ORACLE DATA REDACTION

ORACLE DATA REDACTION es una nueva característica de seguridad avanzada, introducida en Oracle Database 12 c . La función principal de esta función es enmascarar (ocultar / redactar) algunos datos (confidenciales) de los usuarios finales .

ORACLE DATA REDACTION enmascara los datos confidenciales justo antes de que los resultados de la consulta SQL se devuelvan a la aplicación que emitió la consulta. Los datos almacenados en la base de datos NO se cambian de ninguna manera.

Desde el punto de vista de las licencias, forma parte de la opción de seguridad avanzada (solo disponible como opción para Oracle Database Enterprise Edition).
Sin embargo, después, Oracle decidió hacerlo también disponible en Oracle Database 11 g (solo en la versión 11.2.0.4).

En esta guía usted aprenderá:

1. Creación de una política de redacción cuando se utiliza la redacción completa
2. Creando una política de redacción al usar la redacción parcial.
3. Creando una política de redacción al usar redacción aleatoria.
4. Añadiendo una columna a la política de redacción.

NOTA:

- ***Las políticas de redacción aplican si esta activa.***
- ***Se puede establecer solo una política de redacción a una tabla o vista***
- ***Aunque Oracle Data Redaction como concepto es fantástico, debe tener en cuenta que existen algunas limitaciones de implementación (por ejemplo, tipos de datos no compatibles)***

CREACIÓN DE UNA POLÍTICA DE REDACCIÓN CUANDO SE UTILIZA LA REDACCIÓN COMPLETA

CASO 1 :

Implementar una política de redacción completa para la columna SALARY de la tabla HR.EMPLOYEES

ACCIONES PREVIAS:

Conéctese como SYSTEM o como un usuario que tiene privilegios de ejecución de DBMS_REDACT.

```
-------------------------------------------------------------
-- 1. CONSULTAR LA TABLA  DE TRABAJO: HR.EMPLOYEES
--      ( antes de aplicar redacción )
-------------------------------------------------------------
-- Como SYSTEM
SELECT FIRST_NAME , LAST_NAME , HIRE_DATE, SALARY FROM HR.EMPLOYEES;
```

FIRST_NAME	LAST_NAME	HIRE_DATE	SALARY
Steven	King	17/06/2003	24000
Neena	Kochhar	21/09/2005	17000
Lex	De Haan	13/01/2001	17000
Alexander	Hunold	3/01/2006	9000
Bruce	Ernst	21/05/2007	6000
David	Austin	25/06/2005	4800
Valli	Pataballa	5/02/2006	4800
Diana	Lorentz	7/02/2007	4200
Nancy	Greenberg	17/08/2002	12008

```
-------------------------------------------------------------
-- 2. CREE LA POLÍTICA DE REDACCIÓN COMPLETA 'DMSK_SALARY'
--  La política establece que la columna SALARY (tabla HR. EMPLOYEES) se redacte utilizando la
--  redacción tipo FULL, aplica a cualquier usuario excepto a SYSTEM Y SYS:
-------------------------------------------------------------
-- Como SYSTEM

BEGIN
        dbms_redact.add_policy
        (object_schema => 'HR',
        object_name => 'EMPLOYEES',
        policy_name => 'DMSK_EMPLOYEES',
        policy_description => 'Enmascara campo SALARY',
        column_name => 'SALARY',
        function_type => DBMS_REDACT.FULL,
        expression => '1=1');
END;

-------------------------------------------------------------
-- 3. VERIFIQUE LA CREACION DE LA POLITICA
-------------------------------------------------------------
-- Como SYSTEM
SELECT * FROM REDACTION_POLICIES;
```

OBJECT_OWNER	OBJECT_NAME	POLICY_NAME	EXPRESSION	ENABLE	POLICY_DESCRIPTION
HR	EMPLOYEES	DMSK_EMPLOYEES	1=1	YES	Enmascara campo SALARY

```
** El enmascaramiento no aplica al usuario SYS y SYSTEM
```

```
-------------------------------------------------------------
-- 4. REVISAR RESULTADOS DE POLITICA DE REDACCION DEL TIPO FULL
-------------------------------------------------------------
-- Crear nuevo usuario LUISA con privilegios de consulta en la tabla
-- HR.EMPLOYEES

CREATE USER LUISA IDENTIFIED BY 123;
GRANT CREATE SESSION TO LUISA;
GRANT SELECT  ON HR.EMPLOYEES TO LUISA;

-- Conéctese como LUISA, consulte y verifique que la columna SALARY
-- esta enmascarada:

SELECT FIRST_NAME , LAST_NAME , HIRE_DATE, SALARY FROM HR.EMPLOYEES;
```

