Guía de ABP 3: Auditoría de la base de datos

Evaluación Sumativa 3

1. **Presentación**

De acuerdo con lo analizado y conversado en clases, utiliza tus habilidades para resolver el siguiente problema. Tendrás que hacer uso de lo practicado en cuanto a instalación y configuración del ambiente Oracle y demostrar tus conocimientos en cómo se maneja la memoria del mismo.

* Criterios de evaluación

Las actividades consideran los siguientes criterios de evaluación:

3.1.1.- Gestionando disparadores (Triggers) de acuerdo a requerimientos.

3.1.2.- Usando disparadores para auditar accesos a la base de datos.

3.1.3.- Utilizando auditoría estándar y FGA.

3.1.4.- Decidiendo el tipo de auditoría a aplicar.

3.1.5.- Desarrollando sus ideas en torno a un tema central de manera analítica y crítica.

1. **Instrucciones**

1. El trabajo debe realizarse de forma individual.

2. Constará de dos partes, práctica y teórica.

3. Debes utilizar Enterprise Manager y SQLPlus para los ejercicios.

4. En algunos ejercicios será necesario sacar un print de pantalla, como prueba del trabajo que vas realizando, que irás guardando en distintos archivos JPG. Debes darle el formato 01\_XXXXX, donde el número corresponderá al número del ejercicio y XXXXX es un nombre que describe a qué ejercicio corresponde.

5. Para todas las acciones que realices en Entreprise Manager (como crear un usuario), debes utilizar el botón “Mostrar SQL” para obtener la query producida.

6. Crea un archivo word, donde vayas indicando con el número del ejercicio la query correspondiente como solución.

7. En caso de adjuntar imágenes, hazlo sobre el mismo Word, teniendo cuidado de dejarlo en la numeración del ejercicio correcta.

**Unidad de Aprendizaje 3:** Auditoría de la base de datos

**Aprendizaje esperado**

3.1.- Resuelve problemas de control de accesos en la base de datos de acuerdo a requerimientos. (Integrada Competencia Genérica Comunicación Oral y Escrita)

