## 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.

Detallar los pasos para centralizar el control de acceso a las bases de datos con que cuenta la Organización, definiendo lineamientos generales, “involucrados” y encargados para llevar siempre una gestión centralizada de los usuarios de cada una de las bases de datos.

## 2. ALCANCE.

Se define la gestión de usuarios de bases de datos de la organización y sus lineamientos.

## 3. DEFINICIONES

- PROFILE (Perfil de usuario): Un perfil es una forma de limitar los recursos que puede utilizar un usuario, el profile de un usuario define ciertos límites y parámetros que va a tener en el uso de su cuenta en cuanto a las sesiones, tiempos de uso y contraseñas.

- ROL: Un rol es una forma de agrupar permisos (privilegios) para asignarlos luego a los usuarios, cada usuario puede tener varios roles.

- DBA: Administrador de bases de datos.

- SYS – SYSTEM: Usuarios creados en la base de datos por defecto, desde ellos se accede en primera instancia para el inicio de la gestión de la base de datos creada.

## 4. CONTENIDO.

**PAUTAS Y LINEAMIENTOS:**

Las bases de datos son creadas de acuerdo a una necesidad del negocio, que fue autorizada y aprobada previamente por todas las instancias o niveles de autorización respectivos para la implementación.

Luego de la creación de bases de datos, por defecto, la instancia trae dos tipos de usuarios administrativos, denominados usuarios “Sys” y “System”, conectándose desde estos dos usuarios se accederá en primera instancia para la creación de usuarios administradores de la base de datos.

**USUARIOS ADMINISTRADORES**

- Los usuarios administradores se crean de acuerdo a la necesidad de acceso que tenga dicho administrador a la base de datos
- Los únicos cargos a los que se asignarán usuarios administradores serán: administradores de bases de datos y director de bases de datos
- La nomenclatura del nombre de usuario tendrá la estructura definida por el área de seguridad seguida del nombre del usuario.
- La creación de usuarios aplica para todos los ambientes (Pruebas Desarrollo, Preproducción, Producción).

**ROL de usuarios administradores:**

El rol DBA tiene el derecho para ver y manejar todos los datos y la estructura general de las bases de datos, es decir, tiene acceso a todos los privilegios del sistema.

**PROFILE DE USUARIOS**

Estos son los recursos para los cuales se definen limitaciones en cada profile de usuario:

- **SESSIONS_PER_USER:** Especifica el número de sesiones simultáneas a las que puede acceder el usuario.

- **CPU_PER_SESSION:** Especifica el límite de tiempo de CPU para una sesión, expresado en centésimas de segundos.

- **CPU_PER_CALL:** Especifica el límite de tiempo de la CPU para una llamada (un análisis, ejecución o recuperación), expresado en centésimas de segundo.

- **CONNECT_TIME:** Especifica el límite de tiempo transcurrido total para una sesión, expresado en minutos.

- **IDDLE_TIME:** Especifica el periodo permitido de tiempo inactivo continuo durante una sesión, expresados en minutos. Las consultas de larga ejecución y otras operaciones no están sujetas a este límite.

- **LOGICAL_READS_PER_SESSION:** Especifica el número permitido de bloques de datos leídos en una sesión, incluidos los bloques leídos de la memoria y el disco.

- **LOGICAL_READS_PER_CALL:** Especifica el número permitido de bloques de datos leídos para que una llamada procese una declaración SQL (un análisis, ejecución o recuperación.

- **PRIVATE_SGA:** Especifica la cantidad de espacio privado que una sesión puede asignar en el grupo compartido del área global del sistema (SGA).

- **FAILED_LOGIN_ATTEMPTS:** Especifica el número de intentos fallidos para iniciar sesión en la cuenta de usuario antes de que la cuenta se bloquee.

- **PASSWORD_LIFE_TIME:** Especifica el número de días que se puede usar la misma contraseña para la autenticación.

- **PASSWORD_GRACE_TIME:** Especifica un periodo de gracia en el cual el usuario deberá modificar la contraseña para la autenticación, la contraseña caduca si no se modifica dentro del período de gracia y se rechazan las conexiones adicionales. Si no establece un valor para PASSWORD_GRACE_TIME, su valor predeterminado UNLIMITED provocará que la base de datos emita una advertencia, pero permitirá que el usuario continúe conectándose indefinidamente

