ORACLE

Cumplimiento Regulatorio: ¿Como la tecnología Oracle nos puede ayudar?

Miguel Palacios (miguel.palacios@gbsperu.net)

Dominio A11 Sistema de Control de Accesos

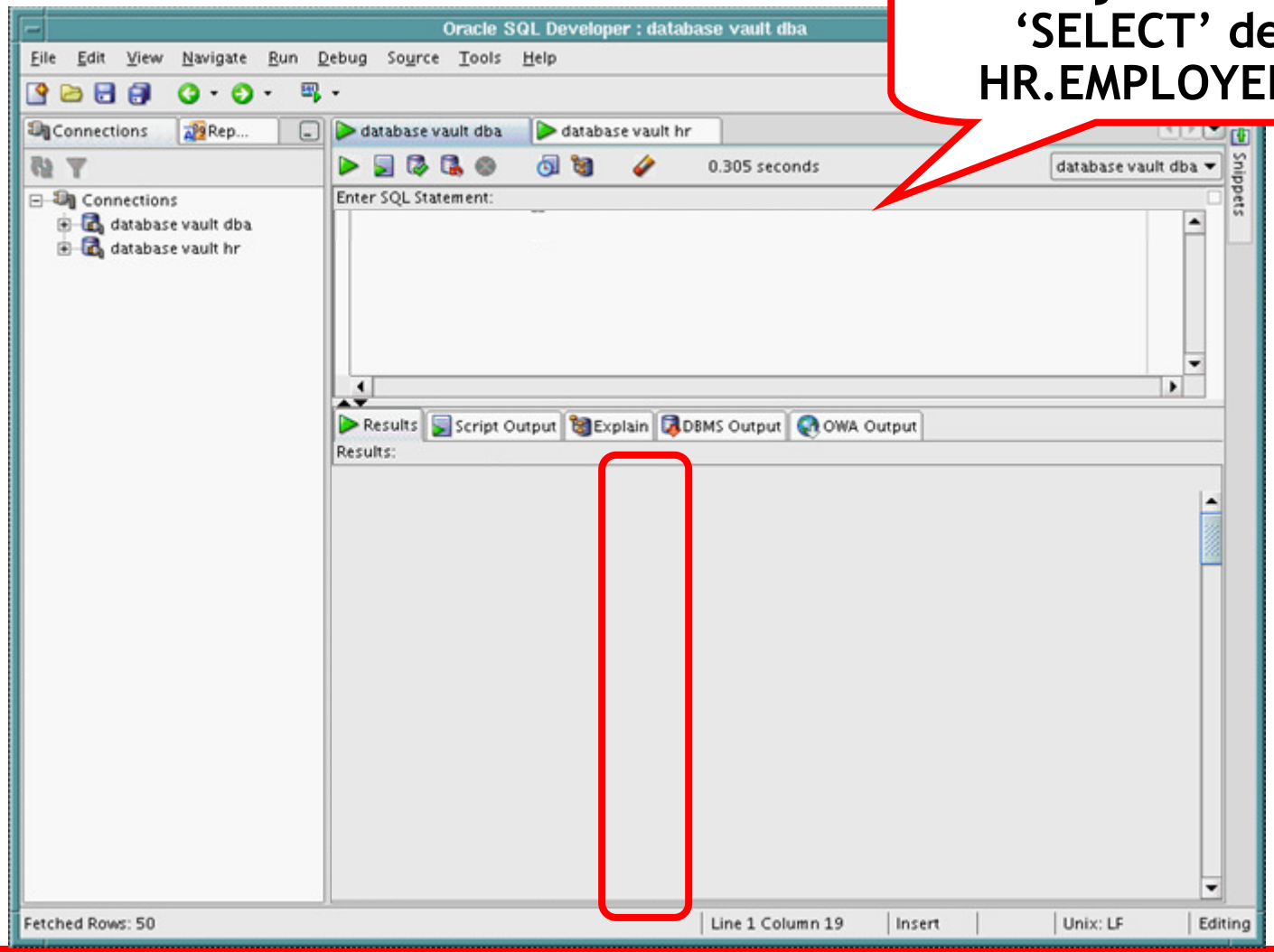
A 11.2.2 Gestión de privilegios

A 11.2.4 Revisión de los derechos de acceso de los usuarios