**Pablo Edorta Abaroa Schilling**

**Sección 15**

**Actividades**

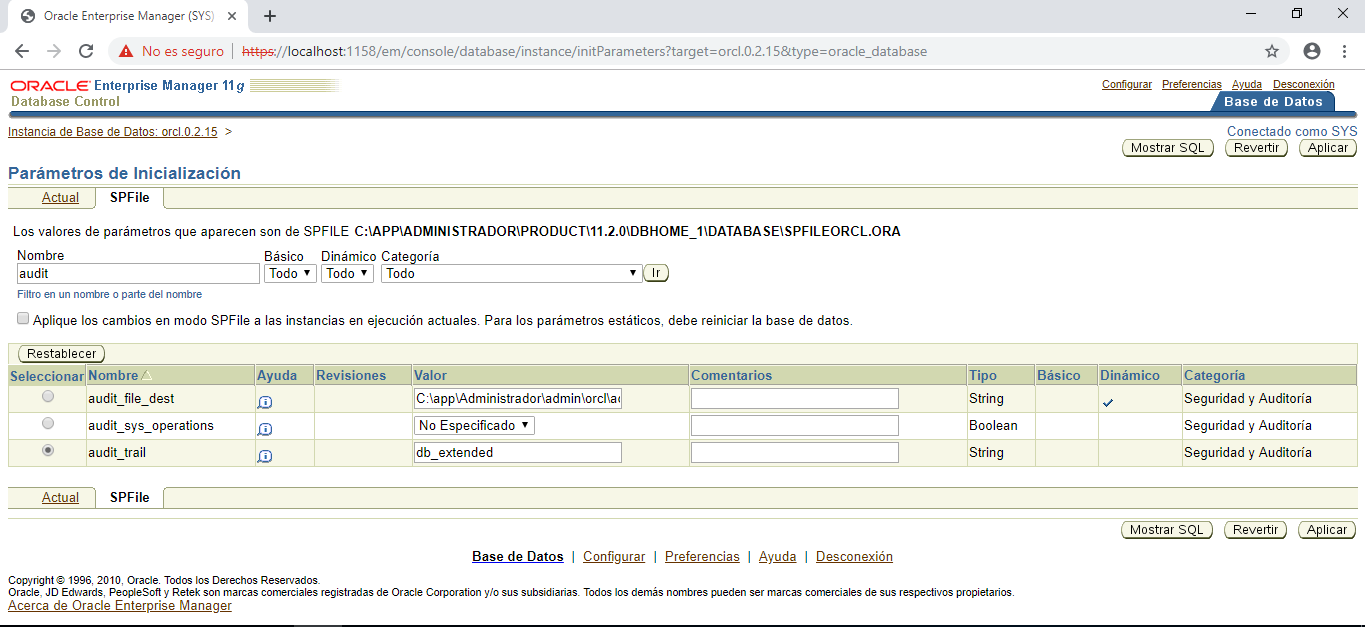
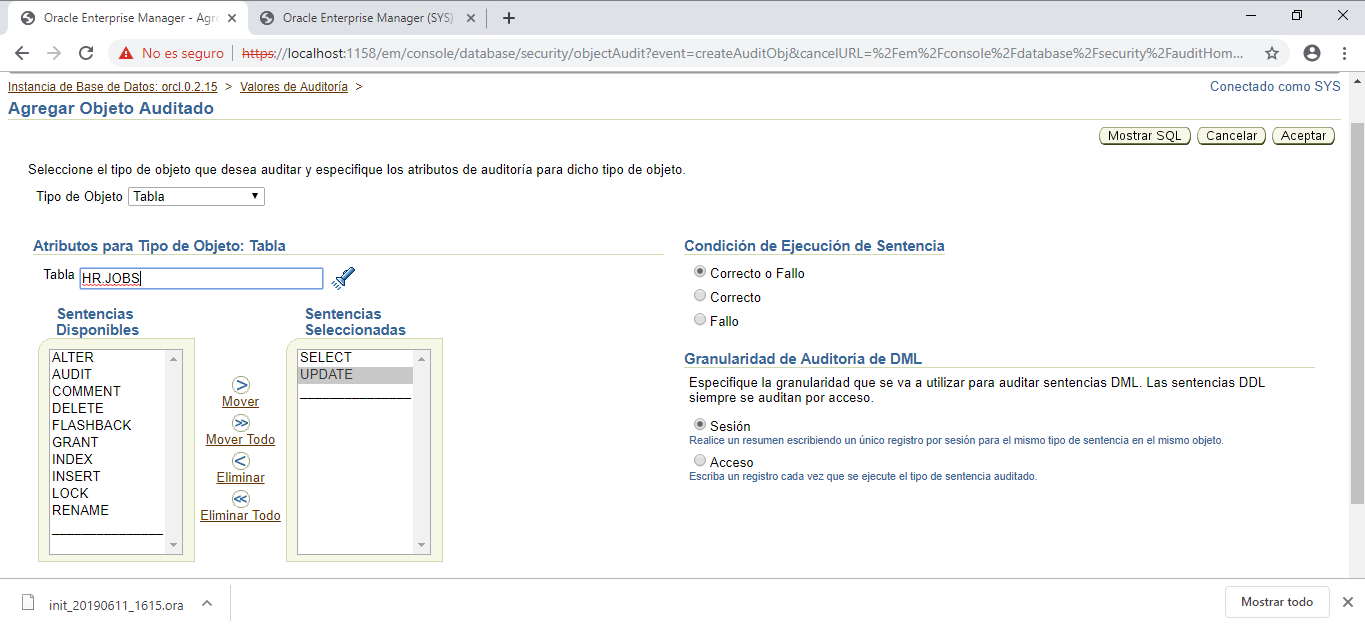
1. Creación de auditoría estándar.
2. Manejo de auditoría basada en valores y detallada (FGA).

