1. Objetivo y Alcance

Dar los lineamientos que deben cumplir los usuarios según correspondan a sus necesidades dentro de aplicativo para la Base de Datos Oracle de Academusoft.

Esta guía comprende desde los aspectos preliminares hasta la actualización de Usuarios al nuevo esquema de roles y perfiles.

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 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

3.2 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.

Se considera a Oracle como uno de los sistemas de bases de datos más completos, destacando su: soporte de transacciones, estabilidad, escalabilidad, soporte multiplataforma.

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 Aspectos Preliminares	Responsable: Coordinador Técnico de Base de Datos

Las características de los usuarios deben corresponder a sus necesidades dentro del aplicativo. Por lo tanto se definen los siguientes lineamientos:

Se debe crear perfiles de usuario en la Base de Datos para asignarlos a los diferentes tipos de usuario (más adelante se detallan). Dentro de estos perfiles se incluyen características de seguridad como aspectos relevantes de las claves que identifican a los usuarios asociados a los mismos.

Para la creación de los perfiles en cuanto a la gestión de contraseñas se necesita una función la cual será la encargada de validar las características de las mismas como por ejemplo la longitud, que tengan al menos un carácter, un número y un signo de puntuación. Para esto se altera la función verify_function con el nombre verify_oracle_password, el script de creación llamado utlpwdmg.sql se encuentra en C:\oracle\ora90\rdbms\admin. El código modificado se muestra a continuación:

```
CREATE OR REPLACE FUNCTION verify_oracle_password
(username varchar2,
  password varchar2,
  old_password varchar2)
  RETURN boolean IS
   n boolean;
   m integer;
   differ integer;
   isdigit boolean;
   ischar  boolean;
   ispunct boolean;
   digitarray varchar2(20);
   punctarray varchar2(25);
   chararray varchar2(52);

BEGIN
   digitarray:= '0123456789';
   chararray:= 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
   punctarray:='!"#$%&()``*+,-/:;<=>?_';

   -- Check if the password is same as the username
   IF NLS_LOWER(password) = NLS_LOWER(username) THEN
     raise_application_error(-20001, 'Password same as or similar to user');
   END IF;

   -- Check for the minimum length of the password
   IF length(password) < 8 THEN
```

```
    raise_application_error(-20002, 'Password length less than 8');
  END IF;

  -- Check if the password is too simple. A dictionary of words may be
  -- maintained and a check may be made so as not to allow the words
  -- that are too simple for the password.
  IF NLS_LOWER(password) IN ('welcome', 'database', 'account', 'user', 'password',
'oracle', 'computer', 'abcd') THEN
    raise_application_error(-20002, 'Password too simple');
  END IF;

  -- Check if the password contains at least one letter, one digit and one
  -- punctuation mark.
  -- 1. Check for the digit
  isdigit:=FALSE;
  m := length(password);
  FOR i IN 1..10 LOOP
    FOR j IN 1..m LOOP
      IF substr(password,j,1) = substr(digitarray,i,1) THEN
        isdigit:=TRUE;
         GOTO findchar;
      END IF;
    END LOOP;
  END LOOP;
  IF isdigit = FALSE THEN
    raise_application_error(-20003, 'Password should contain at least one digit, one
character and one punctuation');
  END IF;
  -- 2. Check for the character
  <<findchar>>
  ischar:=FALSE;
  FOR i IN 1..length(chararray) LOOP
    FOR j IN 1..m LOOP
      IF substr(password,j,1) = substr(chararray,i,1) THEN
        ischar:=TRUE;
         GOTO findpunct;
      END IF;
    END LOOP;
  END LOOP;
  IF ischar = FALSE THEN
    raise_application_error(-20003, 'Password should contain at least one \
          digit, one character and one punctuation');
  END IF;
  -- 3. Check for the punctuation
  <<findpunct>>
  ispunct:=FALSE;
  FOR i IN 1..length(punctarray) LOOP
```

```
      FOR j IN 1..m LOOP
        IF substr(password,j,1) = substr(punctarray,i,1) THEN
          ispunct:=TRUE;
           GOTO endsearch;
        END IF;
      END LOOP;
    END LOOP;
    IF ispunct = FALSE THEN
      raise_application_error(-20003, 'Password should contain at least one \
             digit, one character and one punctuation');
    END IF;

    <<endsearch>>
    -- Check if the password differs from the previous password by at least
    -- 3 letters
    IF old_password IS NOT NULL THEN
      differ := length(old_password) - length(password);

      IF abs(differ) < 3 THEN
        IF length(password) < length(old_password) THEN
          m := length(password);
        ELSE
          m := length(old_password);
        END IF;

        differ := abs(differ);
        FOR i IN 1..m LOOP
          IF substr(password,i,1) != substr(old_password,i,1) THEN
            differ := differ + 1;
          END IF;
        END LOOP;

        IF differ < 3 THEN
          raise_application_error(-20004, 'Password should differ by at \
          least 3 characters');
        END IF;
      END IF;
    END IF;
    -- Everything is fine; return TRUE ;
    RETURN(TRUE);
  END;
  /
```

La ejecución de este script debe hacerse conectado como sysdba.

