Empresas Públicas de Armenia ESP., para proteger las cuentas de usuario, como activos de información, provee las mejores prácticas para la construcción y protección de contraseñas seguras, brindando las pautas correctas para establecerlas, garantizando la confidencialidad, disponibilidad e integridad de la información contenida en los sistemas a los que se accede. Así mismo, a través de esta misma política, muestra las malas prácticas, de modo que no sean aplicadas en la construcción de contraseñas.

Alcance

La Política para la Construcción y Protección de Contraseñas aplica a todos los procesos, Servidores Públicos, terceros, aprendices, contratistas, proveedores, usuarios y partes interesas de la Empresa, cubriendo todas las contraseñas, incluyendo, pero no limitando, a cuentas de nivel de usuario, cuentas a nivel de sistema, cuentas web, cuentas de correo electrónico, protección de salva pantalla, buzón de voz e inicio de sesión de enrutadores locales de las Empresas Públicas de Armenia ESP.

Para dar cumplimiento a la Política para la Construcción y Protección de Contraseñas, Empresas Públicas de Armenia ESP., se compromete a que:

Todas las contraseñas deben cumplir o sobrepasar las siguientes directrices.

Las contraseñas fuertes deben:

- Contener al menos doce (8) caracteres alfanuméricos.
- Contener letras en mayúscula y minúsculas.
- Contener al menos un número (por ejemplo, 0-9).
- Contener por lo menos uno de los siguientes caracteres especiales: ,!$%^&*()_+|~-=\`{}[]:";'<>?,/.
- crear contraseñas que no puedan ser recordadas fácilmente y almacenarlas en un gestor de contraseñas
- Usar generadores aleatorios en línea como http://passwordsgenerator.net/. La Protección de contraseñas.
- Todas las contraseñas de nivel de usuario y de nivel de sistema deben cumplir con la política de construcción de contraseñas.
- Los usuarios no deben usar la misma contraseña para cuentas de Empresas Públicas de Armenia ESP y para otro acceso ajeno a la organización (por ejemplo, cuenta de ISP personal, comercio de opciones, beneficios, etc.).
- En lo posible, los usuarios no deben usar la misma contraseña para diversas necesidades de acceso a Empresas Públicas de Armenia ESP.
- Cuando se utiliza el Protocolo Simple de Administración de Red o SNMP (del inglés, Simple Network Management Protocol), las cadenas comunes deben definirse como algo distinto a los valores predeterminados de público, privado y sistema, y deben ser diferentes de las contraseñas utilizadas para iniciar sesión de forma interactiva. Las cadenas de SNMP deben cumplir con las directrices de construcción de contraseñas.
- Las contraseñas no deben ser compartidas y deben ser tratadas como información sensible, confidencial de Empresas Públicas de Armenia ESP, incluyendo, pero sin limitarse, asistentes

administrativos, secretarios, gerentes, compañeros de trabajo durante las vacaciones y miembros de la familia.

- Las contraseñas no deben insertarse en los mensajes de correo electrónico, ni en ninguna otra forma de comunicación electrónica.
- No revelar las contraseñas por teléfono a nadie, sin importar el mecanismo de presión que se ejerza.
- No revelar la contraseña en cuestionarios o formularios de seguridad.
- No insinuar o dar indicios del formato de una contraseña, por ejemplo: "mi apellido".
- No escribir ni guardar las contraseñas en cualquier lugar de su oficina.
- No almacenar contraseñas en un archivo de un sistema informático o dispositivos móviles (teléfono, Tablet) sin algún tipo de cifrado.
- No utilizar la función "Recordar Contraseña" de las aplicaciones, por ejemplo: navegadores web.
- Cualquier usuario que sospeche que su contraseña puede estar comprometida debe informar el incidente y cambiar todas las contraseñas.

Cambio de contraseñas.

