CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"Uso interno".**
El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.
No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

TABLA DE CONTENIDO

1. OBJETIVO.

La política aseguramiento de base de datos tiene como objetivo dar lineamientos de seguridad estándares que se deben implementar en todas las bases de datos y así garantizar que solo las personas autorizadas puedan acceder a la información.

2. ALCANCE.

El alcance de la presente política cubre: los activos de información ubicados en el data center de Triara y los que se encuentran en las diferentes nubes.

3. DEFINICIONES

- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y sus recursos asociados cuando lo requieran.
- **Información:** Datos relacionados que tienen significado para la organización. Es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y en consecuencia necesita una protección adecuada.
- **Activo de Información:** Toda la información y el conjunto de elementos y medios que la soportan en su procesamiento y almacenamiento.

4. CONTENIDO.

POLÍTICAS ORACLE.

Nota: Para muchas de estas validaciones se puede utilizar la herramienta de Oracle llamada Oracle Database Security Assessment Tool (DBSAT). Esta herramienta se debe ejecutar en cada base de datos productiva al menos 1 vez cada 6 meses y validar los resultados con las recomendaciones que se dan en este documento. Algunos puntos requieren el uso de sentencias sql las cuales se dejan documentadas en los scripts: scripts_validacion_aseguramiento_bd_oracle.sql y script_ejecucion_post_creacion_bd.sql

Cuentas de usuario

- Perfiles. Se deben configurar perfiles de acuerdo al rol de los usuarios, limitando el tiempo de vida de password entre otros. Los usuarios no deben tener el perfil DEFAULT. Los usuarios de la aplicación deben tener un perfil propio sin restricciones.

Ver Apéndice 1 para los valores de los perfiles más comunes que se deben crear.
Herramienta Validación: script:
"scripts_validacion_aseguramiento_bd_oracle.sql"

- Usuarios con password por defecto. Los password por defecto de las cuentas predeterminadas de Oracle son bien conocidas. Se debe cambiar los passwords, bloquear o eliminar la cuenta si no se requiere.
  Herramienta Validación: Oracle DBSAT y script:
  "script_ejecucion_post_creacion_bd.sql"

- Passwords Case Sensitive. Se recomienda siempre usar passwords Case Sensitive ya que incrementa el nivel de dificultad para que un atacante pueda encontrar la clave. Solo aplica para versiones Oracle 11g en adelante.
  Herramienta Validación: Oracle DBSAT
- Usuarios Inactivos. Las cuentas que han estado inactivas por más de 30 días deben ser investigadas para determinar si deben ser bloqueadas o eliminadas.
  Herramienta Validación: Oracle DBSAT
- Esquemas de ejemplo. Las cuentas de ejemplo que provee Oracle tal como SCOTT son bien conocidas y deben ser bloqueadas.
  Herramienta Validación: Oracle DBSAT y
  "script_ejecucion_post_creacion_bd.sql"
- Roles otorgados a PUBLIC. Se debe revisar qué roles están otorgados a PUBLIC y confirmar si se requiere o se puede asignar el ROL a usuarios específicos y quitar el permiso.
  Herramienta Validación: Oracle DBSAT
- Privilegios de sistema otorgados a PUBLIC. Se debe revisar qué privilegios están asignados a PUBLIC y confirmar si se requiere o se puede asignar el permiso a ROLES específicos y quitar el permiso.
  Herramienta Validación: Oracle DBSAT
- Cuentas de usuario en tablespaces SYSTEM – SYSAUX. Los tablespaces SYSTEM Y SYSAUX únicamente deben ser usados por cuentas de usuario provistos por Oracle.
  Herramienta Validación: Oracle DBSAT

Auditoría

- Auditoría DDL. Se debe configurar la auditoría para cualquier modificación de los objetos de la base de datos.
  Ver Apéndice punto 2 para los comandos para activar esta auditoría.
  Herramienta Validación: script:
  "scripts_validacion_aseguramiento_bd_oracle.sql"

