Política de Seguridad y Privacidad de la Información

Empresas Públicas de Armenia ESP.

ARMENIA QUINDÍO.
20 de Junio de 2024

Tabla de contenido

1. Introducción

En la actualidad la información es un activo de gran *valor* para las organizaciones sin importar la categoría de la misma, permite efectividad en la toma de decisiones y fortalece la gobernanza del negocio la continuidad del negocio.

Para la Empresas Públicas de Armenia ESP, esto no es ajeno y la información se reconoce como un activo supremamente valioso que apoya cada vez más los procesos misionales y complementarios, eso nos lleva a no desconocer las amenazas y vulnerabilidades a las que podemos estar expuestos con nuestros activos de información, y la importancia en la gestión los riesgos de seguridad y privacidad de la información con el fin de prevenir o minimizar su impacto y probabilidad.

En consecuencia, de esa conciencia se requiere contar con estrategias de alto nivel que permitan la gestión efectiva a través de la implementación del Sistema de Gestión de Seguridad y privacidad de la Información y su mejoramiento continuo, garantizando que la entidad pueda generar y garantizar valor público en la relación del estado con los ciudadanos, usuarios y grupos de interés, promoviendo el uso y aprovechamiento de las tecnologías de la información a través de servicios seguros, con calidad y transparencia.

La adopción de políticas, normas y procedimientos de seguridad *y privacidad* de la información obedece también al cumplimiento de la normativa nacional, bajo este contexto de trabajo este documento describe:

- Estructura actual de la entidad, describiendo el mapa de procesos y perfiles generales*.*
- Estructura orgánica para la toma de decisiones en seguridad y privacidad de la información.
- Componente de gestión y gobierno en seguridad y privacidad de la información.
- Lineamientos en el manejo y gestión de la política interna de Seguridad y Privacidad de la Información desde Empresas Públicas de Armenia ESP.

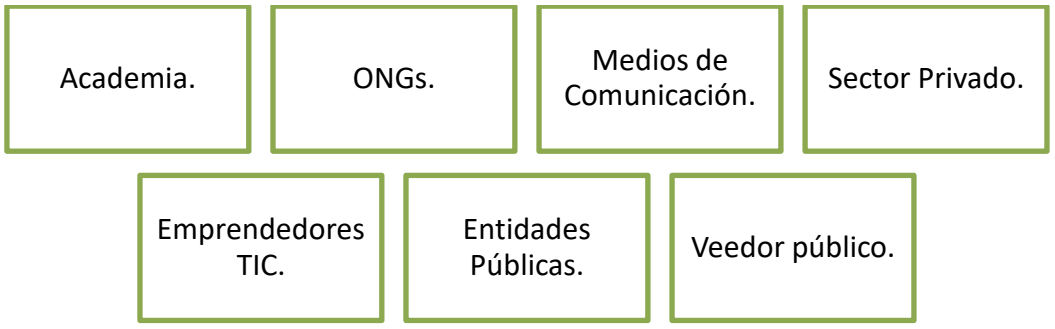
Contar con esta Política de Seguridad y Privacidad de la Información nos permite tener un conducto regular sobre la forma en que Empresas Públicas de Armenia ESP *sus colaboradores y proveedores debe* actuar y comportarse con el fin de gestionar y proteger los activos de información para brindar servicios integrales y eficientes.

2. Alcance

Este documento contempla la descripción de lineamientos y conducto regular referente a la Seguridad y Privacidad de la información de los activos de información que Empresas Públicas de Armenia ESP posee *y gestiona.*

La Política de Seguridad *y Privacidad* de la Información es aplicable en todo el ciclo de vida de los activos de información, estableciendo acciones de atención para la captura, procesamiento, almacenamiento, recuperación, distribución, intercambio, transferencia y consulta de información y destinación final del activo de información.

Esta política aplica a todos los funcionarios, contratistas, practicantes y terceros que tengan algún vínculo con Empresa Publicas de Armenia ESP, así como diferentes entes del ecosistema de negocio como:



Dirigido a todos los empleados, contratistas y proveedores de Empresas Públicas de Armenia ESP.

