

DIVISIÓN DE INGENIERÍA EN SISTEMAS COMPUTACIONALES



MANUAL DE ADMINISTRACIÓN DE BASE DE DATOS

Semestre 2020-1

PRESENTACIÓN DE PRÁCTICAS DE TALLER O LABORATORIO

El estudiante desarrollará la(s) práctica(s), de sus asignaturas, a la par que deberá elaborar el informe de las mismas a través del formato específico para tal fin, el cual podrá ser llenado a mano o en computadora, de acuerdo a las instrucciones específicas del profesor y a la práctica a realizar.

2

LLENADO DE FORMATO A MANO



- El estudiante deberá imprimir el formato de práctica, con la anticipación suficiente para tenerlo listo antes de ingresar a la práctica
- El estudiante lo deberá llenar con letra legible
- El docente lo deberá firmar y/o sellar al final de la práctica

LLENADO DE FORMATO EN COMPUTADORA

- El estudiante lo mostrará al docente, cuando durante la clase éste se lo solicite
- El estudiante deberá llenar el formato, durante la práctica, de acuerdo a los siguientes lineamientos:
 1. Ser concisos y claros
 2. Escribir con interlineado a 1.0
 3. Textos: letra Arial 12, en mayúsculas y minúsculas
 4. Títulos: Arial 14 en mayúscula, negrilla y centrado (nunca lleva punto al final); Subtítulos: Arial 12, mayúscula, al margen izquierdo (lleva punto cuando el texto inicia en el mismo renglón y no lleva punto cuando el texto inicia en el siguiente renglón).
 5. Párrafos: Procurar que la extensión sea de 6 a 10 renglones, aproximadamente. Al inicio de un capítulo o apartado, el primer párrafo no lleva sangría; a partir del segundo párrafo y hasta el último, todos llevan sangría (se puede poner con un tabulador).

6. Citas y referencias según Manual APA¹ (solo cuando sea necesario)
7. Para cuadros y tablas manejar Arial 10
8. Para pie de cuadro, tabla o figura, manejar Arial 8
9. Se entregará al docente en formato electrónico de acuerdo a indicaciones o impreso la siguiente sesión

¹ Ver ANEXO: APLICACIÓN DE ESTILO APA A PARTIR DE WORD

	INGENIERÍA EN SISTEMAS COMPUTACIONALES PRÁCTICA No. 9	
---	--	---

DATOS GENERALES	
ASIGNATURA ADMINISTRACIÓN DE BASE DE DATOS	
TÍTULO DE LA PRÁCTICA: USUARIOS	
DOCENTE M. EN DISW. VIRGINIA AGUILAR GUERRERO	
ESTUDIANTES: <ul style="list-style-type: none"> • Cadena González Luis Raúl. • Cortes Vásquez Gustavo. • Espinosa Sánchez Daniel Antonio. 	FECHA 31/05/2020

OBJETIVO DE LA PRÁCTICA (6) Crear usuarios con sus respectivos roles y privilegios.	
COMPETENCIA(S) ESPECÍFICA(S)(7) Implementar mecanismos de seguridad básicos para el acceso a datos mediante el otorgamiento o denegación de privilegios.	COMPETENCIA(S) GENÉRICA(S)(8) <ul style="list-style-type: none"> <input type="checkbox"/> Capacidad de comunicación oral y escrita. <input type="checkbox"/> Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. <input type="checkbox"/> Capacidad de trabajo en equipo. <input type="checkbox"/> Habilidad para trabajar en forma autónoma.

REQUERIMIENTOS

FÓRMULAS/TÉCNICAS/PROCESOS/PROCEDIMIENTOS (9)

Con ayuda del SGBD asignado por cada equipo realizar lo siguiente en consola.