SIN MASCARA

FIRST_NAME	LAST_NAME	HIRE_DATE	SALARY
Steven	King	17/06/2003	24000
Neena	Kochhar	21/09/2005	17000
Lex	De Haan	13/01/2001	17000
Alexander	Hunold	3/01/2006	9000
Bruce	Ernst	21/05/2007	6000
David	Austin	25/06/2005	4800
Valli	Pataballa	5/02/2006	4800
Diana	Lorentz	7/02/2007	4200
Nancy	Greenberg	17/08/2002	12008

CON MASCARA

FIRST_NAME	LAST_NAME	HIRE_DATE	SALARY
Steven	King	17/06/2003	0
Neena	Kochhar	21/09/2005	0
Lex	De Haan	13/01/2001	0
Alexander	Hunold	3/01/2006	0
Bruce	Ernst	21/05/2007	0
David	Austin	25/06/2005	0
Valli	Pataballa	5/02/2006	0
Diana	Lorentz	7/02/2007	0
Nancy	Greenberg	17/08/2002	0

```
-------------------------------------------------------------
-- 5. AGREGAMOS ENMASCARAMIENTO A 2da COLUMNA HIRE_DATE
-------------------------------------------------------------
-- Como SYSTEM

            BEGIN
             DBMS_REDACT.ALTER_POLICY (
               object_schema     => 'HR',
               object_name       => 'EMPLOYEES',
               policy_name       => 'DMSK_EMPLOYEES',
               action            => DBMS_REDACT.ADD_COLUMN,
               column_name       => 'HIRE_DATE',
               function_type     => DBMS_REDACT.PARTIAL,
              expression => '1=1'  );

            END;
-- Comprobamos como LUISA
```

SELECT FIRST_NAME , LAST_NAME , HIRE_DATE, SALARY FROM HR.EMPLOYEES;

FIRST_NAME	LAST_NAME	HIRE_DATE	SALARY
Steven	King	1/01/2001	0
Neena	Kochhar	1/01/2001	0
Lex	De Haan	1/01/2001	0
Alexander	Hunold	1/01/2001	0
Bruce	Ernst	1/01/2001	0
David	Austin	1/01/2001	0
Valli	Pataballa	1/01/2001	0
Diana	Lorentz	1/01/2001	0
Nancy	Greenberg	1/01/2001	0

Nota : La columna SALARY muestra datos CERO, debido a que el valor por defecto para enmascaramiento de columna TIPO numérico es cero.

La columna HIRE_DATE, muestra como valor de enmascaramiento '01/01/2001', debido a que es el valor por defecto en ese tipo de dato.

La vista REDACTION_VALUES_FOR_TYPE_FULL muestra los valores por defecto de los distintos tipos de datos.

```
-- Conéctese como SYS y consulte:

SELECT * FROM REDACTION_VALUES_FOR_TYPE_FULL
```

NUMBER_VALUE	BINARY_FLOAT_VALUE	BINARY_DOUBLE_VALUE	CHAR_VALUE	VARCHAR_VALUE	NCHAR_VALUE	NVARCHAR_VALUE	DATE_VALUE
0	0	0					01/01/2001

CREACION DE POLITICA DE REDACCION PARCIAL

Redacción parcial significa que solo una parte de los datos en una columna específica será enmascarada, mientras que la otra parte de los datos será visible para el usuario, por ejemplo, los primeros 12 dígitos de la tarjeta de crédito. el número será redactado, mientras que otros 4 dígitos serán visibles.

CASO 2:
Implementar una política de redacción PARCIAL para la columna IDCARD de la tabla HR.CREDIT_CARD reemplazando los primeros 8 caracteres con el símbolo '*'.
Aplica a todos los usuarios que no cuenten con el ROL de ADMINISTRADOR