3. Glosario

- **Accesibilidad:** Garantía de acceso al usuario que lo requiera.
- **Acceso:** Es la capacidad de disponer de una información que ya existe dentro de un sistema informático (fichero, memoria, etc.) y que es posible acceder a ésta, continuando una secuencia fija y predeterminada de operaciones como también a partir de una clave, independientemente de las anteriores operaciones.
- **Activo de Información:** recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).
- **Activo:** cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga

valor para la organización.

- **Activos Tecnológicos:** Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.
- **Actualidad:** Vigencia de la información.
- **Compromiso De Confidencialidad:** Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- **Acuerdos de servicio:** se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes.
- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales: o Detectar cualquier alteración en los servicios TI. o Registrar y clasificar estas alteraciones. o Asignar el personal encargado de restaurar el servicio.
- **Administrador:** Toda persona responsable por la operación día a día de un sistema de cómputo o red de cómputo.
- **Adware:** Es el nombre que se le da a los programas diseñados para mostrar anuncios en el computador, redirigir solicitudes de búsqueda a sitios web publicitarios y recopilar datos de tipo de comercial sobre las personas.
- **Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- **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.
- **Almacenamiento en la Nube**: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

- **Alteración:** Es un tipo de delito informático mediante el cual se puede realizar fraude introduciendo, cambiando o borrando datos informáticos o la interferencia de sistemas informáticos.
- **Amenaza:** Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis De Brecha (Gap):** El GAP Análisis es un estudio preliminar que permite conocer la manera en la que se desempeña una empresa en materia de seguridad de la información, con relación a las mejores prácticas reconocidas en la industria, para esto se utilizan criterios establecidos en normas o estándares. El análisis establece las diferencias entre el desempeño actual y el deseado. Este análisis se puede aplicar a cualquier estándar certificable, lo normal es que se lleve a cabo para nuevos esquemas de certificación.
- **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Antivirus:** El software antivirus es un programa o conjunto de programas diseñados para prevenir, buscar, detectar y eliminar virus de software y otros programas maliciosos como gusanos, troyanos, adware y más.
- **Aplicación:** Una aplicación es cualquier programa, o grupo de programas, que está diseñado para el usuario final. El software de aplicaciones (también llamado programas de usuario final) incluye elementos como programas de bases de datos, procesadores de texto, navegadores web y hojas de cálculo.
- **Aplicativo De Gestión De Recursos Tecnológicos:** Herramienta de gestión que permite registrar, administrar controlar y evaluar todas las solicitudes y servicios de TIC's atendidos por la Dirección de Tecnologías e Información.
- **Árbol De Incidentes:** Es un listado de la estructura jerárquica de los tipos de incidentes, los cuales podrán ser seleccionados para categorizar la problemática reportada por el usuario.
- **Archivo:** Es uno o más conjuntos de documentos, sea cual fuere su fecha, su forma y soporte material, acumulados en un proceso natural por una persona o institución pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información para la persona o institución que los produce, para los ciudadanos, o para servir como fuentes de historia.
- **Archivos PST:** son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Sistema de Gestión de Seguridad de la Información - SGSI de una organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** Proceso mediante el cual se tiene un alto grado de certeza de la correcta identificación de personas, equipos, interfaces, datos y procesos.
- **Automatización:** Ejecución automática de ciertas tareas con el fin de agilizar el desarrollo de los procesos.
- **Autorización:** Proceso de dar privilegios a los usuarios.
- **Backdoor:** Es un programa informático malicioso que se utiliza para proporcionar al atacante acceso remoto no autorizado a un computador comprometido mediante la explotación de vulnerabilidades de seguridad. Un Backdoor funciona en segundo plano y se oculta del usuario. Es muy similar a otros virus de malware y, por lo tanto, es bastante difícil de detectar. Es uno de los tipos de parásitos más peligrosos, ya que le da a una persona maliciosa la capacidad de realizar cualquier acción posible en un computador remoto.
- **Base de datos de gestión de configuraciones (CMDB, Configuration Management Database):** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.
- **Bases de datos:** Es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico. Las bases de datos tradicionales se organizan por campos, registros y archivos. Un campo es una pieza única de información; un registro es un sistema completo de campos; y un archivo es una colección de registros.
- **Botnet:** Es un grupo de computadoras conectadas de manera coordinada con fines maliciosos. Cada computadora en una botnet se llama Bot. Estos bots forman una red de datos que es maliciosamente controlada por un tercero y utilizada para transmitir malware o correo no deseado, o para lanzar ataques. Un botnet también puede ser conocido como un ejército zombie.
- **Buzón:** espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros**.**

