. Perfiles

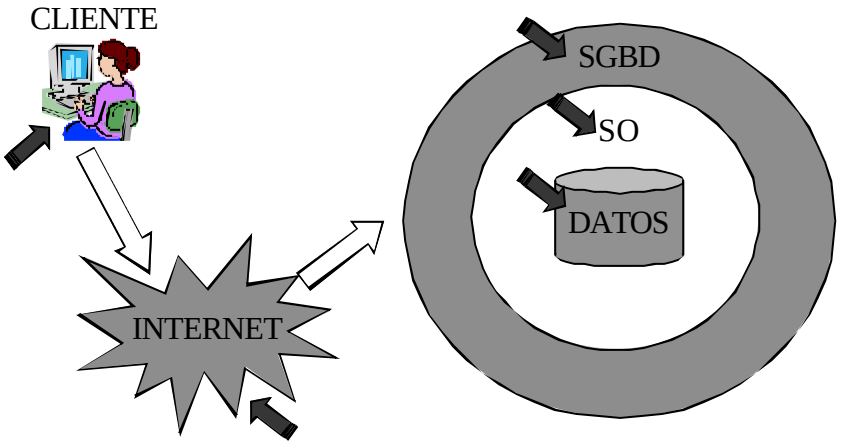
- **Sintaxis Oracle. Perfiles (2/2). Ejercicios**
  - Perfil 'p1' que limite el tiempo de acceso a CPU por llamada a 3000 segundos
  - Perfil 'p2' que limite el número de sesiones concurrentes que puede abrir el usuario a 3 y que limite también el tiempo de inactividad del usuario a 15 minutos
  - Perfil 'p3' que limite el tiempo de cpu por sesión a 500000 segundos y que limite el tiempo de vida de su contraseña a 50 días

4.2.b.- Seguridad. Introducción

- Objetivo: **proteger los datos** de accesos no autorizados
- ¿Quién puede estar interesado en atacar el sistema?
  - Un **antiguo empleado** recientemente despedido
  - Alguien **externo** a la organización
  - Un **usuario** del sistema que trata de obtener mayores privilegios
  - Un *hacker* **profesional** con un propósito específico



4.2.b.- Seguridad. Tipos de Ataques



4.2.b.- Seguridad. Tipos de Ataques. Ejemplos

- **Desbordamiento de memoria** (buffer overflow).
  - Se basa en pasar como entrada a un programa más datos de los que espera recibir.
  - Esto permite escribir en una zona de memoria más allá de la reservada (depende del S.O. entre otras cosas).
- **Inyección de Código SQL**.
  - Consiste en incluir/modificar comando SQL al enviarlos al servidor.

4.2.b.- Seguridad. Auditorías

- Para evitar posibles ataques como los anteriormente descritos deben realizarse auditorías.
- Propiedades:
  - Una **auditoría** es una revisión de los permisos de cada usuario y de los ficheros del sistema con el propósito de detectar agujeros de seguridad.
  - Una auditoría completa no es un **conjunto** estricto de **validaciones** a realizar, sino que **evoluciona** según los riesgos detectados.
  - Es una tarea ardua, consume mucho tiempo y **no asegura al 100%** que el sistema está "limpio".
- La recogida de información de auditoría puede centrarse en distintos elementos:
  - **Sentencias SQL**: Registro de los intentos de conexión con la base de datos.
  - **Privilegios**: Consiste en recopilar las operaciones que se han efectuado sobre la base de datos (inserciones, borrados, modificaciones, etc.) y por qué usuarios.
  - **Objetos**: Se pueden recoger operaciones realizadas sobre determinados objetos de la base de datos.

4.2.b.- Seguridad. Auditorías

- Sintaxis de Oracle. AUDIT

*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

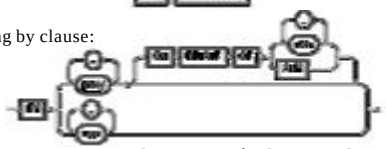
EJEMPLO

```
AUDIT SELECT ON user303.tabla1
```

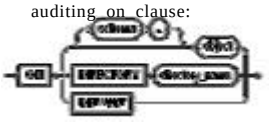
sql_statement_clause:

schema_object_clause:

auditing by clause:



auditing_on_clause:

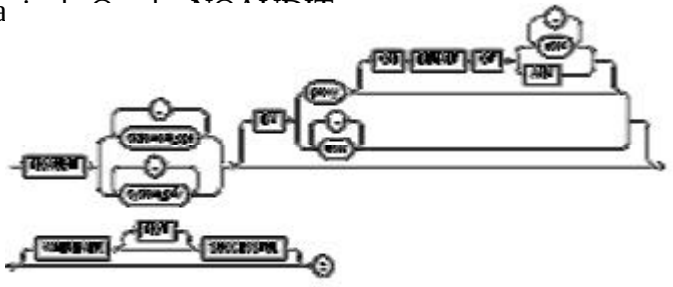


4.2.b.- Seguridad. Auditorías

- Sintaxis de Oracle. AUDIT. Ejercicios
  - Sentencias SQL
    - Auditar cada vez que se cree, borre, modifique, etc. cualquier role (ROLE)
    - Auditar cada vez que se cree, borre, modifique, etc. cualquier role (ROLE) siempre que sea exitosa la operación
    - Idem pero que la operación no sea exitosa:
    - Auditar cada vez que se seleccione (SELECT TABLE) o modifique (UPDATE TABLE) cualquier tabla
  - Privilegios
    - Auditar cada vez que el usuario *user303* o el usuario *user304* seleccione (SELECT TABLE) o modifique (UPDATE TABLE) cualquier tabla
  - Objetos de Esquemas
    - Auditar cada vez que se borre (DELETE) en la tabla *tabla1* del usuario *user303*

4.2.b.- Seguridad. Auditorías

- Sinta



EJEMPLO

```
NOAUDIT SELECT ON user303.tabla1
```

*Imágenes extraídas de [2]. **Oracle9*i* SQL Reference Release 1 (9.0.1).** Part Number A90125-01

Bibliografía

- "Fundamentos y Modelos de Bases de Datos", 2ª Edición, De Miguel y Piattini, RA-MA, 1999. (Capítulo14)
- "Fundamentos de Sistemas de Bases de Datos", 5ª Edición, Elmasri y Navathe, Addison Wesley, 2007. (Capítulo 23)
- "Oracle 9i: Administración y Análisis de Bases de Datos". César Pérez. RA-MA. 2002. (Capítulos 14, 15 y 18)
- "Oracle 10g: Administración y Análisis de Bases de Datos". César Pérez. RA-MA. 2005. (Capítulos 15, 16 y 20)
- Documentación de Oracle online:
  - [1] En General:
    - http://www.oracle.com/technology/documentation/oracle9i_arch_901.html
  - [2] Sobre Administración:
    - http://download-uk.oracle.com/docs/html/A95906_01/toc.htm
    - Todas las imágenes de estas trasparencias se han extraído de esta documentación.
  - [3] Comandos SQL y PL/SQL:
    - http://tahiti.oracle.com/pls/db901/db901.sql_keywords