1. Objetivo y Alcance

Describir los aspectos necesarios para garantizar la seguridad y la realización de las auditorías a las Base de Datos Oracle.

Esta guía comprende desde Introducción a la Seguridad, hasta las Auditorias de las Bases de Datos Oracle.

2. Responsable

El responsable de garantizar la adecuada aplicación y ejecución del presente documento, es el Coordinador Técnico de Base de Datos.

3. Definiciones

3.1 Auditoría

Proceso de seguimiento de un movimiento determinado en una base de datos basándose en la recolección de evidencias guardadas acerca del mismo.

3.2 Base de Datos

Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las Bases de Datos son uno de los grupos de aplicaciones de productividad personal más extendidos

3.3 Oracle

Es un sistema de gestión de base de datos relacional (o RDBMS por el acrónimo en inglés de Relational Data Base Management System), fabricado por Oracle Corporation.

Las demás definiciones que aplican para el presente documento se encuentran contempladas en la Norma **NTC ISO 9000:2000 Sistema de Gestión de la Calidad. Fundamentos y Vocabulario.**

4. Contenido

4.1 Introducción a la Seguridad de Bases de Datos Oracle	**Responsable: Coordinador Técnico de Base de Datos**

La seguridad de los datos y estructuras de las bases de datos es muy importante en un ambiente de producción, incluso de desarrollo para garantizar la disponibilidad y confiabilidad de la información. Por esto se hace necesario configurar un esquema de seguridad para garantizar estos aspectos, valiéndose de las potencialidades que proveen el hardware y el software de los servidores y motores de Base de Datos.

Para acceder a una Base de Datos se debe tener una cuenta de usuario. Se puede utilizar características como la caducidad y reutilización de las claves, perfiles para establecer estándares para las contraseñas y se pueden bloquear las cuentas después de cierto número de intentos fallidos de conexión.

Se debe utilizar privilegios para el control del acceso a los datos y objetos determinados permitidos. Se puede agrupar los privilegios en roles para mejor administración de los mismos para la asignación a usuarios. Además los roles se pueden restringir con contraseñas y pueden activarse y desactivarse dinámicamente.

Roles como el RESOURCE por tener privilegios de sistema como UNLIMITED TABLESPACE no deben ser asignados a cualquier usuario.

4.2 Seguridad en el Sistema Operativo	**Responsable: Coordinador Técnico de Base de Datos**

No se puede acceder a una Base de Datos sin tener acceso al servidor donde reside, por lo tanto, es necesario garantizar las restricciones necesarias a la plataforma y a la red. Se debe proteger también los archivos de la Base de Datos al igual que los archivos de copia de seguridad. Por lo tanto es necesario lo siguiente:

1. Garantizar la restricción por IPs a los servicios SQLNET y SSH al servidor de Base de Datos.
2. El permiso para SSH queda autorizado solo al **Coordinador Técnico de Base de Datos**.
3. El permiso para SQLNET queda autorizado a los integrantes del área de Base de Datos.
4. La clave del usuario Oracle solo será conocida y responsabilidad del **Coordinador Técnico de Base de Datos**.
5. Se debe autorizar el acceso por IPS en el archivo de configuración del SQLNET solo a los integrantes del grupo de Base de Datos y al Publicador de los aplicativos.

4.3 Cuentas de Usuario	Responsable: Coordinador Técnico de Base de Datos

Cuando se crea un usuario la prioridad debe ser crear una cuenta segura y útil que tenga los privilegios y parámetros adecuados.

Los lineamientos a tener en cuenta para la creación de cuentas de usuarios deben ser los siguientes:

En la Base de Datos solo deben existir los usuarios necesarios.

Se debe realizar una inspección periódica para detectar la existencia de usuarios no necesarios o creados sin autorización.

Los usuarios permitidos deben pertenecer a uno de los siguientes tipos:

- **Usuario Dueño:** es aquel dueño de los objetos de la Base de Datos.

- **Usuario Aplicativo**: es aquel que emula al usuario dueño ante el aplicativo y con el cual este se conecta a la Base de Datos y solo debe poseer privilegios sobre datos. No debe tener ningún privilegio sobre las tablas de auditoría. No puede crear objetos. No puede tener cuota sobre ningún tablespace.

- **Usuario Consulta**: es aquel que tiene privilegios solo de consulta a los datos, puede tenerlos también sobre las tablas de auditoría. No puede crear objetos. No puede tener cuota sobre ningún tablespace.