- **Cadena de Custodia:** Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- **CAL (Client Access Licenses – Licencias de Acceso de Cliente):** Es una licencia que otorga a un usuario o dispositivo el derecho a acceder a los servicios de un servidor. El licenciamiento por Servidor está orientado a servidores físicos de uno o dos procesadores. El licenciamiento por Procesador está orientado a instancias físicas y/o virtuales y considera el número de procesadores físicos de cada servidor para licenciar.
- **Calidad:** se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo en el mercado.
- **Canal de comunicación:** medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.
- **Carácter especial de contraseña:** Son aquellos símbolos que se pueden usar al momento de crear un password. Por ejemplo, @ % + \ / ' ! # $ ^ ? : . ( ) { } [] – ' - –
- **Características de la Información:** las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.
- **Carpetas Compartidas:** es básicamente igual que una carpeta normal salvo que su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **Catálogo De Servicios De TI:** Es un documento no técnico que contiene la descripción de los servicios de TI ofrecidos para ser utilizado como guía para orientar y dirigir a los usuarios, incluye los niveles de servicio, recoge las condiciones de prestación de servicios, así como las responsabilidades asociadas a cada uno de estos.
- **Centro de cómputo:** espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón.
- **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- **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.
- **Claves, contraseña o password:** forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.
- **Código malicioso:** Programas potencialmente peligrosos diseñados para dañar los sistemas y los datos, o modificarlos para que funcionen de manera incorrecta.

- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - **Sistema de Gestión de la Seguridad de la Información**.
- **Cómputo forense:** El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006].
- **Conformidad:** Cumplimiento de lineamientos y estándares vigentes
- **Conjunto de Datos:** la serie de datos estructurados, vinculados entre sí y agrupados dentro de una misma unidad temática y física, de forma que puedan ser procesados apropiadamente para obtener información.
- **Contención:** Evitar que el incidente siga ocasionando daños.
- **Continuidad de negocio:** (Inglés: Business Continuity). Incluye la planificación para asegurar la continuidad de las funciones críticas de un negocio en la eventualidad de una falla o desastre. Este tipo de planificación abarca aspectos claves de la operación tales como personal, facilidades, comunicaciones, y cambio de controles. Un plan de continuidad de negocio es inclusive de un Plan de Recuperación de Desastre para la recuperación de infraestructura tecnológica.
- **Continuidad del servicio TI:** Procedimientos de continuidad adecuados y justificables en términos de costos para cumplir con los objetivos propuestos en el renglón de continuidad en la organización. Esto incluye el diseño de planes de recuperación y medidas de reducción de riesgo.
- **Control de Acceso**: Es el que se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que le sea permitido el acceso al sistema.
- **Control informático:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.
- **Control Social:** Es el derecho y el deber de los ciudadanos a participar de manera individual o a través de sus organizaciones, redes sociales e instituciones, en la vigilancia de la gestión pública y sus resultados.
- **Control**: Toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal. En la entidad se aplica por medio de la declaración de aplicabilidad.

