



Administración de bases de datos

D07

M-J 7-9 AM



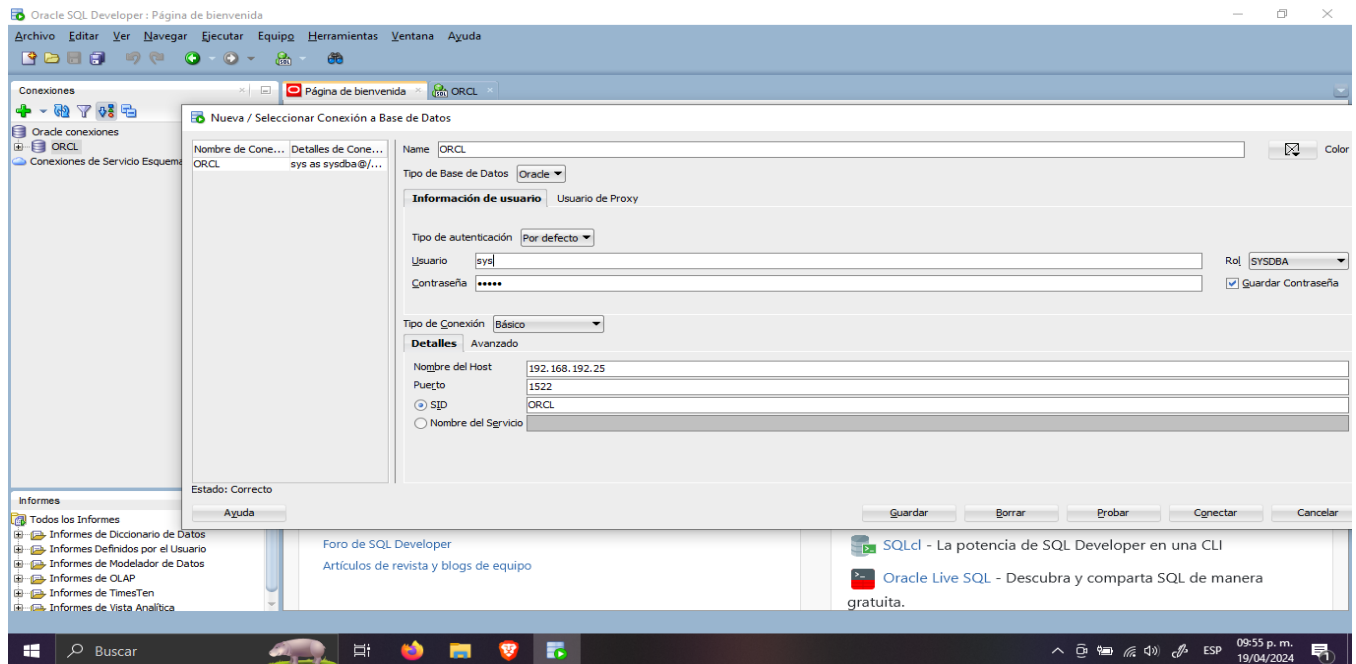
## **Práctica 13: Auditoría en Oracle**

Centro Universitario de Ciencias Exactas e Ingenierías

Universidad de Guadalajara

2024<sup>a</sup>

Dentro de SQL DEVELOPER nos vamos para crear una nueva conexión, pero exclusivamente se hace la conexión con el usuario tipo SYSDBA y las siguientes especificaciones de los parámetros.



## - Login - logout de un usuario específico

Para empezar, se hace un login y logout del usuario mortal\_baruj

```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.4291]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\baruj>sqlplus

SQL*Plus: Release 11.2.0.1.0 Production on S8b Abr 20 10:20:52 2024

Copyright (c) 1982, 2010, Oracle. All rights reserved.

Enter user-name: mortal_baruj
Enter password:

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production

SQL> exit
Disconnected from Oracle Database 11g Release 11.2.0.1.0 - 64bit Production

C:\Users\baruj>
```

Se aplican los siguientes comandos para realizar la auditoría.