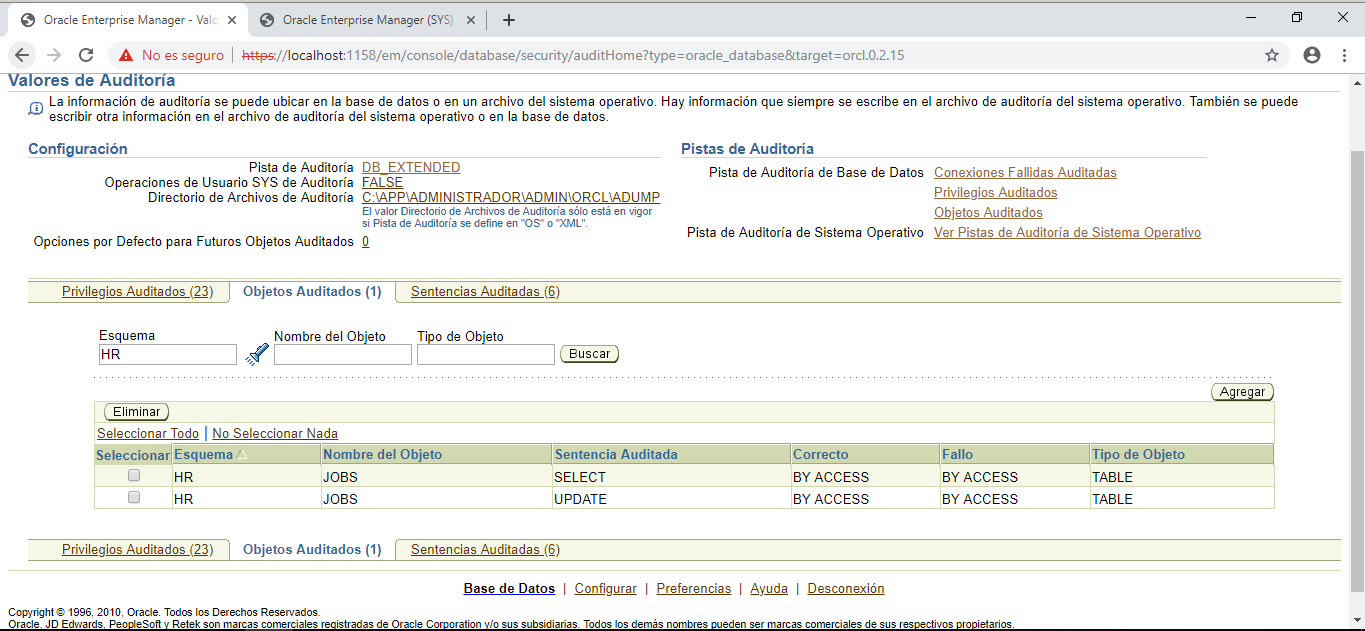
**Evaluación**

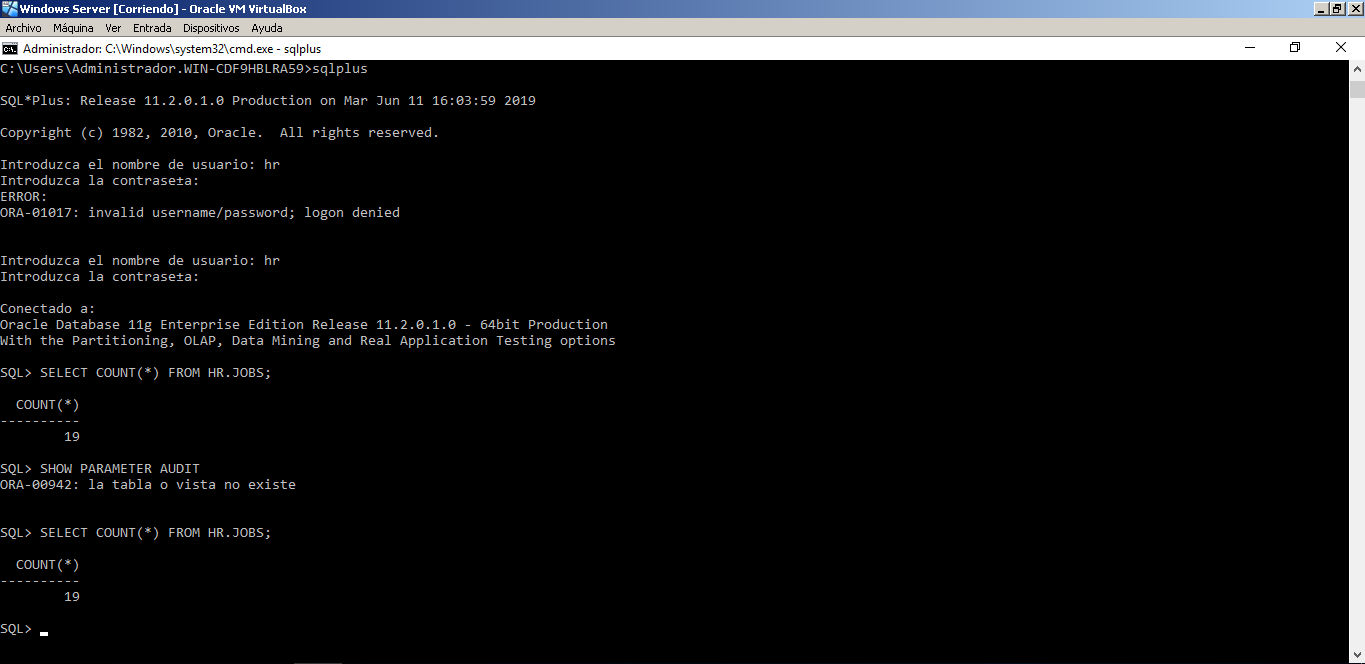
* Evaluación sumativa con Escala de apreciación.
* Ponderación 20%

1. **Actividades**
2. Se plantea el siguiente problema:

Se requiere comprobar la correcta configuración de auditoría de una empresa, por lo que se pide lo siguiente:

* 1. Mostrar dónde se configura pista de auditoría AUDIT\_TRAIL valor DB\_EXTENDED **(print pantalla).**
  2. Otorgar permisos de auditoría estándar sobre la tabla JOBS de HR, cuando haya sentencias select y update **(print pantalla).**

* 1. Provocar que esa auditoría se genere con el usuario HR desde SQLPLus. Muestra el resultado **(print pantalla).**



* 1. Crear una tabla en el esquema SYSTEM, donde se irán guardando los valores: username, ip, dato\_antiguo, dato\_nuevo, fecha\_accion, texto. Usar sys\_context para obtener los 2 primeros valores. Texto hace referencia a un texto personalizado que va a indicar el cambio ocurrido. **(SQL script)**

CREATE TABLE "SYSTEM"."AUDIT\_SYSTEM" ( "USERNAME" VARCHAR2(30), "IP" VARCHAR2(40), "DATO\_ANTIGUO" VARCHAR2(45), "DATO\_NUEVO" VARCHAR2(45), "FECHA\_ACCION" DATE, "TEXTO" VARCHAR2(120))

* 1. Crear un trigger que se accione al hacer update en la tabla JOBS, siempre y cuando se haya aumentado el salario mínimo. **(SQL script)**

CREATE OR REPLACE TRIGGER "SYSTEM"."SALARY\_TRIGGER" AFTER

UPDATE OF "MIN\_SALARY" ON "HR"."JOBS" FOR EACH ROW BEGIN

IF :old.min\_salary < :new.min\_salary THEN

INSERT INTO system.audit\_system

VALUES (sys\_context('userenv','os\_user'), sys\_context('userenv','ip\_address'),old.min\_salary,new.min\_salary,sysdate,

:new.employee\_id ||'job min\_salary changed from '||:old.min\_salary||' to '||:new.min\_salary);

END IF;

END;

* 1. Crear un trigger que se accione siempre que se elimine un país (dejar en null dato\_antiguo y dato\_nuevo). **(SQL script)**