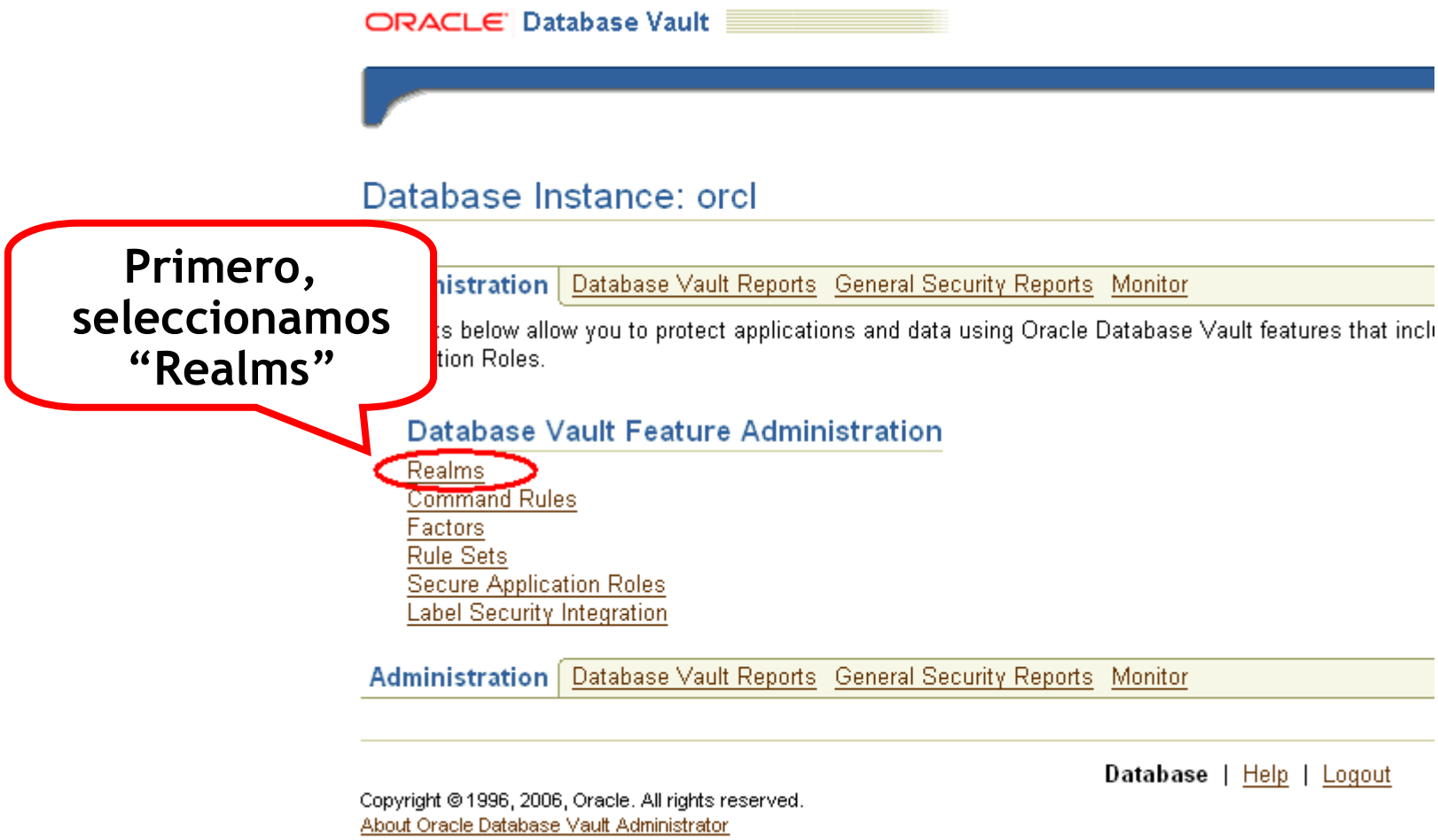
¿Como controlamos los accesos del personal de TI?

Situación concreta: Acceso del DBA a la(s) Bases de datos

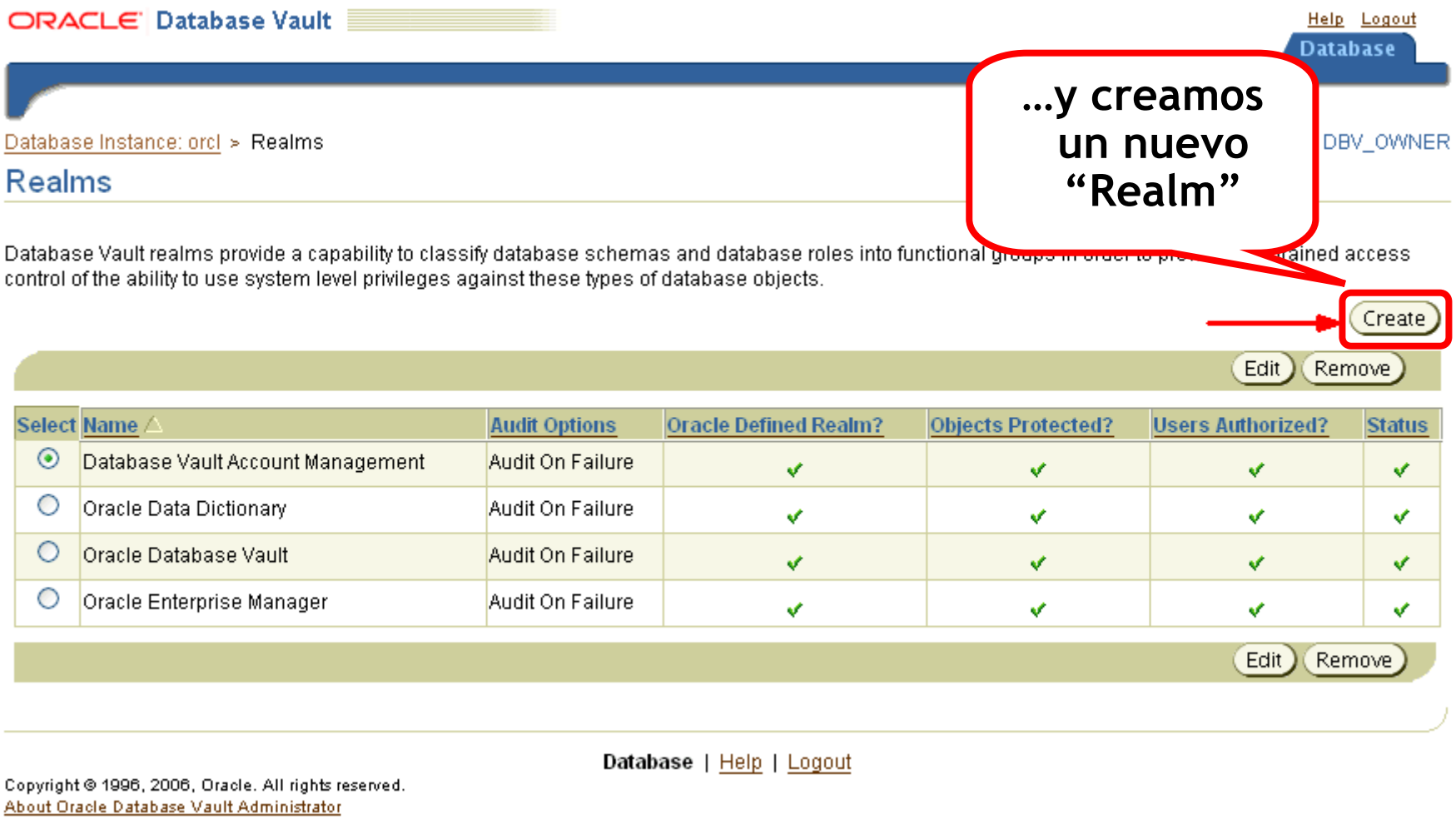
Database Vault - DBA quiere ver informacion sensible