- **PASSWORD_REUSE_TIME y PASSWORD_REUSE_MAX:** Estos dos parámetros deben establecerse en conjunto uno con otro. PASSWORD_REUSE_TIME especifica el número de días antes de los cuales no se puede reutilizar una contraseña. PASSWORD_REUSE_MAX especifica el número de cambios de contraseña requeridos antes de que la contraseña actual pueda ser reutilizada. Para que estos parámetros tengan algún efecto, debe especificar un número entero para ambos.
  Si especifica un número entero para estos dos parámetros, el usuario no podrá reutilizar una contraseña hasta que se haya cambiado la contraseña la cantidad de veces especificada para PASSWORD_REUSE_MAX durante la cantidad de días especificada para PASSWORD_REUSE_TIME.
  Por ejemplo, si especifica PASSWORD_REUSE_TIME a 30 y PASSWORD_REUSE_MAX a 10, el usuario puede reutilizar la contraseña después de 30 días si la contraseña ya se ha cambiado 10 veces.

- **PASSWORD_LOCK_TIME:** Especifique el número de días que se bloqueará una cuenta después del número especificado de intentos de inicio de sesión fallidos consecutivos.

**PROFILE DE USUARIOS ADMINISTRADORES:**

El profile de administradores será el creado por default, cambiando o restringiendo los siguientes parámetros:

| PROFILE | NOMBRE DEL RECURSO | LÍMITE DEL RECURSO |
|---|---|---|
| USUDBA | FAILED_LOGIN_ATTEMPTS | 3 |
| USUDBA | PASSWORD_REUSE_MAX | 24 |
| USUDBA | IDLE_TIME | 240 minutos |
| USUDBA | PASSWORD_REUSE_TIME | 180 días |
| USUDBA | PASSWORD_LIFE_TIME | 30 días |
| USUDBA | SESSIONES_PER_USER | 3 |
| USUDBA | PASSWORD_VERIFY_FUNCTION | ORA12C_STIG_VERIFY_ FUNCTION |

*Tabla 1 Profile de usuarios administradores*

**PROFILE DE USUARIOS DESARROLLADORES:**

El profile de desarrolladores se creará según la necesidad, cambiando o restringiendo los siguientes parámetros:

| PROFILE | NOMBRE DEL RECURSO | LÍMITE DEL RECURSO |
|---|---|---|
| LIMITADO | FAILED_LOGIN_ATTEMPTS | 3 |
| LIMITADO | PASSWORD_REUSE_MAX | 24 |
| LIMITADO | IDLE_TIME | 30 minutos |
| LIMITADO | PASSWORD_REUSE_TIME | 365 días |
| LIMITADO | PASSWORD_LIFE_TIME | 30 días |
| LIMITADO | SESSIONS_PER_USER | 3 |
| LIMITADO | CPU_PER_SESSION | 30000 centésimas de segundo |
| LIMITADO | CPU_PER_CALL | 300 centésimas de segundo |
| LIMITADO | CONNECT_TIME | 30 minutos |
| LIMITADO | PASSWORD_VERIFY_FUNCTION | ORA12C_STIG_VERIFY_ FUNCTION |

*Tabla 2 Profile de usuarios Desarrolladores*

**USUARIOS PARA UNA APLICACIÓN:**

- Generalmente, se crea un solo usuario Tipo Owner para contener los objetos de la aplicación, en algunos casos puede ser más de uno de acuerdo a la necesidad. Para configurar el acceso directamente desde los servidores de aplicación o servicios web, se crean usuarios "WUSU" con los permisos que requieran a los objetos del owner, estos pueden ser tantos como se necesiten. Se crean dos cuentas:
    - **Owner (Propietario de los objetos o esquema):** Se identifica con el tema que va a tratar la aplicación.
      La nomenclatura de la cuenta se maneja con la estructura "USU" o "U" seguida del nombre de la aplicación o una abreviación que identifique la aplicación.

    - **La cuenta con la que se conectará la aplicación a esa base de datos:**
      La nomenclatura de la cuenta se maneja con la estructura definida por el área de seguridad y la palabra "USU" seguida del nombre de la aplicación o una abreviatura o combinación que identifique la aplicación.

- La solicitud para creación de un usuario para un funcionario deberá ser enviada y autorizada por su jefe inmediato o algún superior y deberá contener los siguientes datos del funcionario para el que se requiere la creación de usuario:

    - Nombre completo
    - Jefe inmediato
    - Cargo
    - Número de identificación
    - Área
    - Aplicativo donde se requiere el usuario

## 5. CONTROL DE CAMBIOS.

| FECHA | CAMBIO | VERSIÓN |
|---|---|---|
| 15/05/2024 | Elaboración del documento “Política de control de acceso a bases de datos” | 1.0 |

*Tabla 3 Control de cambios*

## 6. FLUJO DE APROBACIÓN.

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

*Tabla 4 Flujo de aprobación*

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