CREATE OR REPLACE TRIGGER "SYSTEM"."PAIS\_TRIGGER" AFTER

DELETE ON "HR"."COUNTRIES" FOR EACH ROW BEGIN

IF :old.COUNTRY\_ID = :new.COUNTRY\_ID THEN

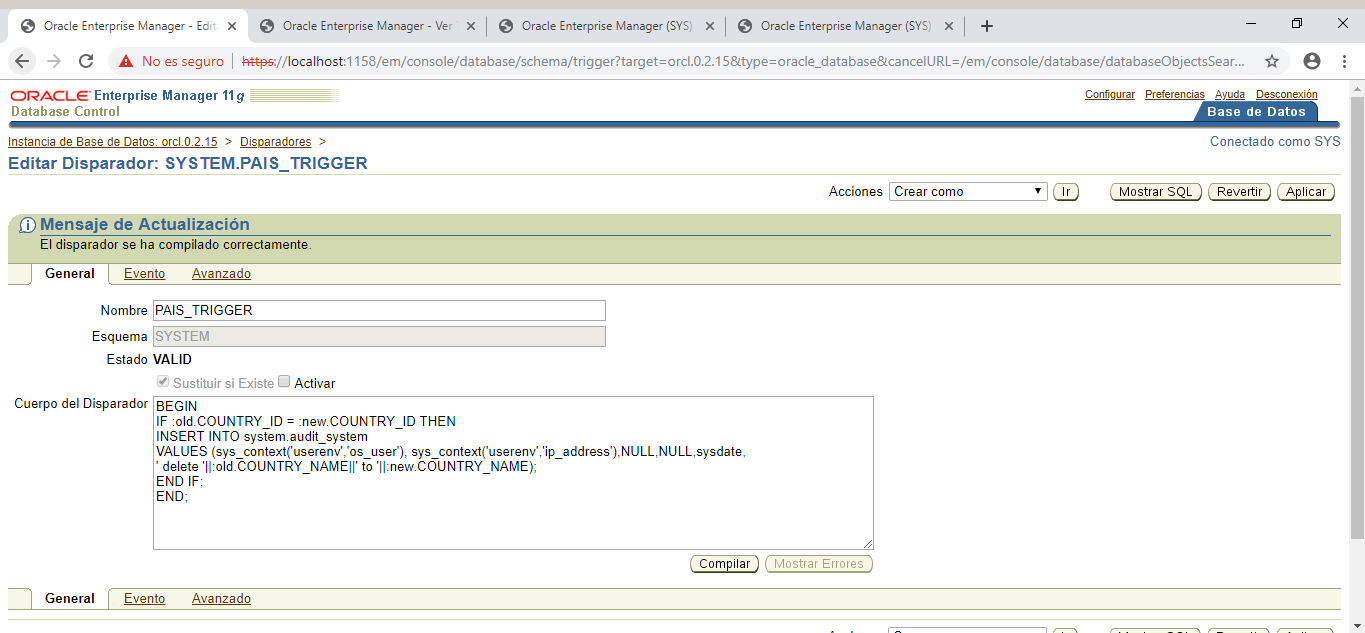
INSERT INTO system.audit\_system