4.2 Perfil Usuario Dueño	Responsable: Coordinador Técnico de Base de Datos

El perfil creado para los usuarios dueños de objetos, se llama **profile_user_owner**. Este debe tener las siguientes características:

IDLE_TIME 60
SESSIONS_PER_USER 2
CONNECT_TIME 60

--De Gestión de contraseñas

FAILED_LOGIN_ATTEMPTS 2
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

4.3 Perfil Usuario Consulta	Responsable: Coordinador Técnico de Base de Datos

El perfil creado para los usuarios, usados para solo consulta de objetos propiedad de otros usuarios, se llama **profile_user_select**. Este debe tener las siguientes características:

IDLE_TIME 30
SESSIONS_PER_USER UNLIMITED
CONNECT_TIME 60

--De Gestión de contraseñas

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

4.4 Perfil Usuario Aplicativo	Responsable: Coordinador Técnico de Base de Datos

El perfil creado para los usuarios, usados para utilización de los aplicativos con permisos de ejecución, select, update y delete y sinónimos sobre objetos del usuario dueño y con los mismos permisos sobre objetos de otros usuarios, se llaman **profile_user_apli**. Este debe tener las siguientes características:

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

Según recomendaciones de administración para Oracle, es necesario manejar los propios roles para no usar por ejemplo el “connect” o “resource”, por lo tanto se crean los siguientes roles para ser usados:

Rol Usuario Dueño

Este rol recibe el nombre de ROLE_USER_OWNER.
Contiene los siguientes privilegios

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

Rol Usuario Consulta

Este rol recibe el nombre de ROLE_USER_SELECT.
Contiene los siguientes privilegios

ALTER SESSION
CREATE SESSION

Rol Usuario Aplicación

Este rol recibe el nombre de ROLE_USER_APLI.
Contiene los siguientes privilegios

CREATE VIEW
ALTER SESSION
CREATE SESSION
CREATE SYNONYM

4.5 Características de los Usuarios	Responsable: Coordinador Técnico de Base de Datos

4.5.1 Características Usuario Dueño:

Es aquel en cuyos objetos se basa un módulo o aplicativo. Por ejemplo académico, general o egresado. Este tipo de usuario es el dueño del esquema donde están los objetos utilizados por el aplicativo, este debe tener los privilegios para modificación y creación de objetos y aquel de inicio de sesión. Este usuario es el utilizado por el personal del área de Base de Datos.

Los privilegios dados al crear el usuario deben ser:
Rol ROLE_USER_OWNER

Se debe dar cuotas de uso sobre los tablespaces creados para utilización del usuario mediante la instrucción:

QUOTA UNLIMITED ON nombre_tablespace

El perfil que se debe asociar a este usuario es el de profile_user_owner (perfil usuario dueño).

4.5.2 Características Usuario Consulta

Es aquel usuario que es utilizado para realizar solo lecturas sobre datos de objetos de otros usuarios dueños, un ejemplo de este tipo de usuario es el reporteador.

Los privilegios dados al crear el usuario deben ser:
Rol ROLE_USER_SELECT

No se le da cuotas sobre tablespace ya que no maneja objetos propios y tampoco se le asigna un tablespace por defecto, solo el tablespace temporal (como se detalla en almacenamiento usuarios de consulta y aplicativo).

El perfil que se debe asociar a este usuario es el de profile_user_select (perfil usuario consulta).

4.5.3 Características Usuario Aplicación

Es aquel usuario que es utilizado para conectar el aplicativo a la Base de Datos y a los objetos del usuario dueño. Esto con el fin de restringir al aplicativo a solo las características que necesita quitándole aquellas de administración de objetos que no le corresponde. Este usuario tiene permisos de ejecución, select, update y delete y sinónimos sobre objetos del usuario dueño y con los mismos permisos sobre objetos de otros usuarios. Este usuario debe ser actualizado según los cambios del usuario dueño al cual está asociado.
Los privilegios dados al crear el usuario deben ser:
Rol ROLE_USER_APLI

Se debe dar cuotas de uso sobre los tablespaces creados para uso del usuario (como se detalla en almacenamiento usuarios de consulta y aplicativo) mediante la instrucción

QUOTA UNLIMITED ON nombre_tablespace
El perfil que se debe asociar a este usuario es el de profile_user_apli (perfil usuario aplicación).

4.6 Almacenamiento Usuarios Consulta y Aplicación	**Responsable: Coordinador Técnico de Base de Datos**

El tablespace permanente, utilizado por usuarios de consulta y aplicativo debe ser diferente al de usuarios dueños, por lo tanto se crea un tablespace para tal fin. Como estos usuarios no necesitan tablespace de auditoría ni de índice, entonces se crean solo el permanente utilizado por defecto. Este tablespace debe tener el siguiente nombre; USUARIOS.

El usuario de aplicativo debe usar el mismo tablespace temporal que el dueño al que está asociado, pero el usuario de consulta debe utilizar el tablespace temporal de usuarios llamado TUSUARIOS.

4.7 Actualización de Usuarios al Nuevo Esquema de Roles y Perfiles	Responsable: Coordinador Técnico de Base de Datos

Los usuarios actuales deben alterarse para acoplarlos al nuevo esquema de roles y perfiles, por lo tanto se procede de la siguiente forma:

4.7.1 Para usuarios Dueños

Se debe garantizar que los objetos de los cuales son dueños estén en los tablespaces correspondientes al usuario. Para llevar a cabo esta tarea se cuenta con los siguientes scripts:

Después de esto se procede entonces a asignar el perfil PROFILE_USER_OWNER y el rol ROLE_USER_OWNER y revocar los roles que tenia de CONNECT y RESOURCE, Adicionalmente se debe dar la QUOTA para los tablespaces correspondientes.

4.7.2 Para usuarios de Consulta

Estos usuarios realmente tienen solo privilegios sobre objetos de otros usuarios por lo tanto solo es alterar su tablespace permanente y temporal y asignarles el perfil PROFILE_USER_SELECT y el rol ROLE_USER_SELECT y revocar los roles de CONNECT y RESOURCE si los tuviese.

4.7.3 Para usuarios de Aplicativo

Estos usuarios por lo general en los aplicativos existentes no se encuentran, por lo tanto hay que crearlos con las características mencionadas anteriormente en este documento.

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”.

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”