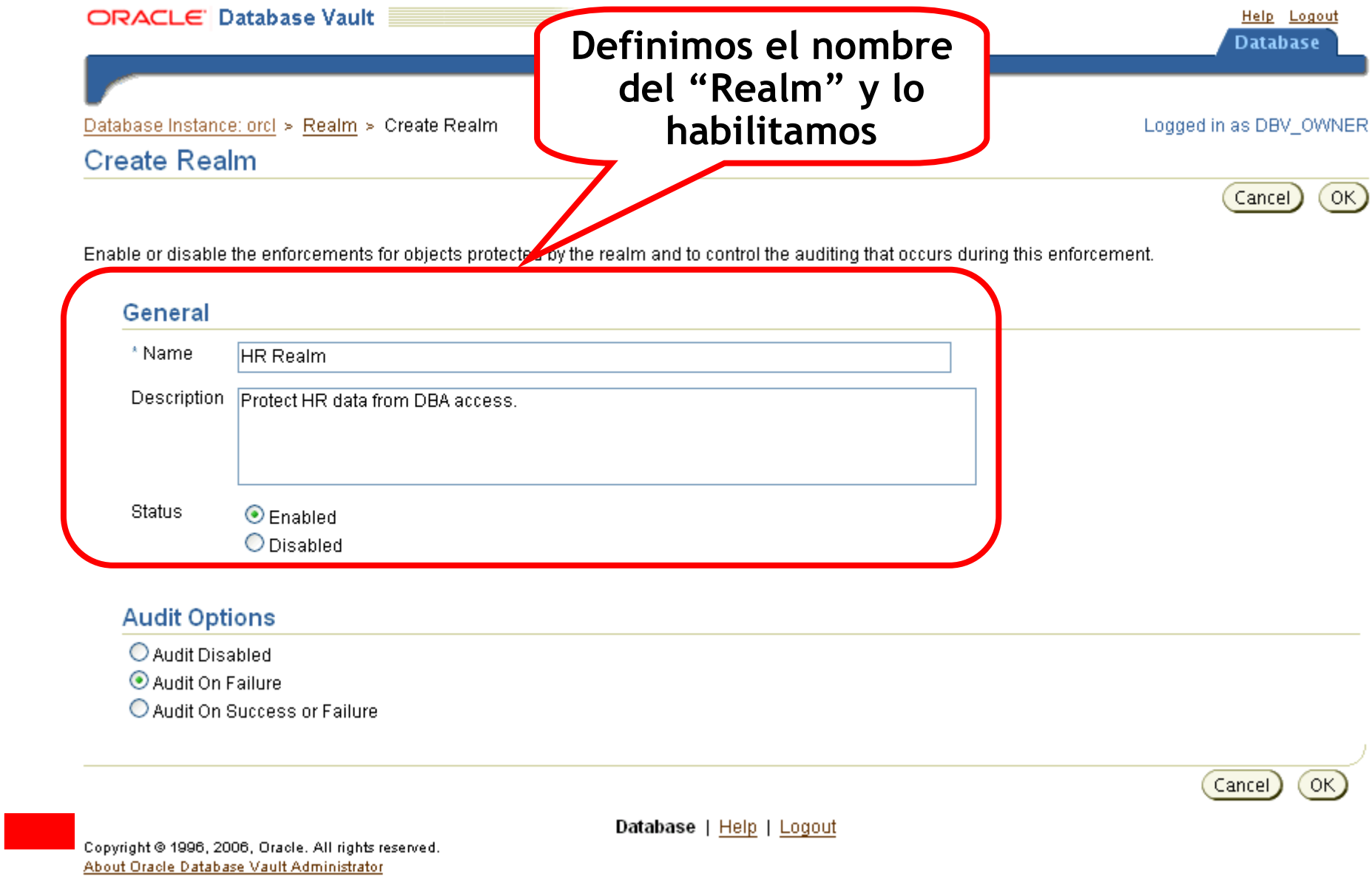
Definamos una regla para prevenir esto
Administración Web de Database Vault



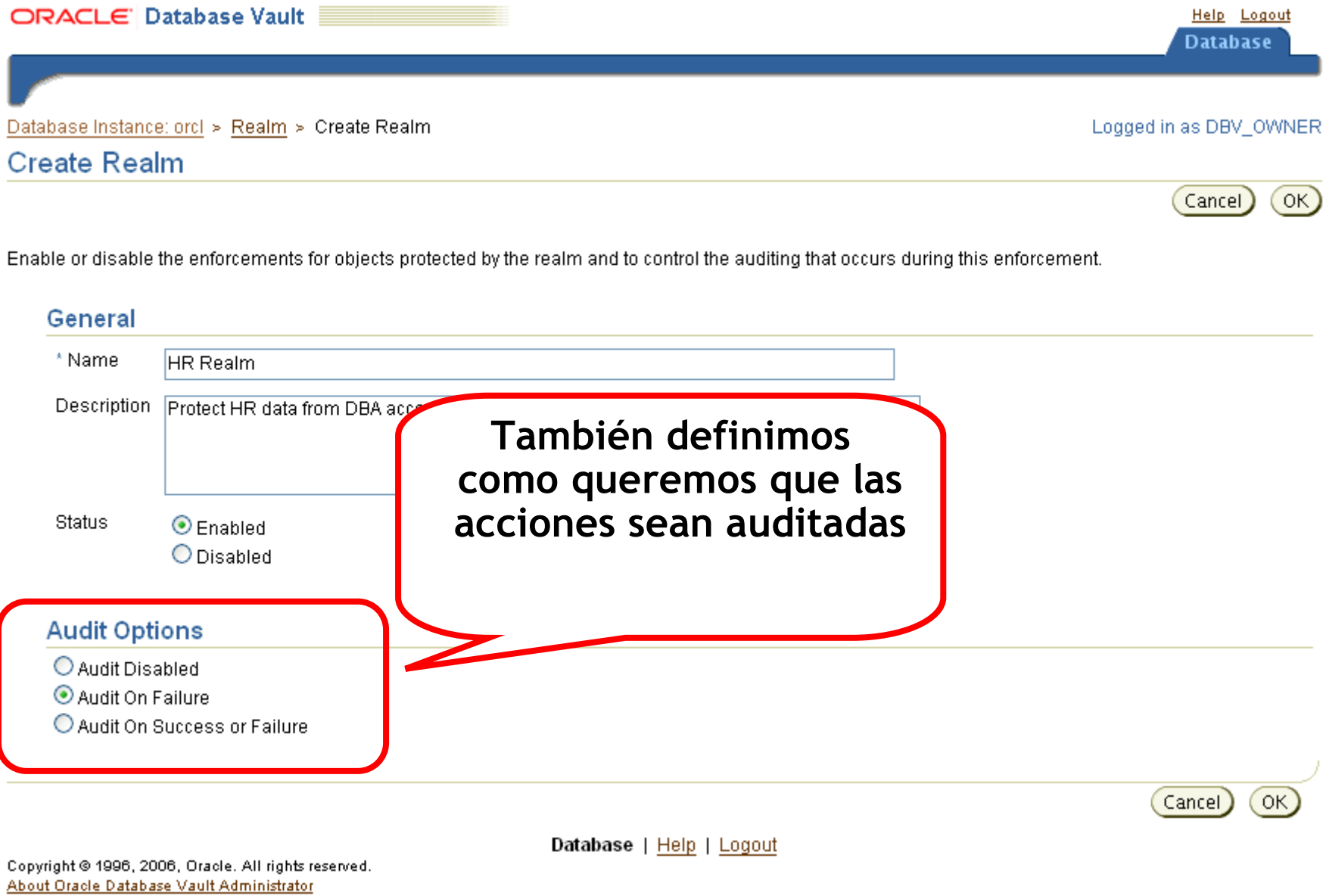
Database Vault - Gestión de “Realms”