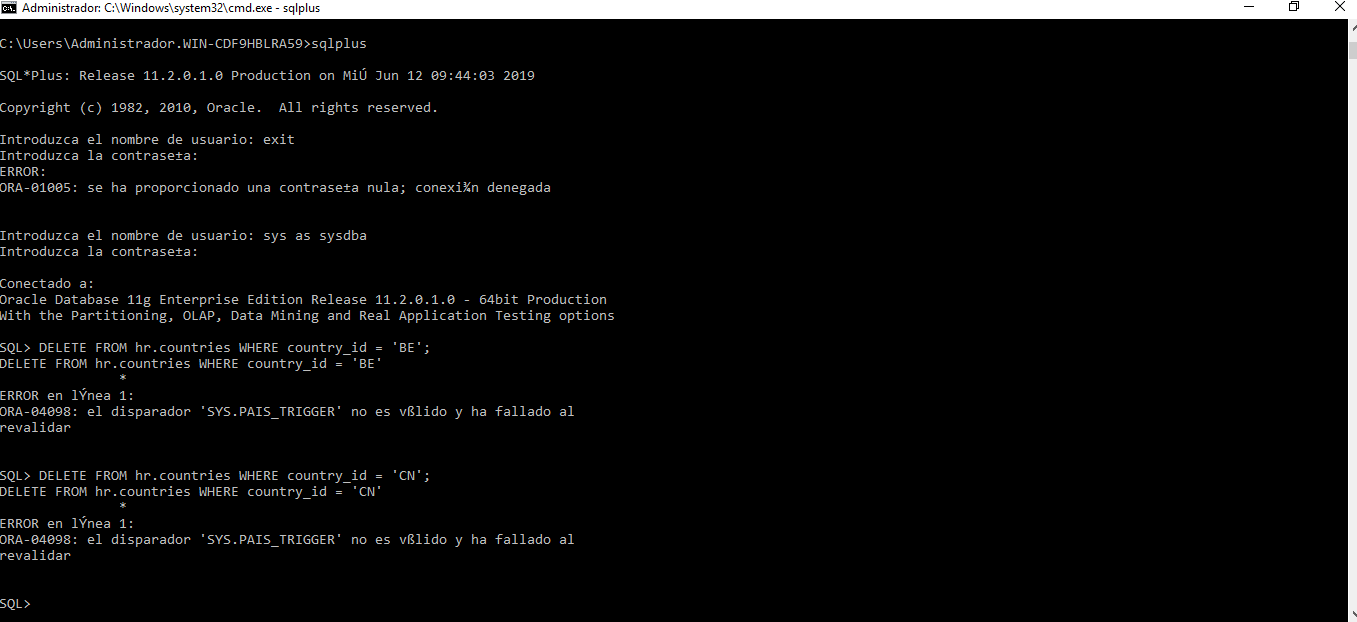
VALUES (sys\_context('userenv','os\_user'), sys\_context('userenv','ip\_address'),NULL,NULL,sysdate,

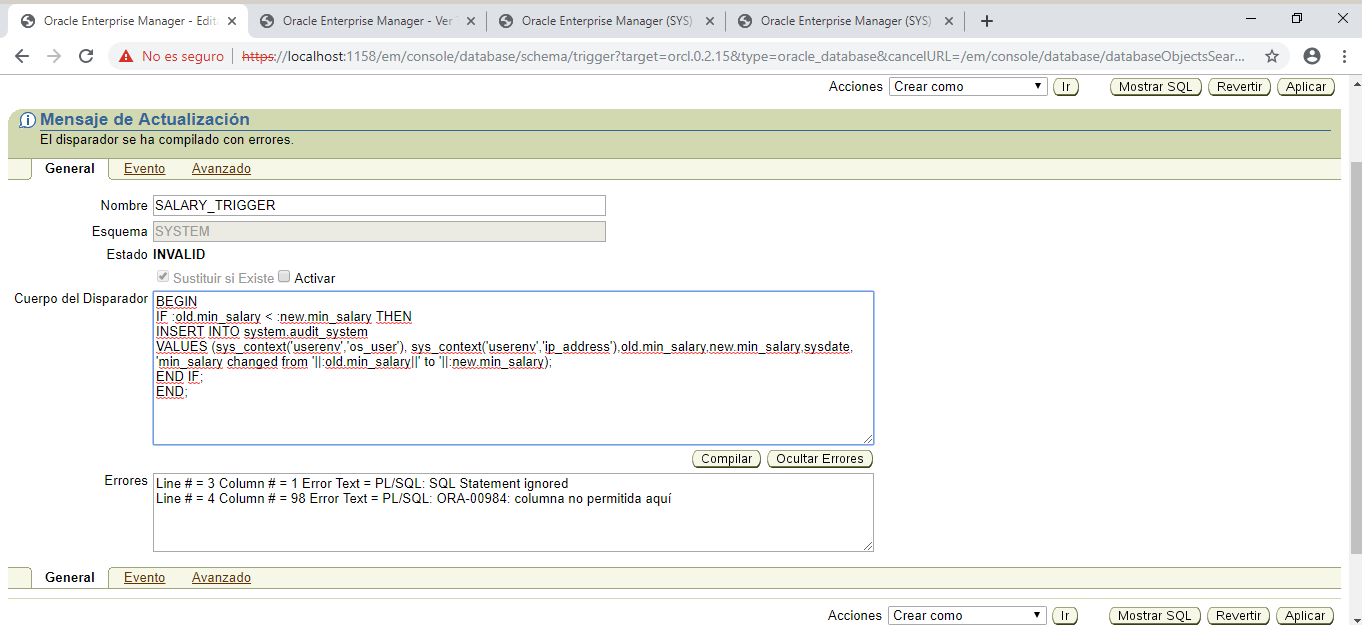
' delete '||:old.COUNTRY\_NAME||' to '||:new.COUNTRY\_NAME);