- **Copia de seguridad (Backup):** Es el proceso de respaldo de archivos o bases de datos físicos o virtuales a un sitio secundario para la preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de datos es fundamental para un plan de recuperación de desastres (DR) exitoso.
- **Correo Basura:** Correos no deseados
- **Correo electrónico:** servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.
- **Correo Spam:** Correo electrónico no deseado que se envía a un destinatario especifico, sin su consentimiento u aprobación, generalmente en forma masiva y con fines comerciales
- **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.
- **Criticidad:** Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
- **Cuenta de usuario:** Es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.
- **Custodio de activo de información:** individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.
- **Custodio:** Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.
- **Dato privado:** dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- **Dato público:** dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
- **Dato semiprivado:** es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- **Dato:** Descripción de hechos, situaciones, sucesos o valores,

representados mediante símbolos físicos o electrónicos.

- **Datos Abiertos:** Datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Datos biométricos:** parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).
- **Datos personales sensibles:** aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **Datos Sensibles:** Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
- **DDOS (Distributed Denial of Service – Ataque Distribuido de Denegación de Servicio):** Un tipo de ataque en el que un número de computadores u otros dispositivos inundan con paquetes de datos un sitio web hasta que se queda sin posibilidad de aceptar más solicitudes y, para los clientes habituales, parece estar fuera de línea. Este es uno de los usos que se les da a los botnets.
- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el SGSI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma ISO 27001
- **Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de las ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

- **Derechos de autor:** Entendida en este contexto como Propiedad Industrial, hace referencia a la protección de los intereses de los creadores al ofrecerles ventajas en relación con sus creaciones. La entidad nacional delegada para la administración de la Propiedad Industrial en Colombia es la Superintendencia de Industria y Comercio a través de la Delegatura para la Propiedad Industrial. Esta entidad cuenta con la Oficina de Servicio al Consumidor y Apoyo Empresarial, OSCAE, quien administra y coordina las actividades de divulgación y formación en temas de Propiedad Industrial. La Oficina tiene entre sus funciones diseñar y promover los mecanismos y herramientas para la divulgación, promoción y fomento de las funciones, trámites y servicios institucionales.
- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
- **Día Cero:** Vulnerabilidad de software que el fabricante desconoce y para la que, por lo tanto, no existen parches o actualizaciones de seguridad. Si los cibercriminales descubren un Día Cero, ejecutan un exploit para atacar los sistemas afectados.
- **Dirección IP:** Cada nodo en una red TCP/IP requiere de una dirección numérica que identifica una red y un anfitrión local o nodo de la red, esta dirección se compone de cuatro números separados por puntos, por ejemplo, 10.2.1.250
- **Directiva o directriz:** Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Directiva:** Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disco duro:** Es parte de una unidad a menudo llamada "unidad de disco" o "unidad de disco duro", que almacena y proporciona un acceso relativamente rápido a grandes cantidades de datos en una superficie o conjunto de superficies cargadas electromagnéticamente.
- **Disponibilidad:** Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Divulgación:** En este contexto, hace referencia a la distribución no autorizada de datos a personas no autorizadas.
- **Documento:** Es cualquier unidad en la cual se registra información, independiente del tipo de soporte en el que se encuentre (papel, cintas y discos magnéticos, películas, fotografías, etc.) el cual puede ser modificado y controlado por técnica de versiones.
- **DVD:** Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.
- **Eficiencia:** Capacidad para realizar análisis y descargas de los datos con

unos niveles de desempeño y tiempos esperados.

- **Entidad:** Institución u organización con la capacidad y/o facultad de definir inventarios de y conjuntos de datos e información a publicar.
- **Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
- **Erradicación:** Eliminar la causa del incidente y todo rastro de los daños.
- **Escalamiento:** El primer nivel de resolución es la mesa de servicios, cuando no sea capaz de resolver en primera instancia, debe recurrir a especialistas o algún superior que tome las decisiones que se escapen de su responsabilidad, es decir escalonar el servicio. Existe un tercer nivel de escalonamiento a expertos para temas muy especializados
- **Especialista:** Usuario a quien se le designan los casos de acuerdo a la clasificación estipulada en el árbol de incidentes o de petición de servicio.
- **Estándar:** Es un conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Para que sea un estándar debe haber sido construido a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular.
- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:20022], es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009]
- **Evento:** Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
- **Exactitud:** Datos diligenciados correctamente.
- **Excepciones (Seguridad de información):** Casos especiales que no cumplen una política, procedimiento o regla.
- **Exploit:** Un exploit es el uso de software, datos o comandos para "explotar" alguna debilidad en un sistema o programa informático para llevar a cabo acciones dañinas, como un ataque de denegación de servicio, caballos de Troya, gusanos o virus. La debilidad en el sistema puede ser un error, un fallo o simplemente una vulnerabilidad de diseño. Un exploit remoto explota la vulnerabilidad de seguridad sin tener acceso