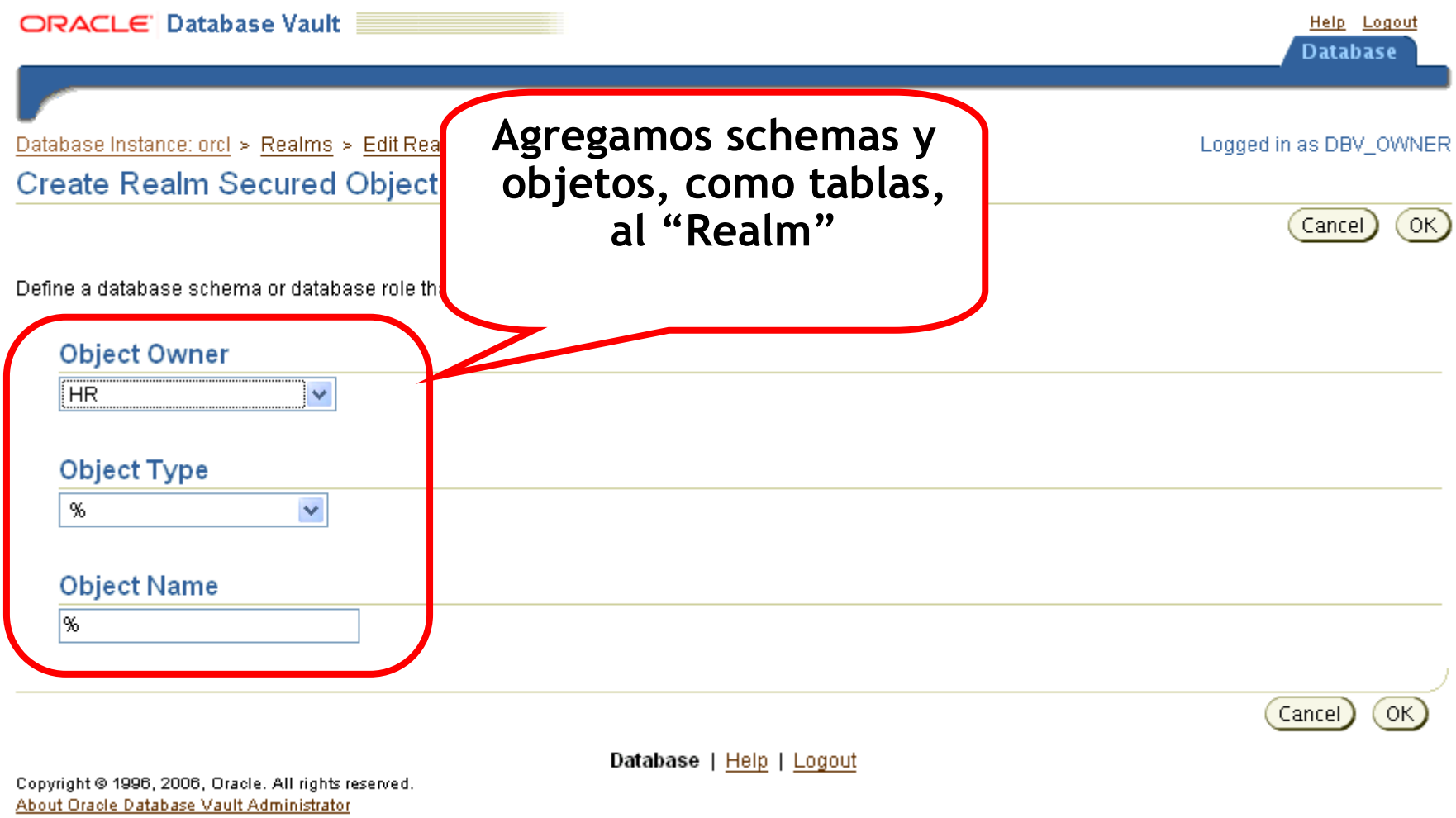
Database Vault - Creación de “Realm”