Ningún usuario debe tener asignado los roles CONNECT y RESOURCE.

Cada tipo de usuario debe tener un perfil con las siguientes características:

1. Tiempo de una sesión sin ser utilizada.
2. Número de intentos de conexión sin éxito.
3. Número de días de uso de una contraseña antes de caducar.
4. Número de veces debe cambiarse una contraseña antes de ser reutilizada.
5. Evaluación de la complejidad de una contraseña.

Los esquemas para cada perfil son los siguientes.

Perfil usuario dueño

```
CREATE PROFILE PROFILE_USER_OWNER LIMIT
IDLE_TIME 30
SESSIONS_PER_USER UNLIMITED
CONNECT_TIME UNLIMITED
```

FAILED_LOGIN_ATTEMPTS 4
PASSWORD_LIFE_TIME 30
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX 10
PASSWORD_GRACE_TIME 5
PASSWORD_VERIFY_FUNCTION VERIFY_ORACLE_PASSWORD -- copia adaptada de verify_function
;

Perfíl usuario consulta

CREATE PROFILE PROFILE_USER_SELECT LIMIT
IDLE_TIME 30
SESSIONS_PER_USER UNLIMITED
CONNECT_TIME 60
FAILED_LOGIN_ATTEMPTS 4
PASSWORD_LIFE_TIME 30
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX 10
PASSWORD_GRACE_TIME 2
PASSWORD_VERIFY_FUNCTION VERIFY_ORACLE_PASSWORD -- copia adaptada de verify_function
;

Perfil usuario aplicación

CREATE PROFILE PROFILE_USER_APLI LIMIT
IDLE_TIME 30
SESSIONS_PER_USER UNLIMITED
CONNECT_TIME UNLIMITED
--de gestión de contraseñas
FAILED_LOGIN_ATTEMPTS 4
PASSWORD_LIFE_TIME 30
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX 10
PASSWORD_GRACE_TIME 5
PASSWORD_VERIFY_FUNCTION VERIFY_ORACLE_PASSWORD -- copia adaptada de verify_function
;

Cada tipo de usuario debe tener un rol en el cual se especifique los privilegios que debe tener como:

1. Privilegio de conexión.
2. Privilegio para creación de objetos.

Los esquemas para cada rol son los siguientes.

Rol usuario dueño

```
CREATE ROLE ROLE_USER_OWNER;
GRANT CREATE VIEW,
CREATE TABLE,
ALTER SESSION,
CREATE CLUSTER,
CREATE SESSION,
CREATE SYNONYM,
CREATE SEQUENCE,
CREATE DATABASE LINK,
CREATE TYPE,
CREATE TRIGGER,
CREATE OPERATOR,
CREATE INDEXTYPE,
CREATE PROCEDURE TO ROLE_USER_OWNER;
```

Rol usuario consulta

```
CREATE ROLE ROLE_USER_SELECT;
GRANT ALTER SESSION,
CREATE SESSION TO ROLE_USER_SELECT;
```

Rol usuario aplicación

```
CREATE ROLE ROLE_USER_APLI;
GRANT CREATE VIEW,
ALTER SESSION,
CREATE SESSION,
CREATE SYNONYM,
CREATE SEQUENCE TO ROLE_USER_APLI;
```

Ningún usuario excepto los usuarios SYSTEM y SYS, debe tener privilegios de sistema y/o administrador. El responsable de las claves de estos usuarios es el Coordinador Técnico de Base de Datos.

Para el acceso a los integrantes del área de Base de Datos a la modificación de objetos por motivos de actualización a la Base de Datos se hará mediante un usuario individual con los privilegios necesarios.

Para esto se debe crear un rol con los privilegios de creación de objetos y de manipulación de datos. Se debe crear para este tipo de usuario también un perfil adecuado.

El perfil del usuario de Base de Datos debe cumplir con los siguientes lineamientos.

1. Solo puede haber una sesión por cada usuario en la Base de Datos.
2. El tiempo de conexión sin actividad debe ser de 30 minutos.
3. El número de intentos fallidos antes de bloquear la cuenta debe ser de dos.
4. El tiempo de vida de la contraseña debe ser de 15 días.
5. El reuso de la clave debe permitirse al décimo cambio.
6. El tiempo de gracia para cambiar la clave antes de bloquear la cuenta debe ser de 2 días.
7. Se debe hacer verificación de la calidad de la contraseña.