previo al sistema. Un exploit local necesita acceso previo al sistema vulnerable y generalmente implica aumentar los privilegios de la cuenta de usuario que ejecuta el exploit. Aquellos que utilizan este tipo de ataques a menudo usan ingeniería social para obtener información crítica necesaria para acceder al sistema.

- **File Server:** Repositorio de información asignado a un área o proceso para guardar información, este sitio debe tener controles de ingreso de escritura, modificación o eliminación.
- **Firewall:** Es un sistema de seguridad de red diseñado para evitar el acceso no autorizado a o desde una red privada. Los firewalls se pueden implementar como hardware y software, o como una combinación de ambos. Los de red se utilizan con frecuencia para evitar que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que ingresan o salen de la intranet pasan por el firewall, que examina cada mensaje y bloquea aquellos que no cumplen con los criterios de seguridad especificados.
- **Formato Libre:** Formato de archivo que se puede crear y manipular mediante cualquier software libre, sin restricciones legales
- **Formato propietario:** Son formatos de archivo que requieren herramientas que no son públicas
- **FTP**: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.
- **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.
- **Garantía:** se deben tener en cuenta los plazos de vigencia de la garantía ofrecidos y los requeridos para el proceso de implementación, adaptación, pruebas, y puesta en funcionamiento.
- **Gestión de claves:** (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.
- **Gestión de incidentes de seguridad de la información:** (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información
- **Gestión de Incidentes:** Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la

información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

- **Gestión documental:** Son las actividades administrativas y técnicas que propenden por la planificación, manejo y organización de la información producida y recibida por las entidades desde que se produce o recibe hasta su disposición final.
- **Gobierno Abierto:** Doctrina política que sostiene que los temas de Gobierno y administración pública deben ser abiertos a todos los niveles posibles en cuanto a transparencia.
- **Gobierno Digital:** Es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones -Ministerio TIC, que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital"
- **Grupo de Interés:** Es un conjunto de personas, organizadas en torno a un tema de interés común, con el fin de actuar conjuntamente en el desarrollo del mismo.
- **Grupos de Valor:** para Función Pública corresponden a las entidades del estado, servidores públicos y ciudadanos.
- **Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.
- **Hardware:** Se refiere a las partes físicas de un computador y dispositivos relacionados. Los dispositivos de hardware interno incluyen motherboards, discos duros y memoria RAM. Los dispositivos de hardware externos incluyen monitores, teclados, mouse, impresoras y escáneres.
- **Hash:** Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- **Impacto:** Daño producido a la organización por la materialización de un riesgo sobre los activos tecnológicos, visto como diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.
- **Incidente Mayor:** Es la categoría de impacto más alta de un incidente. Un incidente mayor produce una severa interrupción del negocio.
- **Incidente:** Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información confidencial:** Información, restringida o secreta, que es extremadamente sensible y únicamente puede ser conocida por personas específicas dentro de la Entidad. Para compartir esta información con

terceros debe existir autorización expresa (escrita) de las directivas de la Entidad. Toda la información definida como reserva bancaria será clasificada como Confidencial

- **Información pública clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.
- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.
- **Información Pública:** Agrupación ordenada de datos públicos, que permite otorgarle a los datos una utilidad y uso en determinado contexto, y que se genera a partir del desarrollo de actividades para el funcionamiento del Estado, es decir de los registros periódicos de las actividades misionales de las entidades, o como consecuencia del ejercicio de funciones de rutina en el Estado.
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **Infraestructura de procesamiento de información:** Cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.
- **Infraestructura tecnológica:** elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.
- **Infraestructura:** Es el conjunto de recursos tecnológicos, hardware y software que permite la optimización de los procesos que soportan los servicios ofrecidos a nuestros clientes.
- **Ingeniería social:** Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para la obtención de una contraseña o acceso a un sistema de información.
- **Instalaciones:** Corresponde a todos los lugares físicos y virtuales en los que se aloja información de la Entidad.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los

activos.