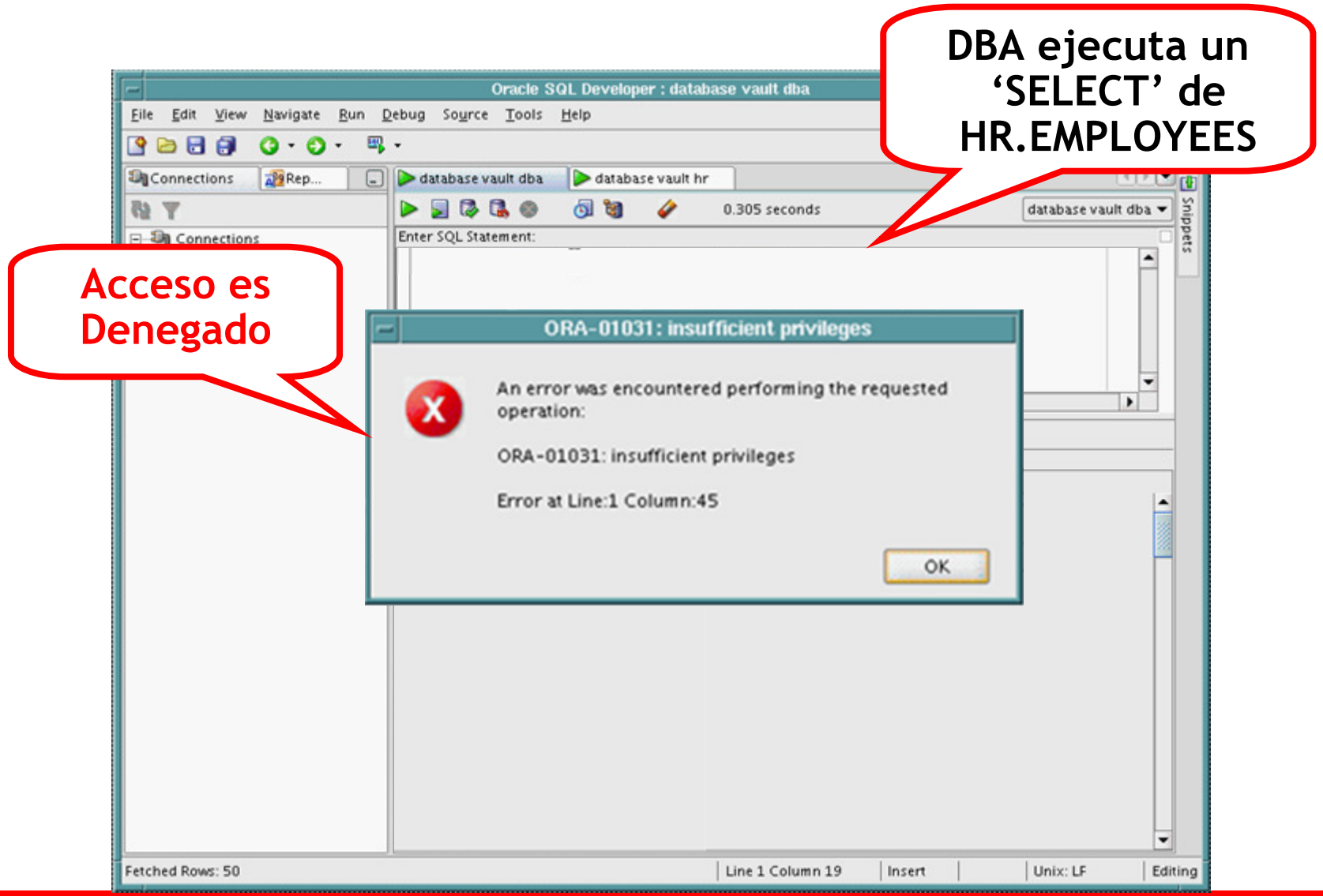
Database Vault - Creación de “Realm”



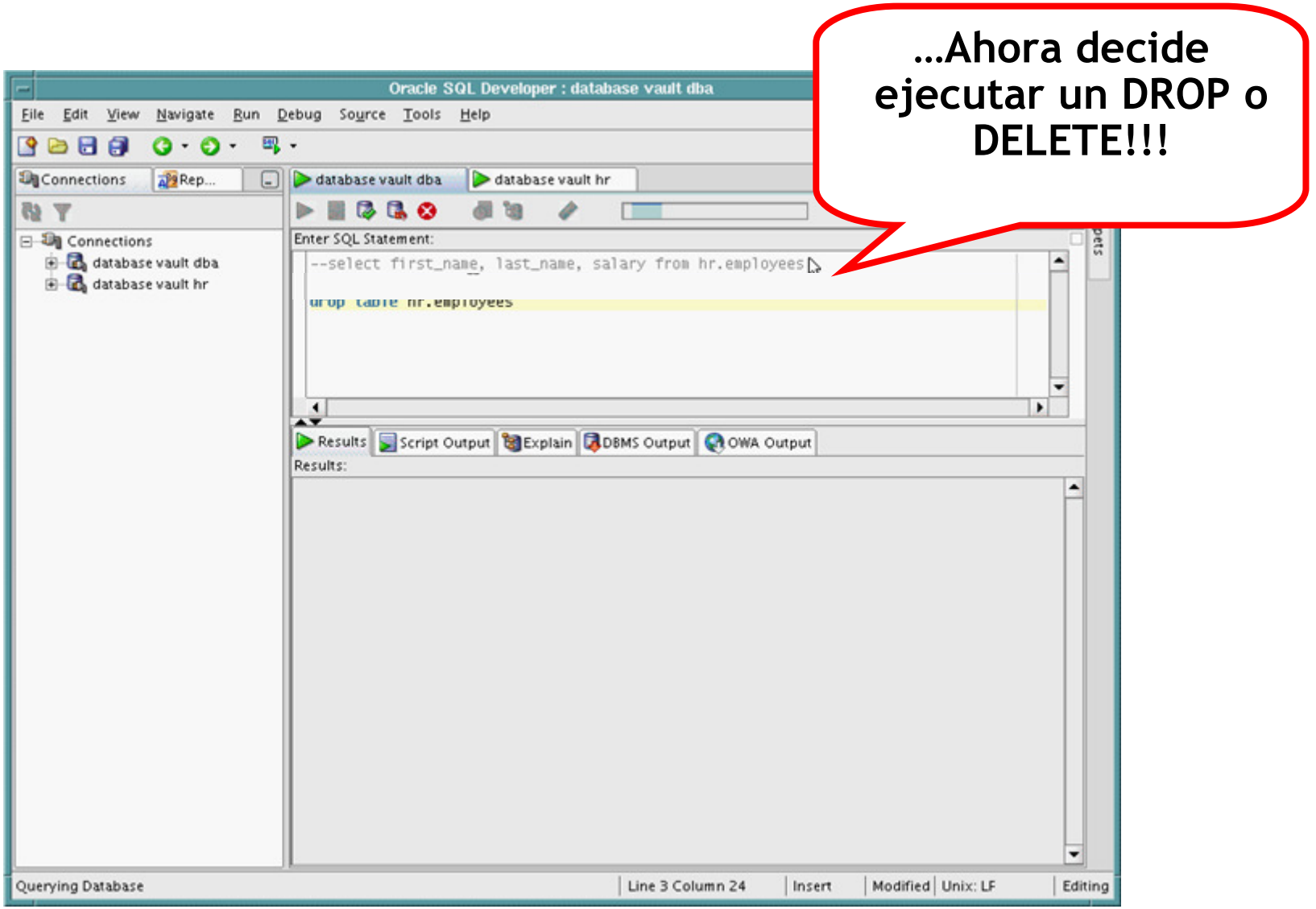
Database Vault - Aplicación de “Realm”