ALTER SYSTEM SET AUDIT\_TRAIL=DB, EXTENDED SCOPE=SPFILE

AUDIT SESSION;

AUDIT SESSION BY MORTAL\_BARUJ BY ACCESS;

SELECT \* FROM DBA\_AUDIT\_TRAIL WHERE USERNAME = 'MORTAL\_BARUJ';

Configura donde se almacena la auditoría y se especifica donde se guarda

Activa la auditoría de sesiones

Se configura la auditoría de sesiones específica del usuario MORTAL\_BARUJ

Muestra los registros de auditoría relacionados a MORTAL\_BARUJ

Esos fueron las funciones respectivamente

The screenshot displays the Oracle SQL Developer interface. The 'Hoja de Trabajo' (Worksheet) pane contains the following SQL commands:

```
ALTER SYSTEM SET AUDIT_TRAIL=DB, EXTENDED SCOPE=SPFILE;  
AUDIT SESSION;  
AUDIT SESSION BY MORTAL_BARUJ BY ACCESS;  
SELECT * FROM DBA_AUDIT_TRAIL WHERE USERNAME = 'MORTAL_BARUJ';
```

The 'Resultado de la Consulta' (Query Result) pane shows the output of the last command, displaying 62 rows of audit trail data for the user MORTAL\_BARUJ. The data is filtered by timestamp, showing the most recent entries. The columns displayed are:

OS_USERNAME	USERNAME	USERHOST	TERMINAL	TIMESTAMP	OWNER	OBJ_NAME	ACTION	ACTION_NAME	NEW_C
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	29/02/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	12/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	12/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	18/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	18/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	18/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	18/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)
DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	101 LOGOFF	(null)	(null)

Esta imagen es después de aplicar un filtro que me muestra los timestamp más recientes.

Oracle SQL Developer: ORCL

Archivo Editar Ver Navegar Ejecutar Origen Equip Herramientas Ventana Ayuda

Conexiones

Oracle conexiones

ORCL

Tablas (Filtrado)

Vistas

Indices

Paquetes

Procedimientos

Funciones

Operadores

Colas

Tablas de Colas

Disparadores

Tipos

Secuencias

Vistas Materializadas

Log de Vistas Materializadas

Sinónimos

Informes

Todos los Informes

Informes de Diccionario de Datos

Informes Definidos por el Usuario

Informes de Modelador de Datos

Informes de CLAP

Informes de TimesTen

Log de Vistas Materializadas

Informes de Vista Analítica

Hoja de Trabajo

Generador de Consultas

SELECT \* FROM DBA\_AUDIT\_TRAIL WHERE USERNAME = 'MORTAL\_BARUJ';

Resultado de la Consulta

SQL Se han recuperado 50 filas en 0.024 segundos

OS_USERNAME	USERNAME	USERHOST	TERMINAL	TIMEST...	OWNER	OBJ_NAME	ACTION	ACTION_NAME	NEW_C
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	20/04/24	(null)	(null)	101	LOGOFF	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	20/04/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	10/04/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	09/04/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	09/04/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	101	LOGOFF	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	101	LOGOFF	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	23/03/24	(null)	(null)	100	LOGON	(null)
SYSTEM	MORTAL_BARUJ	LAPTOP-FLB8VUDQ	LAPTOP-FLB8VUDQ	19/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	100	LOGON	(null)
DESKTOP-GP8VF8B\baru	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	19/03/24	(null)	(null)	100	LOGON	(null)

Línea 1 Columna 63 | Insertar | Modificado | Windows: C

10:25 a. m. 20/04/2024

## - Update de la tabla de empleados -- crear la tabla

Se crea una tabla con el usuario mortal\_baruj llamada empleados, y se insertan algunos datos.

