



## Actividad: "SENTENCIAS EN SQL"

**Describe el uso de cinco sentencias SQL que permiten los privilegios, vistas y cifrados para acceder a la información de una base de datos.**

**PRIVILEGIOS:** son enunciados que especifican cuáles usuarios tienen acceso a cuál información, y cuáles operaciones les está permitido utilizar sobre qué datos. El mecanismo de autorización está diseñado para proteger la base de datos al impedir a las personas la lectura, actualización o eliminación no autorizada del contenido de la base de datos.

**VISTAS:** una vista es una tabla virtual, una tabla que en realidad no existe pero se puede construir al realizar operaciones como selección, proyección, combinación u otros sobre los valores de las tablas existentes , además permite ocultar porciones de la base de datos de ciertos usuarios. El usuario no está al tanto de la existencia de algunos atributos que faltan de su vista. También permite a los usuarios acceder a los datos en una forma "personalizada".

**CIFRADO:** Se utiliza en la base de datos en la que se está gestionando información sensible, o se requiere incrementar el nivel de seguridad de la información, mediante algoritmos de cifrado.

Sólo el sistema de gestión de bases de datos (SGBD) puede descifrarlos, de modo que cualquier persona que los obtenga por otros medios recibirá datos sin sentido. Cuando los usuarios autorizados acceden a la información de manera adecuada, el SGBD recupera los datos y los decodifica en forma automática. El encriptado también debe usarse siempre que los datos se envíen a otros sitios, a fin de que quien intervenga las líneas también los reciba en forma cifrada. El encriptado requiere un sistema de encriptado, que consiste en los componentes que se mencionan a continuación:



**Alumno: Pedro Daniel Rojas Medina**  
**ADMINISTRACIÓN DE BASE DE DATOS**

- Un algoritmo de encriptado, que toma al texto normal (texto plano) como entrada, hace algunas operaciones con éste y produce como salida al texto en clave (texto encriptado)
- Una clave de encriptado, que es parte de entrada para el algoritmo de encriptado, y se elige de un conjunto muy grande de claves posibles
- Un algoritmo de desencriptado, que opera sobre el texto encriptado como entrada y produce al texto plano como salida
- Una clave de desencriptado, que es parte de entrada para el algoritmo de desencriptado y se escoge de un conjunto muy grande de posibles claves.

## PRIVILEGIOS – GESTIÓN DE USUARIOS:

```

Privilegios - Gestión de Usuarios x Administración de Vistas Cifrado Datos

1  /*VISUALIZAR USUARIOS CON SUS PRIVILEGIOS*/
2  • USE mysql;
3  • DESC user;
4  • SELECT * FROM USER;
5  /*Y=YES SIGNIFICA QUE EL USUARIO POSEE ESE PRIVILEGIO*/
6  /*N=NO SIGNIFICA QUE EL USUARIO NO TIENE ESE PRIVILEGIO*/
7
8  /*VISUALIZAR LOS USUARIOS DEL MYSQL - (Previamente deberemos seleccionar una BD con "USE"*/
9  • SELECT USER FROM USER;
10
11 /*CREAR USUARIO*/
12 • CREATE USER 'nombreUsuario'@'ubicación' IDENTIFIED BY 'contraseñaUsuario';
13 /*Ejemplo*/
14 • CREATE USER 'DanielMedina'@'localhost' IDENTIFIED BY 'utelesup123';
15
16 /*ASIGNAR PRIVILEGIOS A UN USUARIO*/
17 • GRANT SELECT , INSERT , UPDATE , DELETE
18   ON nombreBaseDatos.tablaBaseDatos
19   /* EL PRIMER ASTERISCO SIRVE PARA INDICAR EL NOMBRE DE LA BASE DE DATOS , EL PUNTO SEPARA EL NOMBRE DE LA BASE DE DATOS
20   CON EL NOMBRE DE LA TABLA QUE SE VA A ASIGNAR LOS PRIVILEGIOS DEL GRANT*/
21   /*EN CASO DE QUERER ASIGNAR LOS PRIVILEGIOS A TODA LA BASE DE DATOS SE UTILIZA : *.*          */
22   TO 'nombreUsuario'@'ubicación';
23
24 /*Ejemplo : Asignar permisos de selección , insercción , actualización y eliminación de datos*/
25 • GRANT SELECT , INSERT , UPDATE , DELETE
26   ON baseDatosAlumno.Formulario
27   TO 'DanielMedina'@'localhost';
28
29   /*Ejemplo : Asignar TODOS los permisos a 2 usuarios de la base de datos , Los usuarios van separados por comas , su
30   nombre y ubicación van entre comillas simples 'nombre' y su ubicación va separado por arroba @ */
31 • GRANT ALL
32   ON baseDatosAlumno.Formulario
33   TO 'DanielMedina'@'localhost','MaribelSanchez'@'localhost';
34
35 /*QUITAR PRIVILEGIOS A UN USUARIO */
36 • REVOKE SELECT , INSERT , UPDATE , DELETE
37   ON baseDatos.Tabla
38   FROM 'nombreUsuario';
39