ACCIONES PREVIAS :
Conéctese como SYSTEM o como un usuario que tiene privilegios de ejecución de DBMS_REDACT

```
-------------------------------------------------------------
-- 1. Creando tabla CREDIT_CARD
-------------------------------------------------------------
-- Conectado como HR
CREATE TABLE HR.CREDIT_CARD
( ID INTEGER ,
  NOMBRE VARCHAR(50),
  IDCARD VARCHAR(12) );

INSERT INTO HR.CREDIT_CARD VALUES ( 1 , 'JUAN RIVERA SOLIS' , '987234372687');
INSERT INTO HR.CREDIT_CARD VALUES ( 2 , 'ALBERTO JUAREZ PONCE' , '772534961873');
INSERT INTO HR.CREDIT_CARD VALUES ( 3 , 'ROBERTO DE LA FLOR' , '237498428852');
INSERT INTO HR.CREDIT_CARD VALUES ( 4 , 'MACARENA SOLIS AVENDAÑO' , '753298721630');
COMMIT;

SELECT * FROM HR.CREDIT_CARD;
```

```
-------------------------------------------------------------
-- 2. Creando usuarios, roles y privilegios
-------------------------------------------------------------
-- Conectado como HR
-- Creando usuario LUCAS  ( rol: ADMINISTRADOR)
-- Creando usuario MATIAS ( rol: NINGUNO)

-- USUARIOS
CREATE USER LUCAS  IDENTIFIED BY 123;
CREATE USER MATIAS IDENTIFIED BY 123;

-- PRIVILEGIOS
GRANT CREATE SESSION TO LUCAS , MATIAS;
GRANT SELECT ON HR.CREDIT_CARD TO LUCAS, MATIAS;

-- CREAR ROL Y ASIGNAR A LUCAS
CREATE ROLE ADMINISTRADOR;
GRANT ADMINISTRADOR TO LUCAS;


-------------------------------------------------------------
-- 3. CREANDO POLITICA DE REDACCION PARCIAL
-------------------------------------------------------------
-- Formato de presentación: ***-***-2687

BEGIN
   DBMS_REDACT.ADD_POLICY(
   object_schema          => 'HR',
   object_name            => 'CREDIT_CARD',
   column_name            => 'IDCARD',
   column_description     => 'Columna sensible',
   policy_name            => 'CARD_PARCIAL',
   policy_description     => 'Enmascara campo IDCARD',
   function_type          => DBMS_REDACT.PARTIAL,
   function_parameters    => 'VVVFVVVFVVVV, VVV-VVV-VVVV, *, 1,6',
   expression             => 'SYS_CONTEXT(
                              ''SYS_SESSION_ROLES'',
                              ''ADMINISTRADOR'') =
                              ''FALSE''');
 END;
```

Para comprender la ***expresión*** definida en la política de redacción, consulte:

```
SELECT SYS_CONTEXT( 'SYS_SESSION_ROLES','ADMINISTRADOR') FROM DUAL;


-- Consultando como MATIAS (no cuenta con rol de ADMINISTRADOR)
```

ID	NOMBRE	IDCARD
1	JUAN RIVERA SOLIS	***-***-2687
2	ALBERTO JUAREZ PONCE	***-***-1873
3	ROBERTO DE LA FLOR	***-***-8852
4	MACARENA SOLIS AVENDAÑO	***-***-1630

```
-- Consultando como LUCAS (cuenta con rol de ADMINISTRADOR)
```

ID	NOMBRE	IDCARD
1	JUAN RIVERA SOLIS	987234372687
2	ALBERTO JUAREZ PONCE	772534961873
3	ROBERTO DE LA FLOR	237498428852
4	MACARENA SOLIS AVENDAÑO	753298721630

CREACION DE POLITICA DE REDACCION ALEATORIA

El tipo de redacción aleatoria generalmente se usa para los tipos de datos numéricos y fecha y hora debido a que genera valores que hacen muy difícil su aproximación a los valores reales.

CASO 3:
Implementar una política de redacción ALEATORIA en la columna SALARIO de la tabla PERSONAL.
Aplica la política solo al usuario ADAN.

ACCIONES PREVIAS : Conéctese como SYSTEM o como un usuario que tiene privilegios de ejecución de DBMS_REDACT

```
-------------------------------------------------------------
-- 1. Creando tabla HR.PERSONAL
-------------------------------------------------------------
-- Conectado como HR

CREATE TABLE HR.PERSONAL  ( ID INTEGER , DATOS VARCHAR(100) , SUELDO  NUMERIC( 10)) ;

INSERT INTO HR.PERSONAL  VALUES ( 1 , 'ROBERTO SINFUENTES ALVAREZ' , 8500 );
INSERT INTO HR.PERSONAL  VALUES ( 2 , 'ALBERTO RAMIREZ HERRERA' ,   9300 );
INSERT INTO HR.PERSONAL  VALUES ( 3 , 'SOFIA CARDENAS MORALES' ,    5800 );
INSERT INTO HR.PERSONAL  VALUES ( 4 , 'LEOPOLDO MATA ROSALES' ,     4800 );

COMMIT;

-------------------------------------------------------------
-- 2. Creando usuarios, roles y privilegios
-------------------------------------------------------------
-- Conectado como HR

CREATE USER ADAN IDENTIFIED BY 123;

GRANT CREATE SESSION TO ADAN;

GRANT SELECT ON HR.PERSONAL TO ADAN;

-------------------------------------------------------------
-- 3. CREANDO POLITICA DE REDACCION ALEATORIA
-------------------------------------------------------------
-- Columna SUELDO mostrará valor ALEATORIO
-- Conectado como HR

BEGIN
  dbms_redact.add_policy
  (object_schema => 'HR',
  object_name => 'PERSONAL',
  policy_name => 'MASK_PERSONAL_SUELDO',
  column_name => 'SUELDO',
  function_type => DBMS_REDACT.RANDOM,
  expression => 'SYS_CONTEXT(''USERENV'',
                ''SESSION_USER'') = ''ADAN''');
 END;
```

```
-----------------------------------------------------------
-- 4. REVISAR RESULTADOS DE POLITICA DE REDACCION ALEATORIO
-----------------------------------------------------------
-- Conectado como ADAN, consulte varias veces y verificar
que la columna SUELDO cambia, mostrando valores aleatorios.

SELECT * FROM HR.PERSONAL;
```

