Empresas Públicas de Armenia ESP., establece buenas prácticas para el manejo de la información reservada o restringida, que se genera en los diferentes procesos, teniendo en cuenta algunos controles criptográficos para garantizar la confidencialidad e integridad de la información en la entidad. El 100% de las comunicaciones entre los sistemas de información, sin importar si estos son internos o externos o entre usuarios y sistemas de información, deben tener por lo menos un nivel de cifrado, el cual incluye Certificados de Seguridad, Algoritmos Digestivos, Funciones Criptográficas o incluso la combinación de las anteriores.

Alcance.

Esta política está dirigida a todos los servidores públicos de Empresas Públicas de Armenia ESP., que manipulen, modifiquen, generen o custodien información reservada o restringida para cumplir con sus funciones diarias o contribuir con los objetivos misionales de la entidad.

Controles criptográficos.

Empresas Públicas de Armenia ESP., velará porque la información generada, clasificada como reservada o restringida, sea cifrada al momento de almacenarse y/o transmitirse por cualquier medio y para lograrlo se debe:

- Almacenar y/o transmitir la información digital o física clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- Verificar que todo sistema de información o software que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- Desarrollar y establecer.

  Un procedimiento para el manejo y la administración de llaves de cifrado.

  Desarrollar y establecer estándares para la aplicación de controles criptográficos.
- Asegurarse que los controles criptográficos de los sistemas de información utilizados cumplan con los estándares establecidos para garantizar la confidencialidad de la información.

Definiciones y términos.

- **Criptografía:** ámbito de la criptología que se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.
- **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Certificados de seguridad:** Son códigos binarios usados para cifrar los canales de comunicación entre extremos, conocidos como algoritmos de cifrado de clave pública y clave privada, generalmente usados en sitios Web y conexiones seguras a servicios de red.
- **Algoritmos digestivos:** Son transformaciones que se realizan a cadenas de entrada, convirtiéndolas en salidas sin retorno, es decir, las cadenas de entrada digeridas son representadas por códigos diferentes de longitud fija conocidos como HASH, generalmente usados para almacenar contraseñas.

- **Funciones criptográficas:** Son algoritmos matemáticos consistentes en transformaciones y combinaciones que reciben como entrada un bloque de información y generan una salida cifrada con la información que se quiere proteger. Son usados para garantizar la integridad y la confidencialidad de la información.
- **Llaves criptográficas:** clave o palabra clave, es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.