

Prácticas de

Administración de Bases de Datos

Grado en Ingeniería Informática

**PRÁCTICA 10**

Seguridad en las Bases de Datos (privilegios, roles)

# OBJETIVOS

* Adquirir destreza en la gestión de la confidencialidad
* Aprender a gestionar privilegios y roles

**Ejercicios de privilegios y roles**

Para realizar estos ejercicios vamos a partir de una base de datos sencilla (con tres tablas). Esto nos servirá para recordar la sintaxis de la sentencia CREATE TABLE.

La base de datos mantiene información acerca de los alumnos de una academia de preparación para oposiciones donde se imparten cursos de diferentes áreas. La descripción de las tablas es la siguiente:

|  |  |  |  |
| --- | --- | --- | --- |
| **TABLA** | **COLUMNAS** | **TIPO** | **COMENTARIO** |
| **ESTUDIANTE** | nombre | texto(40) | nombre del estudiante |
| dni | texto(8) | clave primaria de la tabla |
| fechaNac | fecha | fecha de nacimiento |
| curso | texto(3) | código del curso en el que está matriculado un estudiante. Clave ajena de  la tabla CURSO |
|  | | | |
| **CURSO** | nomCurso | texto(20) | nombre del curso |
| codCurso | texto(3) | clave primaria de la tabla |
| profesor | texto(8) | nombre del profesor que imparte el curso. Clave ajena de la tabla PROFESOR |
| horas | numérico(3) | número de horas del curso |
|  | | | |
| **PROFESOR** | nombre | texto(40) | nombre del profesor |
| dni | texto(8) | clave primaria de la tabla |
| sueldo | real | sueldo del profesor |

1. Mediante la sentencia SQL CREATE USER, crear un usuario (que será el propietario de las tablas), con las siguientes características:
   * El usuario debe ser identificado por Oracle
   * Nombre: **admin**
   * Contraseña: **admin**
   * El espacio de tablas por defecto debe ser ET\_USUARIOS (se supone que ya lo habéis creado en práctica anterior)
   * El espacio de tabla temporal será TEMP
   * La cuota de usuario será de 2M sobre ET\_USUARIOS
   * Asignar al usuario el perfil ESTUDIANTE\_ABD creado anteriormente
2. Crear el rol ***"mi\_conexion"*** con los privilegios para poder conectarse y crear tablas
3. Desde el usuario SYS, otorgar al usuario ***“admin”*** el rol ***"mi\_conexion"***
4. Comprobar en la vista correspondiente cuales son los roles asignados al usuario

## “admin”

1. Consultar la tabla o vista adecuada para saber en qué espacios de tabla puede escribir el usuario ***“admin”***
2. Con el usuario ***"admin"***, ejecutar el script de creación de las tablas **(es conveniente que, además de ejecutar el script, le echéis un vistazo a la sintaxis para recordar conceptos)**
3. Asignar cuota cero en el espacio de tablas por defecto para el usuario ***"admin"***. Vuelve a consultar la tabla o vista adecuada para saber en qué espacios de tabla puede escribir el usuario ***“admin”.*** Comprobar si Siguen estando sus objetos
4. Cambiarle la cuota a 2 Megas sobre ET\_USUARIOS al usuario admin y conectados como dicho usuario ejecutar el script ***InsertaDatos.sql***.
5. Desde el usuario ***"estudiante"*** intentar consultar los datos introducidos en las tablas. ¿Es posible?, ¿por qué?, ¿cuál es el mensaje de error?, ¿piensas que es intuitivo el mensaje de error?
6. Desde el usuario ***"admin"***, otorgar al usuario ***"estudiante"*** privilegios de consulta sobre la tabla **ESTUDIANTE**. Recordad validar cada operación para que sea efectiva para el otro usuario (comando ***commit***).
7. Volver a intentar el ejercicio 9 con la tabla **ESTUDIANTE**
8. Desde los usuarios ***"admin"*** y ***"estudiante"***, consultar las tablas del diccionario de datos. Para cada tabla (USER\_TAB\_PRIVS, USER\_TAB\_PRIVS\_MADE y USER\_TAB\_PRIVS\_RECD) proporcionar una breve explicación de cada campo
9. Otorgar privilegio de consulta al usuario ***"estudiante"*** sobre todos los atributos de la tabla **PROFESOR** excepto del sueldo (recuerda que al privilegio SELECT no se le puede indicar, explícitamente, las columnas para consultar). Buscar un mecanismo que haga la misma función.
10. Otorgar privilegios de consulta al usuario ***"estudiante"*** sobre todos los atributos de la tabla **CURSO** y de inserción sobre todos los campos excepto el D.N.I. del profesor. Comentar el resultado obtenido al intentar realizar las siguientes operaciones desde la cuenta del usuario ***"estudiante"***:
    * Insertar una tupla completa en la tabla CURSO
    * Insertar una tupla para un CURSO sin poner el D.N.I. del profesor
    * Visualizar el nuevo contenido de la tabla CURSO
11. Desde el usuario ***"admin"*** crear el rol ***"PRIVADO"*** identificado por la contraseña

## "priv"

1. Desde el usuario ***"admin"*** asignarle el rol ***"PRIVADO"*** al usuario ***"estudiante"***
2. Comprobar los roles asignados al usuario ***"estudiante"****.* ¿El rol ***“PRIVADO”*** es un rol por defecto?
3. Desde el usuario ***"admin"***, hacer que el rol ***"PRIVADO"*** no esté activo para el usuario ***"estudiante"*** cuando se conecte
4. Comprobar de nuevo los roles asignados al usuario ***"estudiante"****.* ¿El rol

***“PRIVADO”*** es ahora un rol por defecto?

1. Con el usuario ***"estudiante"*** comprobar en la vista apropiada del diccionario de datos los roles activos en su sesión. Desde el propio usuario, activar el rol ***"PRIVADO"*** y volver a hacer la comprobación
2. La política de seguridad de la empresa está centralizada en el administrador de la base de datos, que debe decidir qué tipos de privilegios deben concederse a cada usuario para el acceso a las tablas **PROFESOR**, **CURSO** y **ESTUDIANTE**. Después de realizar un estudio exhaustivo, el ABD ha decidido crear los siguiente grupos:

# Grupo Estudiantes

Formado por los estudiantes de la academia. Estos sólo podrán consultar datos no significativos de la BD:

* + Nombre de los estudiantes
  + Información de los cursos excepto el dni del profesor
  + Nombre de los profesores

# Grupo Profesores

Este grupo, además de tener los privilegios del grupo de alumnos, también podrá modificar y eliminar información de la tabla PROFESOR

# Grupo Gestores

Este grupo, al que pertenece el usuario ***"admin"***, debe tener todos los privilegios sobre todas las tablas

Teniendo en cuenta esta información, desde el usuario ***"admin"*** realizar los siguientes ejercicios:

1. Crear todos los roles necesarios para implementar esta política de seguridad, asignándole a cada rol los privilegios convenientes en cada caso.
2. Para verificar que se ha realizado bien el ejercicio anterior, crear un nuevo usuario y asignar/revocar diferentes roles, comprobando que cuando lo tiene asignado puede hacer las operaciones que se piden pero no puede hacer otras que tenga prohibidas