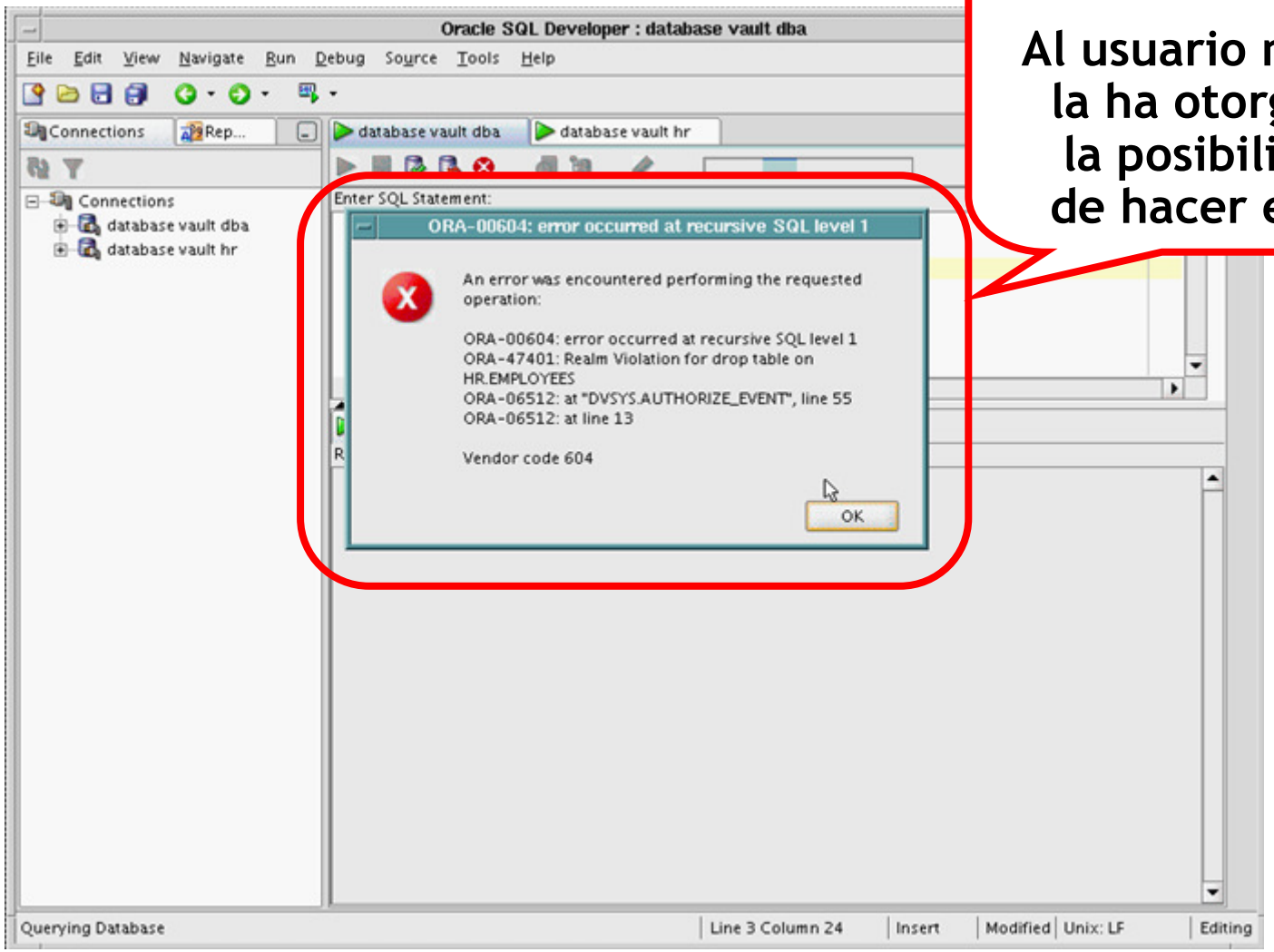
El DBA ejecuta el mismo SELECT



Protegiendo información de la tabla



Protegiendo información de la tabla



Access Denegado

Al usuario no se la ha otorgado la posibilidad de hacer eso…

Dominio A11 Sistema de Control de Accesos

A 11.2.2 Gestión de privilegios

A 11.2.4 Revisión de los derechos de acceso de los usuarios

¿Como controlo que las aplicaciones no accedan en forma indebida a las base de datos?