Alumno	SGBD Asignado
AGUIRRE VELAZQUEZ LUIS RAYMUNDO	Redis
ALVAREZ MUÑOZ LEONARDO DAVID	Elasticsearch
AMARO OLAYA JOSE ALFREDO	Elasticsearch

ARCOS JACOME ELVIA VANESSA	Cubrid
CADENA GONZALEZ LUIS RAUL	Informix
CALDERON PEREZ ANA KAREN	Redis
CORONA LOPEZ RAFAEL	Fox Pro
CORTES VASQUEZ GUSTAVO	Informix
ESCUDERO VILLA JOAQUIN GUSTAVO	Cubrid
ESPINOSA SANCHEZ DANIEL ANTONIO	Informix
ESTRADA HERNANDEZ JUAN CARLOS	Fox Pro
FLORES ALCALA ROBERTO ALDAI	Cassandra
GARCIA CATARINO JOSE MANUEL	DB2
JUAREZ ROSALES KAREN CITLALI	Cassandra
LOPEZ PEREZ JULIO CESAR	Couch DB
LOPEZ RAMIREZ LIZBETH	Elasticsearch
MARTINEZ ALVAREZ GERARDO	Couch DB
MEDINA GARCIA JOSE	Redis
MEJIA MARTINEZ RICARDO	Couch DB
MUJICA HERNANDEZ BRIAN EDUARDO	Neo4j
MUNGUIA OLIVO ANGEL ADRIAN	Apache derby
RAMOS GALICIA VALERIA ALEJANDRA	DB2
RAMOS RAMIREZ MARIA FERNANDA	Cubrid
ROMERO ROSALES ALOYSIUS GABRIEL	Riak
SANTOS PEREZ JOSE MANUEL	Apache derby
SORIANO LOPEZ ALBERTO	Cassandra
TREJO PEREZ ADRIAN	Apache derby
VAZQUEZ BAUTISTA DANIEL	Neo4j
VICTORIA MUÑOZ ADRIAN ALFREDO	Riak

1. Crear tres usuarios en el SGBD asignando.
2. El primer usuario se llamará Administrador cuya contraseña con la cual será identificado será qwerty el cual contendrá un rol llamado admin1 con todos los privilegios.
3. El segundo usuario se llamará cliente cuya contraseña con la cual será identificado asdfg el cual contendrá un rol llamado cli1 con los siguientes privilegios: seleccionar, insertar y actualizar tablas, créate sesión.
4. El tercer usuario se llamará informático cuya contraseña con la cual será identificado poiuy el cual contendrá un rol llamado info1 con los siguientes privilegios: seleccionar tablas, create sesión.
5. Los usuarios dos y tres deben ser creados desde la conexión del usuario administrador (System).

6. Investigar como alterar un usuario y como eliminarlo (sentencia sql aplicada a uno de los usuarios ya creados anteriormente)

RECURSOS MATERIALES (10)
LAP TOP
MAQUINA DE ESCRITORIO

RECURSOS TÉCNICOS/TECNOLÓGICOS (11)
LABORATORIO
SW ORACLE 11G XE

MARCO TEÓRICO (12)

USUARIOS

Información de usuarios

Seguridad de Cuentas

Oracle pone al alcance del DBA varios niveles de seguridad:

- Seguridad de cuentas para la validación de usuarios.
- Seguridad en el acceso a los objetos de la base de datos.
- Seguridad a nivel de sistema para la gestión de privilegios globales.

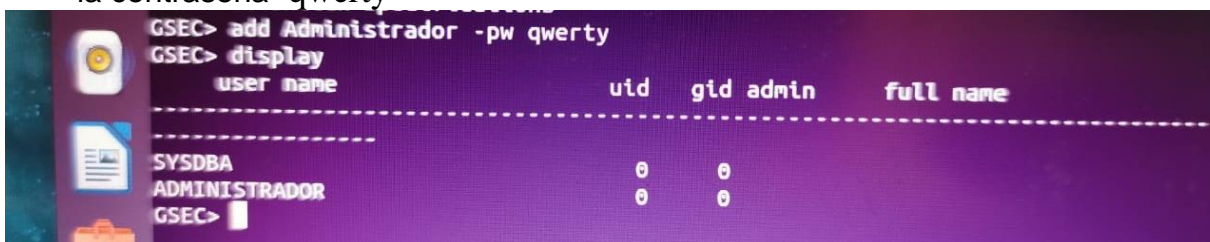
Para acceder a los datos en una BD Oracle, se debe tener acceso a una cuenta en esa BD. Cada cuenta debe tener una palabra clave o *password* asociada. Una cuenta en una BD puede estar ligada con una cuenta de sistema operativo. Los *passwords* son fijados cuando se crea un usuario y pueden ser alterados 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.