- Auditoría GRANTS. Se debe auditar los grants y revoke que se ejecuten sobre la base de datos y validar después de cada despliegue la auditoría para validar si hubo algún permiso no autorizado.
  Ver Apéndice punto 2 para los comandos para activar esta auditoría.
  Herramienta Validación: script:
  "scripts_validacion_aseguramiento_bd_oracle.sql"

- Supplemental Login. Las bases de datos productivas deben tener configurado el supplemental login para asegurarse que los redo logs contengan la información requerida para describir todos los cambios de datos completamente.
  Ver Apéndice punto 3 para el comando de activación del supplemental login.
  Herramienta Validación: script:
  "scripts_validacion_aseguramiento_bd_oracle.sql" y script:
  "script_ejecucion_post_creacion_bd.sql"

Acceso

- Se debe configurar un trigger que sólo permita el ingreso de la aplicación con los usuarios web.
  Ver Apéndice punto 4 para el ejemplo de código del trigger.

CONFIGURACIÓN DE LA BASE DE DATOS

- Acceso a FileSystems. Se recomienda dejar el parámetro UTL_FILE_DIR vacío, ya que cualquier filesystem que esté configurado puede ser accedido por cualquier usuario. En su lugar se deben configurar directorios de Oracle los cuales permiten darle acceso solo a los usuarios que lo requieran.
  Herramienta Validación: Oracle DBSAT

- Autorización Externa. Los parámetros REMOTE_OS_ROLES y OS_ROLES deben estar en FALSE. Estos parámetros determinan si los roles concedidos a los usuarios están controlados por la sentencia GRANT o por el entorno del sistema operativo.
  Herramienta Validación: Oracle DBSAT
- Acceso a objetos del diccionario. Cuando el parámetro de inicio O7_DICTIONARY_ACCESSIBILITY se configura en FALSE, las tablas propiedad del usuario SYS no se ven afectadas por los privilegios del sistema ANY TABLE. Este parámetro siempre se debe establecer en FALSE para versiones anteriores a motor 19c porque las tablas propiedad de SYS controlan el estado general de la

base de datos y no deben estar sujetas a manipulación por parte de usuarios con privilegios ANY TABLE.
Herramienta Validación: Oracle DBSAT

APÉNDICE

1. **Profiles**
   Los siguientes son los valores que deben usarse para configurar los perfiles:

PROFILE	PARAMETRO	TIPO PARAMETRO	VALOR
LIMITADO	SESSIONS_PER_USER	KERNEL	4
LIMITADO	CPU_PER_SESSION	KERNEL	30000
LIMITADO	CPU_PER_CALL	KERNEL	300
LIMITADO	IDLE_TIME	KERNEL	30
LIMITADO	CONNECT_TIME	KERNEL	30
USUDBA	SESSIONS_PER_USER	KERNEL	4
USUDBA	IDLE_TIME	KERNEL	240
USUDBA	FAILED_LOGIN_ATTEMPTS	PASSWORD	3
USUDBA	PASSWORD_LIFE_TIME	PASSWORD	30
USUDBA	PASSWORD_REUSE_TIME	PASSWORD	365
USUDBA	PASSWORD_REUSE_MAX	PASSWORD	10
USUDBA	PASSWORD_LOCK_TIME	PASSWORD	1
USUDBA	PASSWORD_GRACE_TIME	PASSWORD	3
USUWEB	TODO	TODO	UNLIMITED

Tabla 1 Profiles

1. **Auditoría**

   Para activar la auditoría de DDL en las bases de datos se deben ejecutar los siguientes comandos:

   - audit ALTER ANY PROCEDURE by access;
   - audit ALTER ANY TABLE by access;
   - audit ALTER ANY TRIGGER by access;
   - audit ALTER DATABASE by access;
   - audit ALTER PROFILE by access;
   - audit ALTER SYSTEM by access;
   - audit ALTER USER by access;
   - audit AUDIT SYSTEM by access;
   - audit CREATE ANY JOB by access;
   - audit CREATE ANY LIBRARY by access;
   - audit CREATE ANY PROCEDURE by access;
   - audit CREATE ANY TABLE by access;
   - audit CREATE ANY TRIGGER by access;
   - audit CREATE EXTERNAL JOB by access;
   - audit CREATE PROFILE by access;
   - audit CREATE PUBLIC DATABASE LINK by access;
   - audit CREATE SESSION by access;
   - audit CREATE TABLE by access;
   - audit CREATE USER by access;
   - audit DROP ANY LIBRARY by access;
   - audit DROP ANY PROCEDURE by access;
   - audit DROP ANY TABLE by access;
   - audit DROP PROFILE by access;
   - audit DROP USER by access;
   - audit EXEMPT ACCESS POLICY by access;
   - audit GRANT ANY OBJECT PRIVILEGE by access;
   - audit GRANT ANY PRIVILEGE by access;
   - audit GRANT ANY ROLE by access;
   - audit SELECT ANY DICTIONARY by access;

2. **Suplemental Login**

   Se debe activar el suplemental login de la base de datos con el siguiente comando:

   - **alter database add supplemental log data;**

3. **Trigger acceso aplicaciones**

   CREATE OR REPLACE TRIGGER SYS.OSI_TRG_PERMISO_ACCESO

```
  AFTER LOGON
  ON DATABASE
DECLARE
  ipadd          VARCHAR2 (30) := NULL;
  v_osuser       VARCHAR2 (30) := NULL;
  v_sessionuser  VARCHAR2 (30) := NULL;
  v_serverhost   VARCHAR2 (30) := NULL;
  v_servicename  VARCHAR2 (30) := NULL;
  v_module       VARCHAR2 (30) := NULL;
  nmPermitido    NUMBER := 0;
  v_programa     VARCHAR2 (50) := '';
  v_prog_permi   NUMBER := 0;
  v_pro_per_aux  NUMBER := 0;
BEGIN
  ipadd := SUBSTR (SYS_CONTEXT ('USERENV', 'IP_ADDRESS'), 1, 25);
  v_osuser := SUBSTR (SYS_CONTEXT ('USERENV', 'OS_USER'), 1, 30);
  v_sessionuser := SUBSTR (SYS_CONTEXT ('USERENV', 'SESSION_USER'), 1, 30);
  v_serverhost := SUBSTR (SYS_CONTEXT ('USERENV', 'SERVER_HOST'), 1, 30);
  v_servicename := SUBSTR (SYS_CONTEXT ('USERENV', 'SERVICE_NAME'), 1,
30);
  v_module := SUBSTR (SYS_CONTEXT ('USERENV', 'MODULE'), 1, 30);

  SELECT program
    INTO v_programa
    FROM v$session
   WHERE audsid = USERENV ('sessionid')
   and rownum = 1;
```

```
IF v_sessionuser = 'XOMA' AND v_programa <> 'JDBC Thin Client'
THEN
  INSERT INTO SYSTEM.user_logon_denied
       VALUES (
            SYSDATE,
              'Program not autorized->'
            || ipadd
            || '<>'
            || v_osuser
            || '<>'
            || v_sessionuser
            || '<>'
            || v_serverhost
            || '<>'
            || v_servicename
            || '<>'
            || v_module
            || '<>'
            || v_programa);

  COMMIT;
  RAISE_APPLICATION_ERROR (-20001, 'You are not allowed to logon');
ELSE
  NULL;
END IF;
END;
```

5. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
15/05/2024	Elaboración del documento “Política de aseguramiento de base de datos”	1.0

Tabla 2 Control de cambios

6. FLUJO DE APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Elizabeth Díaz Área/Proceso: Directora de base de datos Fecha: 15/05/2024	Nombre: Elizabeth Díaz Área/Proceso: Directora de base de datos Fecha: 07/06/2024	Nombre: Javier Galván Área/Proceso: Gerencia Corporativa de tecnología. Fecha: 07/06/2024

Tabla 3 Flujo de aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.