Situación concreta: SQL Injection

Uso de Bind Variables - Código Inyectable

```
SQL>
  1  create or replace procedure demo01 (nombreUsuario varchar2) as
  2  stmt varchar2(200);
  3  begin
  4  stmt:='SELECT id FROM t1 WHERE nombre = ''' || nombreUsuario || '''';
  5  execute immediate stmt;
  6  dbms_output.PUT_LINE('SQL statement: ' || stmt);
  7  end;

SQL> exec demo01('aaa');
SQL statement: SELECT id FROM t1 WHERE nombre = 'aaa'

SQL> SELECT id FROM t1 WHERE nombre = 'aaa';

        ID
----------
       100
```

Uso de Bind Variables - Código Inyectable

```
SQL>
  1  create or replace procedure demo01 (nombreUsuario varchar2) as
  2  stmt varchar2(200);
  3  begin
  4  stmt:='SELECT id FROM t1 WHERE nombre = ''' || nombreUsuario || '''';
  5  execute immediate stmt;
  6  dbms_output.PUT_LINE('SQL statement: ' || stmt);
  7  end;

SQL> exec demo01('x'' OR ''1''=''1');
SQL statement: SELECT id FROM t1 WHERE nombre = 'x' OR '1'='1'

SQL> SELECT id FROM t1 WHERE nombre = 'x' OR '1'='1';

        ID
----------
       100
       101
       102
```

Uso de Bind Variables - Codigo No Inyectable

```
SQL>
  1  create or replace procedure demo01 (nombreUsuario in varchar2) as
  2  stmt varchar2(200);
  3  begin
  4  stmt:='SELECT id FROM t1 WHERE nombre = :nombreUsuario';
  5  execute immediate stmt using nombreUsuario;
  6  dbms_output.PUT_LINE('SQL statement: ' || stmt);
  7  end;

SQL> exec demo01('aaa');
SQL statement: SELECT id FROM t1 WHERE nombre = :nombreUsuario

SQL> exec demo01('x" OR "1"="1');
SQL statement: SELECT id FROM t1 WHERE nombre = :nombreUsuario
```

Otras opciones para minimizar SQL Injection

- Principio de “least privileges” para los usuarios y roles en la base de datos Oracle: Dar solo los privilegios que realmente necesitan. **Oracle Database Vault** adicionalmente ayudaría a permitir validar de que IP, aplicación, etc. se puede acceder a la información.

  Oracle Virtual Private Database (VPD) y **Oracle Label Security (OLS)** para reducir el universo de información sensible que se podría ver por un SQL inyectado.

  Imaginemos que un usuario malintencionado, inyecta SQL: con **Oracle Advanced Security** se encriptaría la información, logrando que se minimice la perdida o robo de información ya que el usuario estaría limitado.

Otras opciones para minimizar SQL Injection

Si quisiéramos detectar si estamos siendo atacados por SQL Injection, se implementaría auditoria con las siguientes opciones:

Oracle Audit Vault: auditoria centralizada y extendida no solo para sistemas Oracle.
AUDIT database: una seria de comandos AUDIT para auditar operaciones de DML, DDL, LOGIN, SELECT, GRANT, REVOKE
Oracle Fine-Grained Auditing: para auditar el contenido de las operaciones SELECT y verificar si existe código no estándar que esta siendo ejecutado.
Oracle LogMiner: poder hacer minería de toda la información de cambio en la base de datos, tanto DDL (create, alter, drop) como DML (insert, update, delete).

Dominio A10 Gestión de Comunicaciones y Operaciones

A 10.10.1 Registro de auditorias
A 10.10.2 Supervisión de uso del sistema
A 10.10.3 Protección de la información de registro

¿Se requieren activar pistas de auditorias, pero los sistemas críticos en forma nativa no lo implementan?

Oracle Database - Auditoria

- **Oracle Audit Vault**: auditoria centralizada y extendida no solo para sistemas Oracle.
- **AUDIT database**: una serie de comandos AUDIT para auditar operaciones de DML, DDL, LOGIN, SELECT, GRANT, REVOKE.
- **Oracle Fine-Grained Auditing**: para auditar el contenido de las operaciones SELECT y verificar si existe código no estándar que esta siendo ejecutado.
- **Oracle LogMiner**: poder hacer minería de toda la información de cambio en la base de datos, tanto DDL (create, alter, drop) como DML (insert, update, delete).

Dominio A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A 12.3 Controles Criptográficos Requisito 3 y 4 PCI DSS

Es necesario identificar en base a un análisis de riesgos, información almacenada que debe ser necesariamente protegida mediante adecuados sistemas de encriptación.

Oracle Database - Encriptación

- **Oracle Advanced Security** provee:

Transparent Data Encryption (TDE): encriptación transparente de data, usando AES hasta 256 bits o 3DES168, a nivel de columna o tablespace.

Network encryption: para información en movimiento, provee los siguientes estándares de encriptación: RC4 (256, 128, 56 y 40 bits), DES (56 y 40 bits), 3DES (3 y 2 keys),AES (256, 192 y 128 bits).

Integrity of information: asegurando que el mensaje no haya sido modificado en tránsito, usando SHA-1 o MD5.

Strong authentication: con el soporte de los siguientes métodos de autenticación: Kerberos, RADIUS (Remote Authentication Dial-In User Service), Secure Sockets Layer (with digital certificates), PKI .

Dominio A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A 12.4.2 Protección de los datos de prueba del sistema

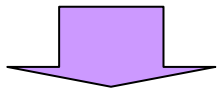
¿Como implementamos un eficiente sistema de protección de la data que se pasa de producción a desarrollo?

Qué es Data Masking?

Que es?

- Es el acto de anonimizar información confidencial de cliente, financiera, etc. para crear una nueva y legible información que mantengan sus propiedades, como ancho, tipo, formato.

LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000
D'SOUZA	989-22-2403	80,000
FIORANO	093-44-3823	45,000



Para que?

- Para proteger información confidencial en ambientes de test y desarrollo, usados por pero personal de desarrollo interno o de terceros.