DESARROLLO

Hay que tener en cuenta que para poder realizar ciertas sentencias tendremos que estar

ubicados entre los apartados GSEC o SQL respectivamente, esto dependiendo de las acciones que se van a realizar. Además, lo principal para poder realizar cualquier primera modificación es tener que iniciar sesión con el usuario SYSDBA ya que es el principal administrador de SGBD.

1. Primero nos pide la creación de un usuario “ADMINISTRADOR” el cual contendrá la contraseña “qwerty”



```
GSEC> add Administrador -pw qwerty
GSEC> display
  user name      uid  gid admin  full name
-----
SYSDBA          0    0
ADMINISTRADOR   0    0
GSEC>
```

2. A continuación, procederemos a realizar la creación de los “ROLES” cada uno de estos con sus respectivos “Privilegios”

- a. Primero crearemos un ROL de nombre “admin1”



```
SQL> CREATE ROLE admin1;
```

Este contendrá todos los PRIVILEGIOS “ALL”



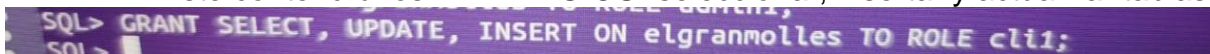
```
SQL> GRANT ALL ON elgranmolles TO ROLE admin1;
```

- b. Posteriormente crearemos un ROL de nombre “cli1”



```
SQL> CREATE ROLE cli1;
```

Este contendrá los PRIVILEGIOS “seleccionar, insertar y actualizar tablas”



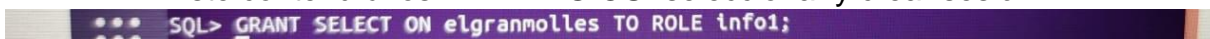
```
SQL> GRANT SELECT, UPDATE, INSERT ON elgranmolles TO ROLE cli1;
```

- c. Por ultimo crearemos un ROL de nombre “info1”



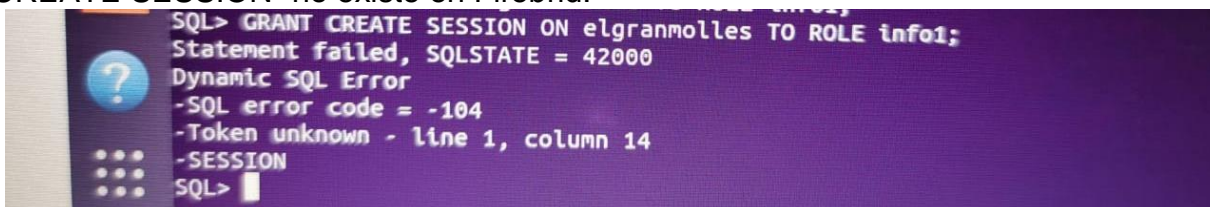
```
SQL> CREATE ROLE info1;
```

Este contendrá los PRIVILEGIOS “seleccionar y crear sesión”



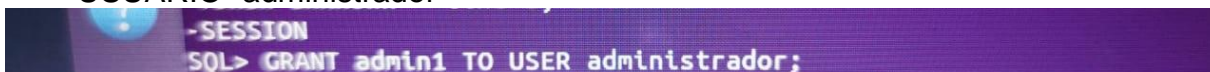
```
SQL> GRANT SELECT ON elgranmolles TO ROLE info1;
```