Simbolo del sistema - sqlplus

```
SQL> SELECT * FROM system.empleados;
SELECT * FROM system.empleados
*
ERROR at line 1:
ORA-01031: privilegios insuficientes

SQL> CREATE TABLE empleados(
  2   empleado_id number,
  3   nombre varchar2(20)
  4 );

Table created.

SQL>
SQL> INSERT INTO empleados (empleado_id, nombre) VALUES (1, 'Juan');

1 row created.

SQL> INSERT INTO empleados (empleado_id, nombre) VALUES (2, 'Meria');

1 row created.

SQL> INSERT INTO empleados (empleado_id, nombre) VALUES (3, 'Carlos');

1 row created.

SQL>
SQL>
SQL> commit;

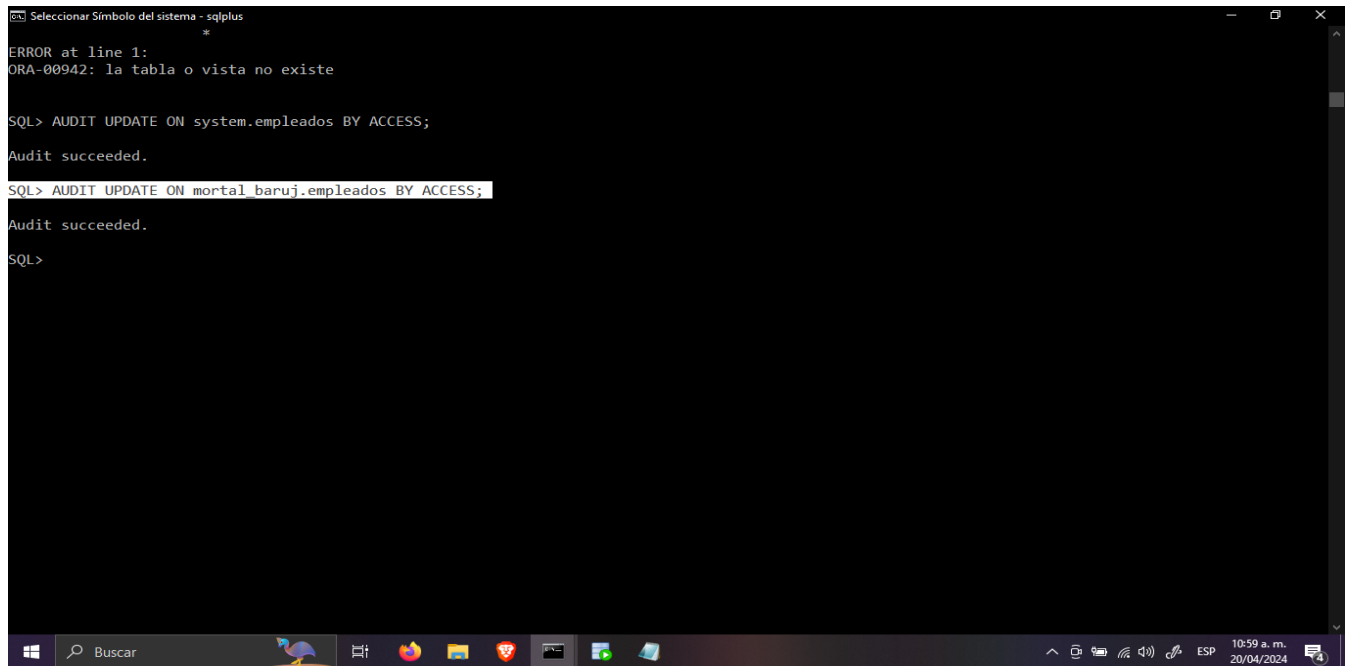
Commit complete.

SQL>
SQL> UPDATE empleados SET nombre='Maria' WHERE empleado_id=2;
```

10:59 a. m. 20/04/2024

Se escribe el comando `AUDIT UPDATE ON mortal_baruj.empleados BY ACCESS;`

Para rastrear la auditoría realizadas por el usuario mortal\_baruj centradas únicamente en las modificaciones realizadas en la tabla empleados.