- Cuando información de cliente debe ser compartida con terceras partes sin revelar informacion confidencial

LAST_NAME	SSN	SALARY
ANSKEKSL	111–23-1111	40,000
BKJHHEIEDK	111-34-1345	60,000
KDDEHLHESA	111-97-2749	80,000
FPENZXIEK	111-49-3849	45,000

Oracle Solution: Oracle EM Data Masking Pack

Dominio A15 Cumplimiento

A 15.1.3 Salvaguarda de los registros de la organización

¿Ok, ya sacamos el backup pero que pasa si se “pierde” la cinta…?

Oracle Database - Encriptación de Backups

- **Oracle RMAN**: puede encriptar un backup completo de base de datos Oracle, usando uno de los siguientes métodos: Oracle Transparent Data Encryption o Passphrase.

- **Oracle Secure Backup**: permite protección de backups, en cinta (tape) de base de datos Oracle y file systems de sistemas UNIX, Linux, Windows y NAS Adicionalmente Oracle Secure Backup permite encriptar el backup de la base de datos.

- **Oracle Data Pump**: puede encriptar archivos EXPORT, usando uno de los siguientes métodos: Oracle Transparent Data Encryption o Passphrase

Resumen: Opciones de Seguridad de Oracle Database

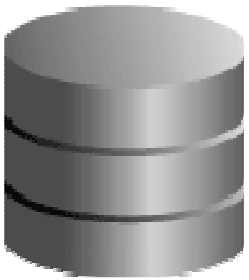
Proteger Información "en movimiento" con encriptación de red usando *Advanced Security Option*

Proteger Información de visualización y alteración, así como de amenazas internas usando *Database Vault*

Database Vault	Operational DBA	Data DBA / Manager
`Select SALARY from users;`	X	✓
`Alter system. Alter table..`	✓	X

* Example roles and privs

Consolidar Información de Auditoria y Reportes usando *Audit Vault*



Operational DBA

`Alter table …`

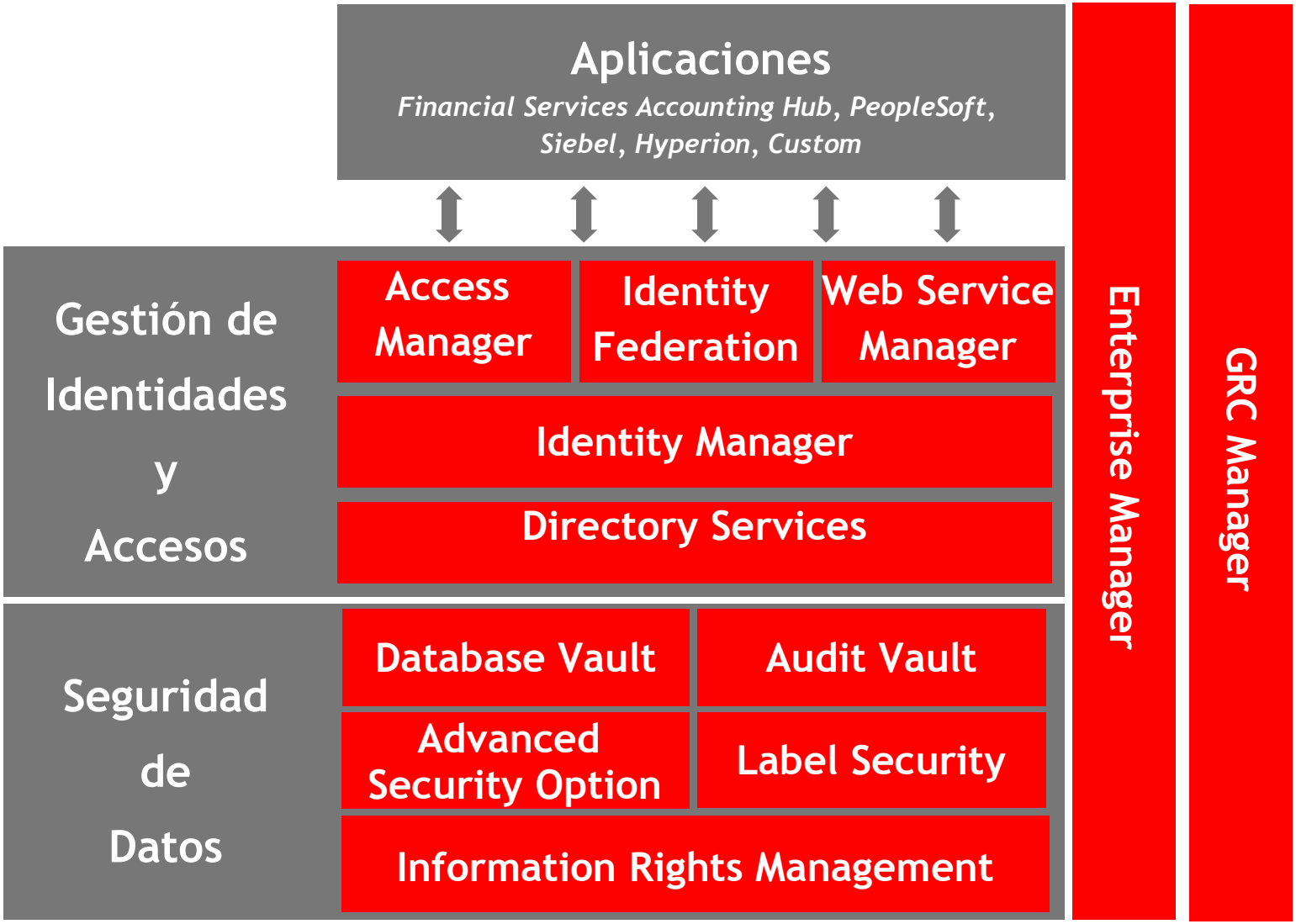
`Select SALARY from USERS;`

Respaldar Información de forma segura en cintas usando *Secure Backup*

Proteger Información de Usuario y Sensible "en reposo", encriptando columnas usando *Advanced Security Option*

LNAME	SSN	SALARY
KING		
SCOTT		
SMITH		

Arquitectura de Seguridad Oracle End-to-End



ORACLE IS THE INFORMATION COMPANY