Empresas Públicas de Armenia ESP, para minimizar el riesgo de pérdida o exposición de información confidencial y reducir el riesgo de adquirir infecciones de malware en computadores operados por la entidad; busca proveer dirección y soporte para la seguridad de la información conforme a los requisitos del negocio, las leyes y reglamentos pertinentes, concientizando a los usuarios para que estén al tanto de las amenazas e inquietudes de la seguridad de la información, buscando que el 100% de los medios extraíbles contengan un mecanismo de cifrado para evitar el compromiso de la confidencialidad de la información, cuando los dispositivos sean extraviados o comprometidos.

Alcance.

La Política para la Transferencia de Información y Medios Extraíbles aplica a todos los procesos, servidores públicos, terceros, aprendices, contratistas, proveedores, clientes y partes interesas de Empresas Públicas de Armenia ESP., y la ciudadanía en general.

Nivel de cumplimiento

El cumplimiento de la política aplica a todas los procesos y personas contempladas en el alcance y aplicabilidad

Para dar cumplimiento a la Política para la Transferencia de Información y Medios Extraíbles Empresas Públicas de Armenia ESP., se compromete a que:

- Los servidores públicos sólo pueden utilizar medios extraíbles en equipos de trabajo aprobados por la Dirección TIC.
- Estos medios extraíbles no se pueden conectar o utilizar en equipos que no estén bajo la calidad de propiedad o arrendamiento de Empresas Públicas de Armenia ESP., a no ser que sea autorizado su uso explícitamente por parte de la Dirección TIC.
- La información confidencial debe ser almacenada en medios extraíbles sólo cuando se requiera, bajo la responsabilidad de un funcionario de la entidad, en el desempeño de sus deberes asignados o al proporcionar información requerida por una entidad de control.
- Cuando la información confidencial se almacene en medios extraíbles, ésta debe contar con un mecanismo de cifrado de acuerdo con la política de cifrado aceptada por Empresas Públicas de Armenia ESP.
- Las excepciones a esta política pueden ser solicitadas mediante oficio, a la Dirección TIC desde donde se evaluará la viabilidad.
- La Dirección TIC se encargará de establecer los mecanismos de control y monitoreo para evitar que los demás servidores públicos usen dispositivos extraíbles sin la previa autorización y estará facultado para inhabilitar los puertos de conexión de forma física o lógica, según sea la necesidad.

Estándares, políticas o procesos relacionados.

Se debe tener especial cuidado con la información altamente sensible que maneja la empresa y añadir medidas de seguridad adicionales para evitar que esta información pueda ser sustraída o robada, acudiendo al bloqueo de los puertos USB en aquellos equipos que contengan este tipo de información.

Aquellos dispositivos extraíbles que sean de tipo promocional o no se tenga certeza de su origen, no deben ser usados en el ámbito laboral bajo ningún concepto, y mucho menos "**activarlos**" con un equipo corporativo. Este tipo de dispositivos, deben ser preparados convenientemente, examinando que no contengan ningún tipo de malware, siendo incluso necesario dar formato al dispositivo previamente para usarlo de forma segura, evitando el riesgo de infecciones mediante código dañino ejecutable o similar.

Definiciones y términos.

- **Cifrado:** En criptografía, se entiende como un proceso que utiliza un algoritmo de cifrado en conjunto con una clave que permite transformar un mensaje, de manera que sea incomprensible para todo individuo que intente acceder al mensaje sin la debida autorización.
- **Malware:** También conocido como código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo atentar contra la integridad de un sistema de información o un computador sin el consentimiento de su propietario.
- **Medios extraíbles:** Para el almacenamiento de datos, se entienden como aquellos dispositivos diseñados para retener cualquier tipo de información de manera externa e independiente a un computador por un tiempo prolongado.
- **Información sensible:** Se refiere a la información personal y privada de un individuo u organización, los cuales no deben ser accedidos por terceros sin una justificación válida.