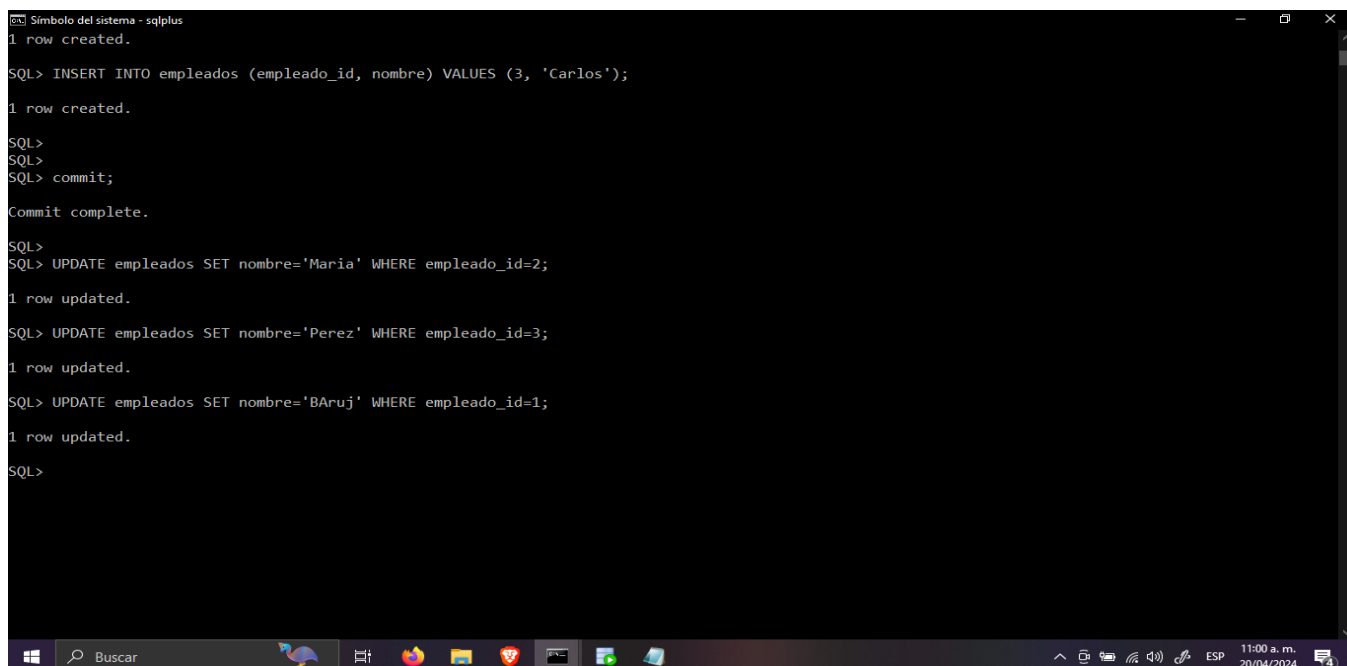
```
Selecciónar Símbolo del sistema - sqlplus
*
ERROR at line 1:
ORA-00942: la tabla o vista no existe

SQL> AUDIT UPDATE ON system.empleados BY ACCESS;
Audit succeeded.

SQL> AUDIT UPDATE ON mortal_baruj.empleados BY ACCESS;
Audit succeeded.

SQL>
```