Perfil usuario coordinación Base de Datos

```
CREATE PROFILE PROFILE_USER_CDB LIMIT
IDLE_TIME 30
SESSIONS_PER_USER 1
CONNECT_TIME 30
FAILED_LOGIN_ATTEMPTS 2
PASSWORD_LIFE_TIME 15
PASSWORD_REUSE_TIME UNLIMITED
PASSWORD_REUSE_MAX 10
PASSWORD_GRACE_TIME 2
PASSWORD_VERIFY_FUNCTION VERIFY_ORACLE_PASSWORD -- copia adaptada de verify_function
;
```

El rol del usuario de Base de Datos debe cumplir con los siguientes lineamientos.

1. Tener privilegio para crear y alterar objetos para los usuarios tipo dueño de la Base de Datos.
2. El tablespace permanente y el temporal por defecto debe ser el de usuarios.

Rol usuario coordinación Base de Datos

```
CREATE ROLE ROLE_USER_CDB;
GRANT CREATE ANY VIEW,
INSERT ANY TABLE,
SELECT ANY TABLE,
UPDATE ANY TABLE,
DELETE ANY TABLE,
EXECUTE ANY PROCEDURE,
CREATE ANY TABLE,
ALTER SESSION,
CREATE ANY CLUSTER,
CREATE SESSION,
CREATE ANY SYNONYM,
CREATE ANY SEQUENCE,
CREATE DATABASE LINK,
CREATE ANY TYPE,
```

```
CREATE ANY TRIGGER,
CREATE ANY OPERATOR,
CREATE ANY INDEXTYPE,
CREATE ANY PROCEDURE,
ALTER ANY TABLE,
ALTER ANY CLUSTER,
ALTER ANY SEQUENCE,
ALTER ANY TYPE,
ALTER ANY TRIGGER,
ALTER ANY OPERATOR,
ALTER ANY INDEXTYPE,
ALTER ANY PROCEDURE,
DROP ANY VIEW,
DROP ANY TABLE,
DROP ANY CLUSTER,
DROP ANY SYNONYM,
DROP ANY SEQUENCE,
DROP ANY TYPE,
DROP ANY TRIGGER,
DROP ANY OPERATOR,
DROP ANY INDEXTYPE,
DROP ANY PROCEDURE TO ROLE_USER_CDB;
```

Para garantizar que el usuario puede realizar cualquier actividad sin restricciones se puede usar esta consulta para generarle los permisos. Conectado como usuario system.

```
SELECT DISTINCT 'GRANT '||PRIVILEGE||' TO ROLE_USER_CDB;' FROM DBA_SYS_PRIVS
WHERE (PRIVILEGE LIKE '%SELECT%'
OR PRIVILEGE LIKE '%CREATE%'
OR PRIVILEGE LIKE '%ALTER%'
OR PRIVILEGE LIKE '%DROP%'
OR PRIVILEGE LIKE '%EXECUTE%'
OR PRIVILEGE LIKE '%DELETE%'
OR PRIVILEGE LIKE '%INSERT%'
OR PRIVILEGE LIKE '%UPDATE%'
OR PRIVILEGE LIKE '%ANALYZE%'
OR PRIVILEGE LIKE '%COMMENT%'
OR PRIVILEGE LIKE '%GRANT%'
OR PRIVILEGE LIKE '%RESTRICTED%'
OR PRIVILEGE LIKE '%UNLIMITED%'
OR PRIVILEGE LIKE '%BACKUP%')
AND NOT (PRIVILEGE LIKE '%ROLE%'
OR PRIVILEGE LIKE '%RULE%'
OR PRIVILEGE LIKE '%PROFILE%');
```