VALORES REALES (HR)

ID	DATOS	SUELDO
1	ROBERTO SINFUENTES ALVAREZ	8500
2	ALBERTO RAMIREZ HERRERA	9300
3	SOFIA CARDENAS MORALES	5800
4	LEOPOLDO MATA ROSALES	4800

VALORES ALEATORIOS (ADAN)

ID	DATOS	SUELDO
1	ROBERTO SINFUENTES ALVAREZ	1082
2	ALBERTO RAMIREZ HERRERA	608
3	SOFIA CARDENAS MORALES	1340
4	LEOPOLDO MATA ROSALES	3001

```
-----------------------------------------------------------
-- 5. AGREGAMOS ENMASCARAMIENTO A 2da COLUMNA DATOS
-----------------------------------------------------------
-- Como SYSTEM
BEGIN
  dbms_redact.ALTER_POLICY
  (object_schema => 'HR',
  object_name => 'PERSONAL',
  policy_name => 'MASK_PERSONAL_SUELDO',
  action     => DBMS_REDACT.ADD_COLUMN,
  column_name => 'DATOS',
  function_type => DBMS_REDACT.RANDOM,
  expression => 'SYS_CONTEXT(''USERENV'',
                ''SESSION_USER'') = ''ADAN''');
END;

-- Conectado como ADAN: Datos aleatorios
```

ID	DATOS	SUELDO
1	~32Z)%-:';:b1-5B/CBj95=J7K	811
2	`aaBu+@khiiJ}3HspqqR&;P	2867
3	hAK<<2lxpISDD:t!xQ[LLB	4856
4	_;wO(+-IgC W035QoK(_8	824

```
-- Conectado como HR: Datos originales
```

ID	DATOS	SUELDO
1	ROBERTO SINFUENTES ALVAREZ	8500
2	ALBERTO RAMIREZ HERRERA	9300
3	SOFIA CARDENAS MORALES	5800
4	LEOPOLDO MATA ROSALES	4800

CAMBIO DEL VALOR POR DEFECTO DE ENMASCARAMIENTO DE COLUMNAS

Inicialmente los tipos de datos compatibles con DATA REDACTION, tienen asignados valores predeterminados por defecto.
Por ejemplo el VARCHAR2 utiliza el espacio en blanco, el NUMBER el valor cero. Utilizaremos el procedimiento **UPDATE_FULL_REDACTION_VALUES** para cambiar el valor predeterminado.

Conectado como SYS modifiquemos el valor por defecto de VARCHAR2 a''X'

```
exec dbms_redact.UPDATE_FULL_REDACTION_VALUES ( varchar_val => 'X' );
```

Comprobar cambio :

```
select varchar_value from REDACTION_VALUES_FOR_TYPE_FULL;
```

NUMBER_VALUE	BINARY_FLOAT_VALUE	BINARY_DOUBLE_VALUE	CHAR_VALUE	VARCHAR_VALUE	NCHAR_VALUE	NVARCHAR_VALUE	DATE_VALUE
0	0	0		X			01/01/2001

Reiniciar el servidor, conéctese como LUISA y consulte :

```
SELECT FIRST_NAME , LAST_NAME , HIRE_DATE, SALARY
FROM HR.EMPLOYEES;
```

FIRST_NAME	LAST_NAME	HIRE_DATE	SALARY
Jennifer	X	13/08/1997	3600
Timothy	X	11/07/1998	2900
Randall	X	19/12/1999	2500
Sarah	X	04/02/1996	4000
Britney	X	03/1997	3900
Samuel	X	01/07/ 08	3200
Vance	X	17/03/1999	2800