En este apartado solo que coloca el PRIVILEGIO “select”, dado que “CREATE SESSION” no existe en Firebird.



```
SQL> GRANT CREATE SESSION ON elgranmolles TO ROLE info1;
Statement failed, SQLSTATE = 42000
Dynamic SQL Error
-SQL error code = -104
-Token unknown - line 1, column 14
-SESSION
SQL>
```

3. Una vez creados los roles con sus respectivos privilegios, deberemos crear dos usuarios más, pero esto deberán ser creados con el primer usuario “administrador”. Para esto primero tendremos que asignarle el ROL “admin1” al USUARIO “administrador”



```
SQL> GRANT admin1 TO USER administrador;
```

4. Una vez realizada dicha acción, procederemos a la creación de dichos usuarios, estos se llamarán “cliente” e “informático” con las contraseñas “asdfg” y “poiuy” respectivamente.


```
SQL> CREATE USER cliente PASSWORD 'qwerty';
SQL> CREATE USER informatico PASSWORD 'poiuy';
```

5. Posteriormente procederemos a asignarles sus respectivos ROLES a cada uno de estos usuarios.

```
SQL> GRANT cli1 TO USER cliente;
SQL> GRANT info1 TO USER informatico;
SQL>
```

6. Por último, se nos pide la realización de una investigación de sentencias, estas son: Alterar y borrar un USUARIO.

SINTAXIS:

- ALTER USER NombreUsuario [SET] [PASSWORD 'Contraseña'];
- DROP USER NombreUsuario;

```
SQL> ALTER USER cliente SET PASSWORD 'walter';
SQL> DROP USER informatico;
SQL>
```

RESULTADOS

Como se puede observar en las capturas de pantalla, correspondientes a cada uno de los procesos establecidos, se puede intuir que dichos objetivos establecido en la práctica se encuentran cumplidos, sin problemas o error alguno.

CONCLUSIONES

Esta práctica ha puesto a prueba nuestros conocimientos de investigación, puesto que ha sido complicado encontrar y aplicar los comandos (sentencias), dado a que se encuentra muy poca información para sistemas basado en Linux y a esto sumándole la versión más reciente del mismo SGBD. En general, dicha práctica tuvo una complejidad difícil pero no imposible.

Esta práctica ha sido una de las más difíciles en cuanto a su desarrollo, puesto que se encuentra muy poca información sobre este gestor de base de datos, también que tiene una gran complejidad al momento de realizar sentencias, ya que muchas de estas se tienen que ejecutar en GSEC o SQL, dependiendo de lo que se desea realizar.

Este trabajo es más que nada de investigación y bastante paciencia ya que se debe de crear y tener en cuenta las diferentes sentencias que manejan los Sistemas Gestores de Base de Datos logrando ser muy cauteloso al momento de crear los usuarios asignándoles ciertos privilegios con ayuda de los roles logrando así la manipulación de sus privilegios de cada uno de ellos.

FUENTE(S) DE INFORMACIÓN

<https://firebird21.wordpress.com/2013/04/21/agregando-modificando-y-borrando-usuarios/>
https://www.firebirdsql.org/file/documentation/papers_presentations/html/paper-fb-macosx-getstart.html#paper-fb-macosx-getstart-usrsroles
<https://firebirdsql.org/refdocs/langrefupd25-security-rdbadmin.html>
https://firebirdsql.org/file/documentation/reference_manuals/fblangref25-en/html/fblangref25-ddl-role.html

https://firebirdsql.org/file/documentation/reference_manuals/fblangref25-en/html/fblangref25-security-privs.html#fblangref25-security-privs-grant
https://firebirdsql.org/file/documentation/release_notes/html/en/3_0/rnfb30-access-sql.html
https://firebirdsql.org/file/documentation/reference_manuals/fblangref25-en/html/fblangref25-security-auth.html
https://firebirdsql.org/refdocs/langrefupd25-intfunc-set_context.html

NOMBRE Y FIRMA DEL DOCENTE (17)

EVALUACIÓN (18)