Para quitar los permisos que no debiera tener se puede basar en la negación de la

anterior consulta así:

```
SELECT DISTINCT 'REVOKE '||PRIVILEGE||' FROM ROLE_USER_CDB;' FROM DBA_SYS_PRIVS
WHERE NOT ((PRIVILEGE LIKE '%SELECT%'
OR PRIVILEGE LIKE '%CREATE%'
OR PRIVILEGE LIKE '%ALTER%'
OR PRIVILEGE LIKE '%DROP%'
OR PRIVILEGE LIKE '%EXECUTE%'
OR PRIVILEGE LIKE '%DELETE%'
OR PRIVILEGE LIKE '%INSERT%'
OR PRIVILEGE LIKE '%UPDATE%'
OR PRIVILEGE LIKE '%ANALYZE%'
OR PRIVILEGE LIKE '%COMMENT%'
OR PRIVILEGE LIKE '%GRANT%'
OR PRIVILEGE LIKE '%RESTRICTED%'
OR PRIVILEGE LIKE '%UNLIMITED%'
OR PRIVILEGE LIKE '%BACKUP%')
AND NOT (PRIVILEGE LIKE '%ROLE%'
OR PRIVILEGE LIKE '%RULE%'
OR PRIVILEGE LIKE '%PROFILE%'));
```

El usuario entonces debe crearse de la siguiente forma:

```
CREATE USER  usuario IDENTIFIED BY passusuario
DEFAULT TABLESPACE  usuarios
TEMPORARY TABLESPACE tusuarios
PROFILE PROFILE_USER_CDB;

GRANT ROLE_USER_CDB, SELECT_CATALOG_ROLE, SELECT ANY DICTIONARY TO usuario;
```

4.4 Seguridad de la Contraseña Durante Inicios de Sesión	**Responsable: Coordinador Técnico de Base de Datos**
Se debe obligar a Oracle a que cifre las contraseñas antes de ser enviadas al momento de conectar a una Base de Datos desde un equipo remoto o al momento de establecer un enlace de Base de Datos. Para esto en la maquina cliente se de be configurar el parámetro ORA_ENCRYPT_LOGIN = TRUE en el archivo sqlnet.ora. En las maquinas servidor se debe configurar el parámetro DBLINK_ENCRYPT_LOGIN = TRUE en el archivo init.ora.	

4.5 Auditoría de las Bases de Datos	**Responsable: Coordinador Técnico de Base de Datos**
Se debe auditar todo movimiento sobre la estructura de los objetos y de conexiones. Para esto se debe activar la auditoría de la Base de Datos mediante la configuración del parámetro AUDIT_TRAIL = DB y activar la auditoria para el inicio y desconexiones de sesión, también para cualquier acción sobre los objetos involucrados como lo son las tablas, los trigger, los procedimientos y demás. Es responsabilidad del **Coordinador Técnico de Base de Datos** hacer esta configuración y realizar el control de las pistas de auditoría y su resguardo periódicamente para evitar consumo innecesario de recursos de la Base de Datos y garantizar la disponibilidad de estas pistas en el momento que se requieran.	

4.6 Auditoría de las Bases de Datos	**Responsable: Coordinador Técnico de Base de Datos**
Se debe auditar todo movimiento sobre la estructura de los objetos y de conexiones. Para esto se debe activar la auditoría de la Base de Datos mediante la configuración del parámetro AUDIT_TRAIL = DB y activar la auditoria para el inicio y desconexiones de sesión, también para cualquier acción sobre los objetos involucrados como lo son las tablas, los trigger, los procedimientos y demás. Es responsabilidad del **Coordinador Técnico de Base de Datos** hacer esta configuración y realizar el control de las pistas de auditoría y su resguardo periódicamente para evitar consumo innecesario de recursos de la Base de Datos y garantizar la disponibilidad de estas pistas en el momento que se requieran. Para información detallada para la implementación de los tipos de usuarios refiérase a los archivos IMPLEMENTACION CREACION DE USUARIOS.doc y LINEAMIENTOS CREACION DE USUARIOS.doc.	

5. Documentos de Referencia

- **NTC ISO 9000:2000** Sistema de Gestión de la Calidad. Fundamentos y Vocabulario.
- **NTC ISO 9001:2000** Sistema de Gestión de la Calidad. Requisitos.
- **NTC GP 1000:2004** Norma Técnica de Calidad en la Gestión Pública.
- **PAC-01** “Elaboración y Control de Documentos del Sistema de Gestión de la Calidad”.
- IMPLEMENTACION CREACION DE USUARIOS.doc
- LINEAMIENTOS CREACION DE USUARIOS.doc.

6. Historia de Modificaciones

Versión	Naturaleza del Cambio	Fecha del Cambio	Aprobación del Cambio
00	Actualización del Documento	29/05/2009	19/06/2009

7. Administración de Registros

Cod.	Nombre	Responsable	Ubicación	Acceso	Tiempo de Retención	Disposición

8. Anexos

“No aplica”