```

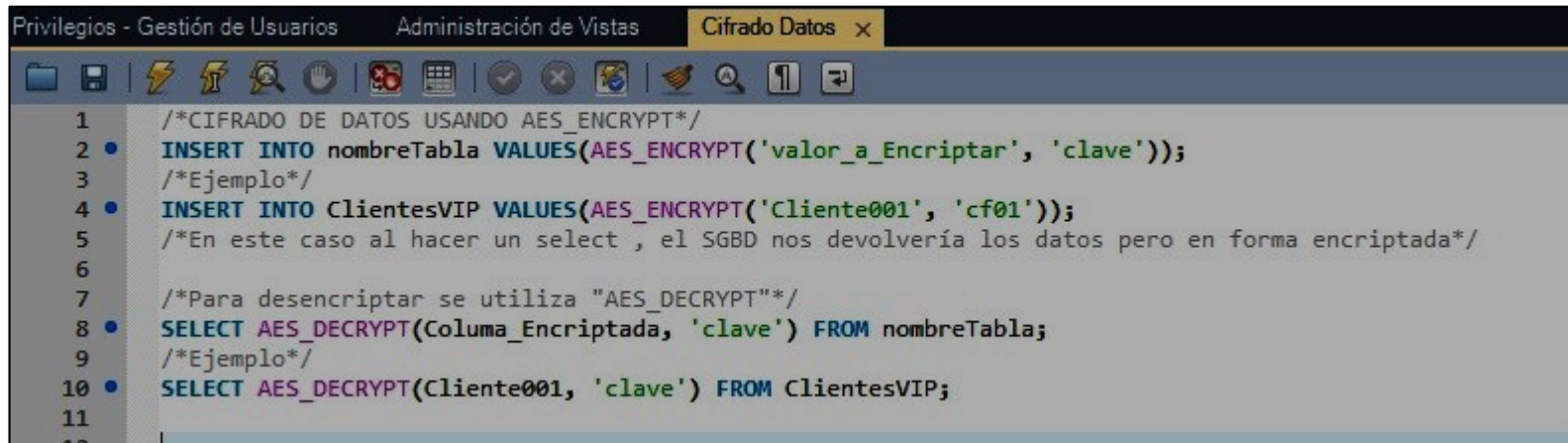
```
40  /*Ejemplo : Quitar privilegios de inserción y actualización , en la tabla transacciones de la
41  BD "Finanzas" , a 2 usuarios de la base de datos@ */
42  • REVOKE INSERT , UPDATE
43  ON baseFinanzas.Transacciones
44  FROM 'Isabel'@'localhost', 'Andrea'@'localhost';
45
46  /*Ejemplo : Quitar TODOS los permisos a un usuario de la BD "Personal" y todas las tablas */
47  • REVOKE ALL
48  ON Personal.*
49  FROM 'Isabel'@'localhost';
50
51  /*BORRAR UN USUARIO*/
52  • DROP USER 'nombreUsuario'@'ubicación';
53
54  /*Ejemplo : Borrar al usuario "DanielMedina" */
55  • DROP USER 'DanielMedina'@'localhost';
56
57  /*VISUALIZAR PRIVILEGIOS*/
58  • SHOW GRANTS FOR 'nombreUsuario';
59
60  /*Visualizar los permisos del usuario "DanielMedina"*/
61  • SHOW GRANTS FOR 'DanielMedina';
62
```

## VISTAS:

```
Privilegios - Gestión de Usuarios  Administración de Vistas x  Cifrado Datos

1  /*CREACIÓN DE UNA VISTA */
2  • CREATE VIEW nombreVista AS SELECT * FROM nombreTabla;
3
4  /*Crear una vista para la base de datos "PRODUCTO" llamada vista_productos y que describa el nombre del producto , su
5  descripción , precio y cantidad disponible*/
6
7  • CREATE VIEW Vista_Productos AS SELECT nombre_producto,descripción_producto,precio_producto,
8  stock_disponible AS 'Cantidad Disponible en Tienda' FROM producto;
9
10 /*Para consultar la vista creada anteriormente */
11 • SELECT * FROM Vista_Productos;
12
13 /*Para actualizar una vista usando "OR REPLACE"*/
14 • CREATE OR REPLACE VIEW Vista_Productos AS SELECT nombre_producto,descripción_producto FROM producto;
15
16 /*Visualizar la definición de una vista*/
17 • SHOW CREATE VIEW nombre_Vista;
18 /*Ejemplo*/
19 • SHOW CREATE VIEW Vista_Productos;
20
21
22 /*ELIMINAR UNA VISTA*/
23 • DROP VIEW nombre_Vista;
24 /*Ejemplo*/
25 • DROP VIEW Vista_Productos;
26
```

### **CIFRADO:**



```
Privilegios - Gestión de Usuarios  Administración de Vistas  Cifrado Datos x
1  /*CIFRADO DE DATOS USANDO AES_ENCRYPT*/
2  • INSERT INTO nombreTabla VALUES(AES_ENCRYPT('valor_a_Encriptar', 'clave'));
3  /*Ejemplo*/
4  • INSERT INTO ClientesVIP VALUES(AES_ENCRYPT('Cliente001', 'cf01'));
5  /*En este caso al hacer un select , el SGBD nos devolvería los datos pero en forma encriptada*/
6
7  /*Para desencriptar se utiliza "AES_DECRYPT"*/
8  • SELECT AES_DECRYPT(Columa_Encriptada, 'clave') FROM nombreTabla;
9  /*Ejemplo*/
10 • SELECT AES_DECRYPT(Cliente001, 'clave') FROM ClientesVIP;
11
```