ES-13 CONFIGURACIÓN SEGURIDAD BASES DE DATOS

1. Normatividad Relacionada

NO-07 Responsabilidad de Usuarios
NO-11 Administración de Cuentas
NO-13 Comandos Especiales y Administración de Componentes Tecnológicos
NO-14 Administración y Configuración de Parámetros de Seguridad
NO-15 Nombres de Usuario
NO-16 Usuarios Privilegiados
NO-17 Usuarios Genéricos
NO-19 Administración de Accesos a Componentes Tecnológicos
NO-20 Claves de Acceso
NO-40 Software y Hardware Utilizado
ES-03 Contraseñas de Acceso
ES-04 Parámetros de Acceso
ES-05 Registro de Eventos

2. Objetivos

Establecer los parámetros básicos de seguridad a configurar en las Bases de Datos ORACLE y SQL Server.

3. Componentes Tecnológicos Afectados

Bases de Datos ORACLE y SQL*Server.

4. Descripción

Valores de los parámetros a configurar:

- **Configurable o parametrizable:**
  - ✓ Método de autenticación de usuarios: Por contraseña
  - ✓ Método de asignación de privilegios: Roles
  - ✓ Vigencia de la contraseña de usuario: 30 días
  - ✓ Cambio forzoso de contraseña: Habilitado
  - ✓ Asignación de derechos a usuarios del grupo PUBLIC sobre DB_LINKS: Permitir
- **No Configurable o configuración Manual:**
  - ✓ Cambiar periódicamente las contraseñas de usuarios SYS y SYSTEM: SI

- ✓ Asignación de roles a Desarrolladores que permitan ejecutar acciones sobre objetos en esquemas de ambientes de producción: No Permitir

- ✓ Crear tablas de aplicaciones en el tablespace SYSTEM: No Permitir

- ✓ Las tablas de aplicaciones tienen como propietarios a cuentas privilegiadas (SYS, SYSTEM): No Permitir

- **Responsabilidad del Líder Técnico y del Desarrollador:**

  - ✓ Longitud mínima de contraseña: 10 caracteres

  - ✓ Asignación de roles por defecto (CONNECT, RESOURCE, DBA, entre otros) a usuarios o grupos particulares: Evitar al máximo esta asignación

  - ✓ El grupo PUBLIC tiene acceso a objetos de la base de datos: No Permitir

  - ✓ Restringir a usuarios de la base de datos el permiso “GRANT…. WITH GRANT OPTION”, para propagar privilegios del sistema a otros usuarios; en caso de ser estrictamente necesario solamente asignar a usuarios privilegiados o usuarios propietarios de objetos.

  - ✓ Controlar la asignación de privilegios del sistema otorgados a través de la opción ADMIN OPTION, con la cual el privilegio recibido se puede asignar a otros usuarios y roles; en caso de ser estrictamente necesario su asignación debe ser previamente autorizada.

  - ✓ Controlar los roles asignados a los usuarios de acuerdo con las necesidades de su función en la organización: SI

- **Registros de Auditoria:**

  - ✓ Habilitar registros de auditoria en la Base de Datos, que permitan conocer el usuario que se conecta, la máquina desde la cual se conecta, la herramienta utilizada, las fechas y horas de conexión y desconexión: HABILITADO

  - ✓ Habilitar la auditoria de Base de Datos a nivel de RDBMS (motor), para que permita identificar el usuario, la fecha y la hora en que se ejecuta una instrucción de DELETE o UPDATE sobre campos de las tablas definidas como críticas o sensibles: HABILITADO.