- Todas las contraseñas a nivel de sistema (por ejemplo, root, cuentas de administración de aplicaciones, etc.) deben cambiarse al menos trimestralmente.
- Todas las contraseñas a nivel de usuario (por ejemplo, correo electrónico, web, computador de escritorio, etc.) deben cambiarse al menos cada cuatro meses.
- El cruce de contraseñas o las conjeturas pueden realizarse de forma periódica o aleatoria por el equipo de seguridad de la información o sus delegados. Si se detecta una falla o se rompe una contraseña durante una de estas exploraciones, se le solicitará al usuario que la cambie para que cumpla con las directrices de construcción de contraseñas.
- muestra un ejemplo:

Características de las contraseñas débiles:

- Cuentan con menos de 8 caracteres.
- Se encuentra en un diccionario, incluyendo un idioma extranjero, o existe en una lengua, dialecto o jerga.
- Cuentan con información personal como fechas de cumpleaños, direcciones, números telefónicos, o nombres de familiares, mascotas, amigos o personajes de fantasía.
- Tienen información relacionada con el trabajo como nombre del edificio en donde se trabaja, comandos de un sistema, lugares de la empresa y elementos hardware o software.
- Cuentan con patrones numéricos como aaabbb, qwerty, zyxwvuts o 123321.
- Cuentan con palabras comunes deletreadas hacia atrás, precedidas o seguidas por un número (por ejemplo, oterces, secreto1 o 1secreto).
- Utilizan alguna versión de “Bienvenido123”, “Contraseña123”, “Cambiame123”.
- Generación una contraseña de forma manual.

Protección de contraseñas.

- Todas las contraseñas de nivel de usuario y de nivel de sistema deben cumplir con la política de construcción de contraseñas.
- Los usuarios no deben usar la misma contraseña para cuentas de Empresas Públicas de Armenia ESP y para otro acceso ajeno a la organización (por ejemplo, cuenta de ISP personal, comercio de opciones, beneficios, etc.).
- En lo posible, los usuarios no deben usar la misma contraseña para diversas necesidades de acceso a Empresas Públicas de Armenia ESP.
- Cuando se utiliza el Protocolo Simple de Administración de Red o SNMP (del inglés, Simple Network Management Protocol), las cadenas comunes deben definirse como algo distinto a los valores predeterminados de público, privado y sistema, y deben ser diferentes de las contraseñas utilizadas para iniciar sesión de forma interactiva. Las cadenas de SNMP deben cumplir con las directrices de construcción de contraseñas.
- Las contraseñas no deben ser compartidas y deben ser tratadas como información sensible, confidencial de Empresas Públicas de Armenia ESP, incluyendo, pero sin limitarse, asistentes administrativos, secretarios, gerentes, compañeros de trabajo durante las vacaciones y miembros de la familia.
- Las contraseñas no deben insertarse en los mensajes de correo electrónico, ni en ninguna otra forma de comunicación electrónica.
- No revelar las contraseñas por teléfono a nadie, sin importar el mecanismo de presión que se ejerza.
- No revelar la contraseña en cuestionarios o formularios de seguridad.
- No insinuar o dar indicios del formato de una contraseña, por ejemplo: "mi apellido".
- No escribir ni guardar las contraseñas en cualquier lugar de su oficina.
- No almacenar contraseñas en un archivo de un sistema informático o dispositivos móviles (teléfono, Tablet) sin algún tipo de cifrado.
- No utilizar la función "Recordar Contraseña" de las aplicaciones, por ejemplo: navegadores web.
- Cualquier usuario que sospeche que su contraseña puede estar comprometida debe informar el incidente y cambiar todas las contraseñas.

Cambio de contraseñas.

- Todas las contraseñas a nivel de sistema (por ejemplo, root, cuentas de administración de aplicaciones, etc.) deben cambiarse al menos trimestralmente.
- Todas las contraseñas a nivel de usuario (por ejemplo, correo electrónico, web, computador de escritorio, etc.) deben cambiarse al menos cada cuatro meses.
- El cruce de contraseñas o las conjeturas pueden realizarse de forma periódica o aleatoria por el equipo de seguridad de la información o sus delegados. Si se detecta una falla o se rompe una contraseña durante una de estas exploraciones, se le solicitará al usuario que la cambie para que cumpla con las directrices de construcción de contraseñas.