EMPRESA DISTRIBUIDORA ELECTRICA SALVADOREÑA
MANUAL DE POLÍTICAS -POLÍTICAS INFORMÁTICAS

Código de Política: PIT-02-PCU-A10-2018
POLÍTICA DE CONTRASEÑAS Y USUARIOS (PCU)

- ***Consideraciones generales***

1. La asignación de usuarios y contraseñas es un permiso que EDESAL, S.A. de C.V. otorga a sus empleados y contratistas con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información de la Empresa.
2. Las cuentas de usuario son entera responsabilidad del empleado y contratista al que se le asigne. La cuenta es para uso personal, institucional e intransferible.
3. Las cuentas de usuario (usuario y contraseña) son sensibles a mayúsculas y minúsculas, es decir que estas deben ser tecleadas como se definan y no podrán ser cambiadas.
4. De ser necesaria la divulgación de la cuenta de usuario y su contraseña asociada, debe solicitarlo por escrito y dirigido al Departamento de Informática previa autorización del Jefe Inmediato o Gerente de área responsable.
5. Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración del Departamento de Informática.

- ***Tipos de cuenta de usuario***

6. Todas las cuentas de acceso a las plataformas tecnológicas como a los sistemas de información y aplicaciones son propiedad de la Empresa. Se definen tres tipos de cuentas:
   a) Cuenta de Usuario de Red: Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes equipos tecnológicos a su disposición y que permite la identificación del empleado o contratista en la red interna de datos de EDESAL, S.A. de C.V. para el desarrollo de sus labores con la respectiva restricción y/o permisos de acceso a los recursos informáticos disponibles en los servidores de datos.
   b) Cuenta de Usuario de Sistema de Información: Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información. Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.
   c) Cuenta de Administración de Sistema de Información: Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como, por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte del Departamento de Informática.
7. Todas las contraseñas de usuarios administradores deben ser cambiadas al menos cada 3 meses.
8. Todas las contraseñas de usuario de red y/o sistema de información deben ser cambiadas al menos cada **3 meses.**
9. Todas las contraseñas deben ser tratadas con carácter confidencial.

10. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica ni cualquier otro medio soportado a través de un recurso tecnológico físico o virtual.
11. Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otras personas o capturar a través de medios tecnológicos el ingreso de la misma.
12. Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.
13. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.
14. Se evitará el activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones

- ***Uso apropiado de usuarios y contraseñas***

15. Para el uso apropiado de usuarios y contraseñas se recomienda:
    - Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.
    - Cambiar periódicamente las contraseñas de los sistemas de información o servicio tecnológicos autorizados.

- ***Uso indebido del servicio de usuarios y contraseñas***

16. Se considera un uso indebido del servicio de usuarios y contraseñas:
    - Permitir el conocimiento de las claves a terceros.
    - Almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, etc. Si se requiere el respaldo de las contraseñas en medio impreso, el documento generado deberá ser único y bajo resguardo.
    - Almacenar las credenciales sin protección, en sistemas electrónicos personales (computadores portátiles, Tablets, memorias USB, teléfonos celulares, agendas electrónicas, etc.).

- Intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.
- Usar identificadores de terceras personas para acceder a información no autorizada o suplantar al usuario respectivo.
- Utilizar su usuario y contraseña para propósitos comerciales ajenos a la empresa.
- Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de EDESAL, S.A. de C.V.

- ***Monitoreo***

17. Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.
18. El Departamento de Informática podrá revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.