# Unidad IV: Seguridad

## 4.1 Tipos de usuario

El objetivo de la creación de usuarios es establecer una cuenta segura y útil, que tenga los privilegios adecuados y los valores por defecto apropiados


Para acceder a los datos en una BD Oracle, se debe tener acceso a una cuenta en esa BD. Cada cuenta debe tener una palabra clave o password asociada. Una cuenta en una BD puede estár ligada con una cuenta de sistema operativo. Los passwords son fijados cuando se crea un usuario y pueden ser alterados por el DBA o por el usuario mismo. La BD almacena una versión encriptada del password en una tabla del diccionario llamada dba_users. Si la cuenta en la BD está asociada a una cuenta del sistema operativo puede evitarse la comprobación del password, dándose por válida la comprobación de la identidad del usuario realizada por el SO.

Un usuario Oracle tiene las siguientes caracteristicas

- Un nombre de usuario de 30 caracteres o menos, sin caracteres especiales y que inicie con una letra.
- Un metodo de autentificacion, el más comun es un password pero Oracle 10G soporta otros métodos como biometric, certificado y autentificacion por medio de token.
- Un tablespace de default, el cuál es donde el usuario va a poder crear sus objetos por defecto. Ojo, no porque tenga un tablespace de default va a significar que puede crear objetos, o una quota de espacio. Estos permisos se asignan de forma separada.
- Un tablespace temporal, donde el usuario pueda crear sus objetos temporales y hacer ordenar las consultas.
- Un perfile de usuario, es decir las restricciones o privilegios de su cuenta.

Una cuenta MySQL se define en términos de un nombre de usuario y el equipo o equipos desde los que el usuario puede conectar al servidor. La cuenta también tiene una contraseña (deseable). Los nombres de usuario y contraseñas en MySQL no están relacionadas con los del sistema operativo.

- Nombre de usuarios en MySQL pueden tener como máximo 16 caracteres de longitud
- La contraseña es segura incluso si los paquetes TCP/IP pasan por un sniffer o la base de datos mysql se captura.

## 4.2 Creación de usuarios

`CREATE USER`: Crear un usuario oracle.

Un usuario es un nombre de acceso a la base de datos oracle asociado a una clave (password).

Lo que puede hacer un usuario logeado a la base de datos depende de los permisos que tenga asignados ya sea directamente (`GRANT`) como sobre algun rol que tenga asignado (`CREATE ROLE`).

El perfil que tenga asignado influye en los recursos del sistema de los que dispone un usuario a la hora de ejecutar Oracle (`CREATE PROFILE`).

```
CREATE USER usuarioLimitado
IDENTIFIED BY miClaveSecreta;

CREATE USER usuarioLimitado2
IDENTIFIED BY miClaveSecreta
PASSWORD EXPIRE;
```

ORACLE

```
CREATE USER usuarioLimitado
IDENTIFIED BY 'miClaveSecreta';
```

MySQL

## 4.3 Privilegios a usuarios

Una vez creados los usuarios será necesario dotarlos de privilegios para que puedan realizar operaciones específicas en la base de datos. Estos privilegios suelen clasificarse en privilegios del sistema (operaciones que afectan a todo el sistema) y privilegios de objeto (tablas, vistas, etc.). Para conocer los privilegios y su sintaxis es necesario consultar los manuales de referencia de su SGBD.

SELECT * FROM system_privilege_map;

Las sentencias `GRANT` y `REVOKE` permiten a los administradores de SGBD crear cuentas de usuario, conceder y revocar derechos de esas cuentas.

```
GRANT CONNECT, RESOURCE, CREATE TABLE
TO usuarioLimitado;
```

## 4.4 Roles

Un rol es una colección de privilegios del sistema y de objetos que se otorgan a usuarios y a otras tareas. Oracle dispone de muchos roles predeterminados mientras que MySQL no los soporta.

El rol `CONNECECT` permite al usuario conectarse a la base de datos, crear tablas, vistas, secuencias, sinónimos y otros objetos en el esquema asociado.

El rol `RESOURCE` permite permite al usuario utilizar los recursos típicos para la programación de aplicaciones (clusters, disparadores, paquetes, funciones, etc.)

El rol DBA, típico de los administradores, permite al usuario realizar cualquier función de base de datos y disponer de cualquier privilegio

La sentencia que permite crear roles es CREATE ROL. Su sintaxis es la siguiente

```
CREATE ROLE rol
[ NOT IDENTIFIED
| IDENTIFIED {BY password | USING [usuario.] paquete
| EXTERNALLY | GLOBALLY }
];
```

`NOT IDENTIFIED` indica que no se requiere contraseña para utilizar el rol, `INDENTIFIED BY` password indica que se requiere la contraseña especificada. `EXTERNALLY` crea un rol de usuario externo y `GLOBALLY` crea un rol de usuario global.

## 4.5 Vistas

Una vista es una tabla virtual cuyo contenido está definido por una **consulta**

Una vista es sencillamente un objeto de base de datos que presenta datos de tablas. Se trata de una consulta SQL que está permanentemente almacenada en la Base de datos y a la que se le asigna un nombre, de modo que los resultados de la consulta almacenada son visibles através de la vista, y SQL permite acceder a estos resultados como si fueran de hecho una tabla real en la base de datos.

Las tablas y las vistas comparten el mismo espacio de nombres en la base de datos, por lo tanto, una base de datos no puede contener una tabla y una vista con el mismo nombre.

Las vistas suelen utilizarse para centrar, simplificar y personalizar la percepción de la base de datos para cada usuario. Las vistas pueden emplearse como mecanismos de seguridad, que permiten a los usuarios obtener acceso a los datos por medio de la vista, pero no les conceden el permiso de obtener acceso directo a las tablas subyacentes de la vista. Las vistas se pueden utilizar para realizar

particiones de datos y para mejorar el rendimiendo cuando se copian, se importan y se exportan datos.

Mediante vistas es posible presentar datos de distintos servidores. Por ejemplo, para combinar datos de distintos servidores remotos o en un servidor de multiples procesadores, cada uno de los cuales almacenan datos para una región distinta de su organización, puede crear consultas distribuidas o paralelas aumentando la eficiencia de las consultas.

Mediante diversas cláusulas es factible crear, modificadar, eliminar y administrar vistas. La sintaxis básica para estas cláusulas es generica entre diversos gestores de base de datos. Sin embargo en lo particular cada gestor implementa la administración de estas de forma diferente. En este documentos se presenta la sintaxis particular dee Oracle 10g, comparando en forma generica con MySQL 5.

La sintaxis básica de una vista (Oracle y MySQL) es:

```
CREATE VIEW nombre_vista AS consulta;
```