1. Política General de Seguridad y Privacidad de la Información

"Empresas Públicas de Armenia ESP *se encuentra* comprometida *con una adecuada gestión de la información y sus derivados, garantizando* su integridad, confidencialidad y la disponibilidad, *acorde con las necesidades y expectativas de sus grupos de interés.*

Enfocando las acciones a la identificación de riesgos y vulnerabilidades, para la protección de la información y la disminución del impacto generado sobre sus activos.

1. objetivos:

Establecer los controles necesarios para la minimización del riesgo:

- En las diferentes funciones *y procesos misionales de la EPA ESP.*
- *Garantizar el* cumplimiento de los principios de seguridad de la información establecidos en la empresa.
- *Dar* cumplimiento a los principios de la función administrativa; *como lo son la buena fe, igualdad, moralidad, celeridad, economía, imparcialidad, eficacia, eficiencia, participación, publicidad, responsabilidad y transparencia.*
- *Incentivar y fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Empresas Públicas de Armenia ESP.*
- Mantener la confianza de sus grupos de interés.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Implementar el Sistema de Gestión de Seguridad de la Información.
- Garantizar la continuidad del negocio frente a incidentes generados por la materialización de riesgos en seguridad de la información.

2. Alcance

Esta política aplica a todos los procesos, servidores públicos, terceros, aprendices, contratistas, proveedores, usuarios y partes interesas de Empresas Públicas de Armenia ESP., y la ciudadanía en general.

3. Principios de seguridad de la información

- *Definir, compartir, publicar y aceptar las responsabilidades frente a la seguridad de la información de cada uno de los empleados, contratistas o terceros.*
- *Proteger la informacion:*
  - *Generada, procesada o resguardada por los procesos, su infraestructura tecnológica y activa de la información que hacen parte de los mismos.*
  - *Creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a su uso incorrecto, aplicando controles de acuerdo con la clasificación de la información de su propiedad o en custodia.*
  - *De las amenazas originadas por parte del personal.*
- *Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.*

- *Controlar la operación de sus procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.*
- *Implementar control de acceso a la información, sistemas y recursos de red.*
- *Garantizar:*
  - *Que la seguridad sea parte integral del ciclo de vida de los sistemas de información.*
  - *Un modelo de seguridad, a partir de las posibles amenazas y vulnerabilidades que pueden llegar a tener los sistemas de información.*
  - *La disponibilidad de sus procesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.*
  - *El cumplimiento de las obligaciones legales, reglamentarias y normativas aplicables a su gestión.*
  - *La protección de los datos personales de los grupos de interés, estableciendo prácticas y/o políticas específicas para su tratamiento.*

4. Lineamientos específicos que de la Política de General de Seguridad y Privacidad de la Información.

4.1. Política de Dispositivos Móviles GG-D-023

Proveer las condiciones para el manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas, entre otros) personales y de la organización, en los que se almacena información de clientes, proveedores, acceso a cuentas institucionales y de procesos que se desarrollan en Empresas Públicas de Armenia ESP.

4.2. Política de Gestión de Activos GG-D-025

Establece los requisitos y buenas prácticas para el manejo de los activos de información que se tienen en la empresa, teniendo en cuenta responsabilidades, clasificación y uso de cada uno de estos para cumplir con las funciones diarias en la entidad.

4.3. Política de Control de Acceso a Bases de Datos GG-D-017

Establece, los requisitos para almacenar y recuperar de forma segura los nombres de usuario y las contraseñas de acceso a la base de datos (es decir, las credenciales de la base de datos) para su uso, o por un programa o usuario que acceda a ésta y que se ejecute en la red de Empresas Públicas de Armenia ESP.

4.4. Política de Acceso a Redes y Recursos de Red GG-D-021

Definir los lineamientos base para la asignación de privilegios de acceso a todos los usuarios, sobre los diferentes segmentos de red dentro de Empresas Públicas de Armenia ESP y establecer los controles que deben ser implementados internamente para el monitoreo de todos los accesos no autorizados en la infraestructura de la organización.

4.5. Política de Controles Criptográficos GG-D-022

Establece buenas prácticas para el manejo de la información reservada o restringida que se genera en los diferentes procesos de la empresa, teniendo en cuenta algunos controles criptográficos para garantizar la confidencialidad e integridad de la información en la entidad.

4.6. Política para la Construcción y Protección de Contraseñas GG-D-022

Proveer las mejores prácticas para la creación de contraseñas seguras, aplicando las pautas correctas y del mismo modo identificar las malas prácticas que acostumbran tener los usuarios al crear sus contraseñas, lo cual genera bajos niveles de seguridad.

Establecer un estándar para la protección de contraseñas y su frecuencia de cambio en la empresa.

4.7. Política para la Seguridad física y del entorno GG-D-027

Mitigar los riesgos generados por acceso a instalaciones físicas como centros de datos, centros de cableado y puestos de trabajo, que pueden causar afectación la continuidad del negocio, y generar cultura en el cumplimiento de lineamientos de seguridad de física y del entorno por medio de buenas prácticas y control de los accesos.

4.8. Política de Escritorio y Pantalla Limpios GG-D-024

Definir las pautas específicas para la protección de la información en escritorios, durante y fuera de los sitios de trabajo de funcionarios para poder minimizar los riesgos a los que están expuestos donde la información sea volátil y de posible manipulación de malintencionados.

5.10. Política de Respaldo y Almacenamiento GG-D-026

Establece buenas prácticas, para el respaldo de la información que es generada, procesada y custodiada por Empresas Públicas de Armenia ESP, así como garantizar la disponibilidad de los datos institucionales cuando se presente una falla o sean solicitados.

5.11. Política para la Transferencia de Información y Medios Extraíbles GG-D-028

Minimizar el riesgo de pérdida o exposición de información confidencial, conservada por Empresas Públicas de Armenia ESP y reducir el riesgo de adquirir infecciones de malware en computadores operados por la empresa.