Empresas Públicas de Armenia ESP., establece los requisitos para almacenar y recuperar de forma segura los nombres de usuario y las contraseñas de acceso a las bases de datos para su uso o por un programa o usuario que acceda a ésta y que se ejecute en la red de datos. El usuario debe autenticarse presentando credenciales válidas otorgadas por el administrador, se deben custodiar correctamente para garantizar la confidencialidad e integridad de la información contenida en los sistemas de información.

Las credenciales utilizadas para esta autenticación no deben residir en el código fuente del programa y no deben ser almacenadas en una ubicación a la que se pueda acceder a través de un servidor web.

Alcance.

Esta política está dirigida a todos los implementadores de sistemas y/o ingenieros de software que pueden estar codificando aplicaciones que tendrán acceso a un servidor de base de datos de producción y que utiliza la red de Empresas Públicas de Armenia ESP. Esto cubre aquellas bases de datos de sistemas licenciados de la entidad y que se soportan por infraestructura externa y a todos los programas de software (programas, módulos, bibliotecas o APIS que accedan a una base de datos de producción multiusuario).

Almacenamiento de nombres de usuario y contraseñas de base de datos.

- Los usuarios y contraseñas se deben almacenar en un archivo separado del código fuente del programa.
- Las credenciales de acceso pueden residir en el servidor de la base de datos. Para este caso un número de comprobación (hash) puede ser almacenado en el código fuente del programa.
- Las credenciales de acceso a la base de datos pueden ser almacenadas como parte de un servidor de autenticación (es decir, un directorio de derechos), como un servidor LDAP utilizado para la autenticación de usuarios. La autenticación de la base de datos puede ocurrir en nombre de un programa como parte del proceso de autenticación del usuario en el servidor de autenticación.
- Las credenciales de la base de datos pueden no residir en el árbol de documentos de un servidor web.
- La autenticación de paso (es decir, la autenticación de Oracle OPS $) no debe permitir el acceso a la base de datos basada únicamente en la autenticación de un usuario remoto en el host remoto.
- Las contraseñas o frases utilizadas para acceder a una base de datos deben cumplir con la Política para la Construcción de Contraseñas

Recuperación de nombres de usuario y contraseñas de la base de datos.

- Si se almacena en un archivo que no es código fuente, los nombres de usuario y las contraseñas de la base de datos se deben leer del archivo inmediatamente antes de su uso, posteriormente de la autenticación de la base de datos, se debe liberar o borrar la memoria que contiene el nombre de usuario y la contraseña.
- El ámbito en el que puede almacenar credenciales de base de datos debe estar físicamente separado de las otras áreas de su código, por ejemplo, las credenciales deben estar en un archivo de origen independiente. El archivo que contiene las credenciales no debe contener ningún otro código excepto las credenciales (es decir, el nombre de usuario y la contraseña) y cualquier función, rutina o método que se utilizará para acceder a las credenciales.
- Para los lenguajes que se ejecutan desde el código fuente, el archivo de origen de las credenciales no debe residir en el mismo árbol de directorios de archivos explorables o ejecutables en el que reside el código de ejecución.

Acceso a nombres de usuarios y contraseñas de la base de datos.

- Cada programa o cada colección de programas que implementan una única función de negocio debe tener credenciales de base de datos únicas. No se permite compartir credenciales entre programas.
- Las contraseñas de base de datos utilizadas por los programas son contraseñas a nivel de sistema definidas por la Política para la Construcción de Contraseñas.
- Los grupos de desarrolladores, sean de la propia Dirección TIC, o terceros, deben tener un procedimiento establecido para garantizar que las contraseñas de la base de datos se controlan y cambian de acuerdo con la Política para la Construcción de Contraseñas. Este procedimiento debe incluir un método para restringir el conocimiento de las mismas a un manejo de “necesidad de conocer”.

Definiciones y términos.

- **Credenciales**: Son el inicio de sesión, utilizadas para tener acceso a un servidor y a sus bases de datos determinan las clases de orígenes de datos que puede recuperar y mostrar el explorador de servidores.
- **Código fuente**: De un programa, está escrito por un programador en algún lenguaje de programación, pero en este primer estado no es directamente ejecutable por el computador.
- **Función Hash**: Es una función criptográfica basada en un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

- **LDAP**: (Protocolo Ligero de Acceso a Directorios). Hace referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
- **Módulo**: Parte autónoma de un programa de computador, en términos informáticos, se refiere a la división de un programa en una serie de subprogramas, denominados módulos.