END IF;

END;

* 1. Mostrar que se hayan generado registros por el primer trigger **(print pantalla)**



* 1. ****Mostrar que se hayan generado registros por el segundo trigger **(print pantalla).**

1. Demuestra que manejas los siguientes conceptos:
   1. ¿Qué tipos de auditoría tiene Oracle? Mencione 3.

Auditoria basada en valores

Auditoria Detallada (FGA)

Auditoria Estándar

* 1. ¿Cómo se debe configurar la pista de auditoría para capturar el texto SQL exacto que se ejecutó?

Se debe agregar una política con el formato de Auditoria Detallada, ósea DBMS\_FGA.ADD\_POLICY, seleccionar el esquema y objeto, darle un nombre a la política, seleccionar las columnas que se quieren capturar, habilitar o deshabilitar la política y sus condiciones (select, update,delete,etc).

* 1. ¿Por qué debe hacerse mantenimiento a las auditorías activas?

Las listas de las pistas de auditoria se pueden incrementar rápidamente lo cual afectara al rendimiento de la base de datos ralentizándola, lo cuas de deben configurar adecuadamente las auditorias para que este problema no ocurra.

* 1. ¿En qué se diferencian la auditoria basada en valores de la detallada (FGA)?

La auditoria basada en valores captura los datos que se quisieron cambiar o insertar como unSELECT,UPDATE, DELETE,etc.

La auditoria detallada (FGA) captura el SQL exacto del dato que se quiso operar y además la pista auditada

* 1. Observe la siguiente auditoría FGA y conteste según corresponda:

dbms\_fga.add\_policy (

object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'audit\_emps\_salary',

audit\_condition=> 'department\_id=10',

audit\_column => 'SALARY,COMMISSION\_PCT',

handler\_schema => 'secure',

handler\_module => 'log\_emps\_salary',

enable => TRUE,

statement\_types => 'SELECT,UPDATE');

Escribir 2 scripts, uno que toque la tabla de la política creada, pero que no audite; y otro script donde sí audite.

1.

dbms\_fga.add\_policy (

object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'audit\_emps\_salary',

audit\_condition=> 'department\_id=10',

audit\_column => 'SALARY,COMMISSION\_PCT',

handler\_schema => 'secure',

handler\_module => 'log\_emps\_salary',

enable => FALSE,

statement\_types => 'SELECT,UPDATE');

2.

dbms\_fga.add\_policy (

object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => 'audit\_emps\_salary',

audit\_condition=> 'department\_id=10',

audit\_column => 'SALARY,COMMISSION\_PCT',

handler\_schema => 'secure',

handler\_module => 'log\_emps\_salary',

enable => TRUE,

statement\_types => 'SELECT,UPDATE');

* 1. En base al ejercicio anterior, generar una auditoría FGA llamada AUDIT\_CLIENTE, que audite la columna SALARY de la tabla EMPLOYEES, cuando a ésta se le haga una consulta o modificación.

dbms\_fga.add\_policy (

object\_schema => 'HR',

object\_name => 'EMPLOYEES',

policy\_name => ' AUDIT\_CLIENTE ',

audit\_condition=> 'department\_id=10',

audit\_column => 'SALARY',

handler\_schema => 'secure',

handler\_module => 'log\_emps\_salary',

enable => TRUE,

statement\_types => 'SELECT,UPDATE');