Con el usuario mortal\_baruj, lo que haremos serán varios UPDATES a la tabla de empleados



```
Símbolo del sistema - sqlplus
1 row created.

SQL> INSERT INTO empleados (empleado_id, nombre) VALUES (3, 'Carlos');
1 row created.

SQL>
SQL>
SQL> commit;
Commit complete.

SQL>
SQL> UPDATE empleados SET nombre='Maria' WHERE empleado_id=2;
1 row updated.

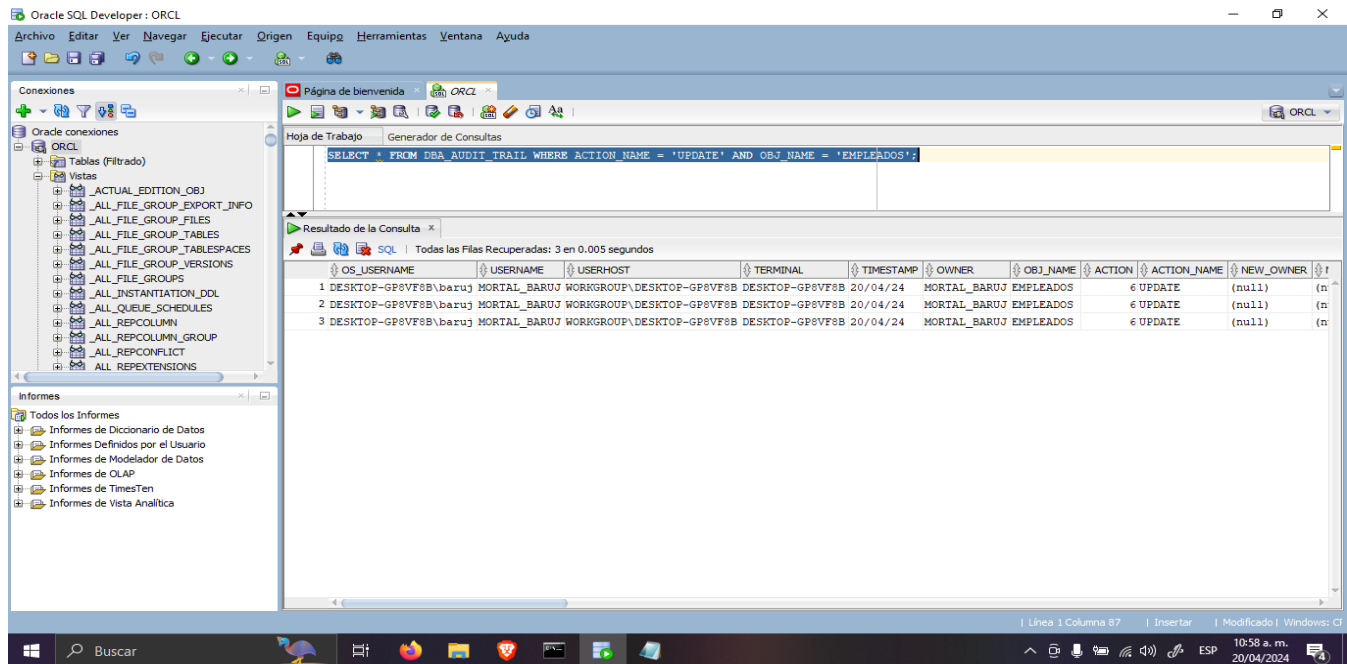
SQL> UPDATE empleados SET nombre='Perez' WHERE empleado_id=3;
1 row updated.

SQL> UPDATE empleados SET nombre='BARuj' WHERE empleado_id=1;
1 row updated.

SQL>
```

Utilizando `SELECT * FROM DBA_AUDIT_TRAIL WHERE ACTION_NAME = 'UPDATE' AND OBJ_NAME = 'EMPLEADOS';`

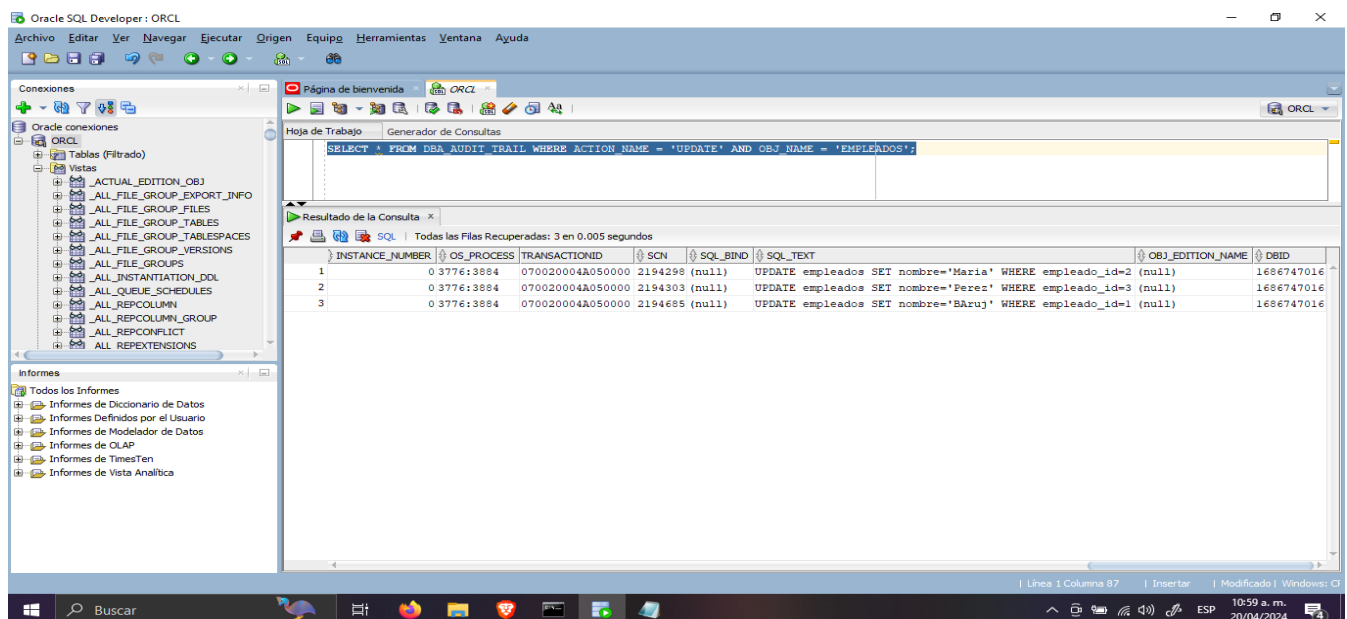
Esto para revisar la auditoría de los datos que involucran una acción UPDATE, nos muestra todos los datos como el OS\_USERNAME, el USERNAME que hizo la acción, la terminal, el timestamp, la acción, etc..



The screenshot shows the Oracle SQL Developer interface. The query `SELECT * FROM DBA_AUDIT_TRAIL WHERE ACTION_NAME = 'UPDATE' AND OBJ_NAME = 'EMPLEADOS';` is entered in the SQL editor. The results pane displays the following data:

	OS_USERNAME	USERNAME	USERHOST	TERMINAL	TIMESTAMP	OWNER	OBJ_NAME	ACTION	ACTION_NAME	NEW_OWNER
1	DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	20/04/24	MORTAL_BARUJ	EMPLEADOS	6 UPDATE	(null)	(n
2	DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	20/04/24	MORTAL_BARUJ	EMPLEADOS	6 UPDATE	(null)	(n
3	DESKTOP-GP8VF8B\baruj	MORTAL_BARUJ	WORKGROUP\DESKTOP-GP8VF8B	DESKTOP-GP8VF8B	20/04/24	MORTAL_BARUJ	EMPLEADOS	6 UPDATE	(null)	(n

Además, se muestran datos, como el texto que se vio involucrado al momento de hacer el UPDATE.



The screenshot shows the Oracle SQL Developer interface. The query `SELECT * FROM DBA_AUDIT_TRAIL WHERE ACTION_NAME = 'UPDATE' AND OBJ_NAME = 'EMPLEADOS';` is entered in the SQL editor. The results pane displays the following data:

	INSTANCE_NUMBER	OS_PROCESS	TRANSACTIONID	SCN	SQL_BIND	SQL_TEXT	OBJ_EDITION_NAME	DBID
1	0.3776:3884	070020004A050000	2194298 (null)			UPDATE empleados SET nombre='Maria' WHERE empleado_id=2 (null)		1686747016
2	0.3776:3884	070020004A050000	2194303 (null)			UPDATE empleados SET nombre='Perez' WHERE empleado_id=3 (null)		1686747016
3	0.3776:3884	070020004A050000	2194685 (null)			UPDATE empleados SET nombre='Baruj' WHERE empleado_id=1 (null)		1686747016