- **Internet:** A veces llamada simplemente "la red", es un sistema mundial de redes informáticas que proporciona una variedad de instalaciones de información y comunicación y que consta de redes interconectadas que utilizan protocolos de comunicación estandarizados.
- **Intranet:** Es un servidor Web seguro, interno y exclusivo, que le da a los empleados y al personal de una institución o compañía la posibilidad de compartir información sin que se exponga a la comunidad Web en general.
- **Inventario de activos: L**ista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)
- **Inyección SQL: (SQLi)** se refiere a un ataque de inyección en el que un atacante puede ejecutar sentencias SQL maliciosas (también comúnmente denominadas carga maliciosa) que controlan el servidor de bases de datos de una aplicación web. Dado que una vulnerabilidad de Inyección SQL podría afectar a cualquier sitio web o aplicación web que utilice una base de datos basada en SQL, la vulnerabilidad es una de las más antiguas, más prevalentes y más peligrosas de las vulnerabilidades de las aplicaciones web.
- **ISO 27001:** ISO 27001 es una norma emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ITIL IT Infrastructure Library:** Un marco de gestión de los servicios de tecnologías de la información. **Keyloggers:** Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este término con malware dmalware del tipo daemondaemon (demonio), es decir, actúa como un proceso iproceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.
- **Keylogger:** Es un spyware malicioso que se utiliza para capturar información confidencial mediante el registro de teclas. Éste captura información de contraseñas o información financiera, que luego se envía a terceros para su explotación criminal.

- **LAN:** Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.
- **Lineamiento:** Es una directriz o norma obligatoria para efecto de esta política que debe ser implementada por la entidad para el desarrollo de la política de Datos Abiertos. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas.
- **Llamadas De Servicio:** Requerimiento que no interrumpe o disminuye la calidad del servicio, como: solicitud de préstamo, asignación y traslado de equipos de cómputo o video, configuración de telefonía, entre otros.
- **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.
- **Malware (malicious software):** Es cualquier programa o archivo que es dañino para un usuario de computador. El malware incluye virus informáticos, gusanos, caballos de Troya y spyware. Estos programas maliciosos pueden realizar una variedad de funciones, que incluyen robar, cifrar o eliminar datos confidenciales, alterar o secuestrar funciones de cómputo central y supervisar la actividad del computador de los usuarios sin su permiso.
- **Mantenimiento, actualizaciones y soporte:** se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice.
- **Medios de almacenamiento extraíbles:** Medios para guardar y portar información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB, etc.
- **Mesa de Ayuda de Tecnología:** es el único Centro de Atención al Usuario en donde la DIRECCIÓN TICS presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TICs.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **Navegar por la red**: Es la acción de visitar páginas en la World Wide Web por medio de una aplicación llamada explorador y que contiene documentos de hipertexto interconectados y accesibles vía Internet.
- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.
- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar

la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **No repudio:** servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).
- **Parte interesada (Stakeholder):** persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Participación Ciudadana:** Es la intervención de los ciudadanos en los asuntos de carácter público que le son de su interés o en donde pueden decidir. El propósito de la Participación Ciudadana es permitir que las entidades públicas garanticen la incidencia efectiva de los ciudadanos y sus organizaciones en los procesos de planeación, ejecución, evaluación -incluyendo la rendición de cuentas- de su gestión, a través de diversos espacios, mecanismos, canales y prácticas de participación.
- **Periférico:** Elemento o dispositivo del computador que no hace parte de la unidad central, tales como el monitor, mouse, teclado, parlantes, impresora, escáner, unidades de almacenamiento, etc.
- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de recuperación de desastres:** (Inglés: Disaster Recovery Plan - DRP). Es parte de un plan mayor de Continuidad de Negocios que incluye los procesos y soluciones con miras a restaurar aplicaciones críticas, información, hardware, comunicaciones y redes y otras infraestructuras propias de sistemas de información y tecnología.
- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento (orientado por el Decreto 612 de 20183) de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la información de la Entidad.
- **Plan Institucional de Publicación de Datos Abiertos:** es un programa formal de carácter público que debe actualizar anualmente cada una de las Instituciones Obligadas, con las fechas comprometidas de publicación de los Conjuntos de Datos aprobados por el Grupo de Trabajo.
- **POCA Plan-Oo-Check-Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Principios de Seguridad de la información:** Confidencialidad, disponibilidad e integridad.
- **Privacidad De La Información:** Derecho que tienen todos los titulares de

la información, en relación con la información que involucre datos personales y la información clasificada que éstos hayan entregado o esté en poder de la entidad, en el marco de las funciones que a ella le compete realizar y que generan en las entidades, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.[1]

- **Proceso:** conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)
- **Propietario del riesgo:** (Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- **Propietario/responsable de la información**: Individuo, Entidad o unidad de negocio que tienen bajo su responsabilidad la administración p a r a el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. Los propietarios de la información deben garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de políticas con otros propietarios de información y con propietarios de infraestructura. Los propietarios deben especificar cómo se debe utilizar la información y como se debe proteger, además de definir cómo se administrarán los procedimientos de control y cómo se aplicarán los niveles apropiados de protección para la información acorde con su clasificación (Pública, Pública Clasificada y Pública Reservada).
- **Propietarios de infraestructura:** Administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados. Los propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la información y de la Entidad.
- **Protección a la duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.
- **Pruebas de penetración:** Su principal propósito detectar vulnerabilidades que resultan de fallas de software, configuraciones inapropiadas, etc. Se puede realizar de forma remota o local y se ejecutan las pruebas tal y como lo intentaría un intruso con propósitos adversos para la organización.

[1] 1 Modelo de Seguridad y Privacidad de la Información.

- **Publicar:** Es el acto mediante el cual se publica información, esta puede ser pública, interna, restringida y reservada.
- **Punto Único de Contacto (PUC):** Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.
- **Recuperabilidad:** Atributos que permiten mantener y preservar un nivel especifico de operaciones y de calidad.
- **Recuperación de desastres:** Consiste en las precauciones que se adoptan para minimizar los efectos de un desastre y que la organización pueda continuar operando o reanudar rápidamente las funciones de misión crítica.
- **Recurso de Datos:** son los archivos descargables en formatos abiertos y accesibles mediante diversos medios de distribución.
- **Recursos informáticos I Activos informáticos:** Hardware, software, equipos de cómputo y telecomunicaciones
- **Recursos Tecnológicos:** Son todos los bienes tangibles e intangibles que posee la entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias.
- **Red:** Es un sistema de comunicación que se da entre diversos recursos informáticos por medio de protocolos para permitir el intercambio de información.
- **Registro De Eventos:** En ingles Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.
- **Regla de negocio:** Describe las políticas, normas, operaciones, definiciones y restricciones presentes en una organización y que son de vital importancia para alcanzar los objetivos misionales.
- **Reportes o salidas:** se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.
- **Requerimiento:** Son solicitudes estándar asociadas a los servicios de TI para las cuales existe una aprobación predefinida y un impacto controlado. Dentro de los objetivos específicos en su atención se encuentran: • Aconsejar a los usuarios sobre el uso adecuado de los servicios de tecnología dispuestos para su utilización. • Proveer información a los usuarios sobre la disponibilidad de los servicios y los procedimientos requeridos para obtenerlos. • Otorgar y entregar los componentes de las peticiones de servicio estándar.
- **Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.
- **Responsable de activo de información:** Persona idónea de la Entidad, que tiene la responsabilidad de adelantar acciones para que la

información cumpla con los tres ejes de la seguridad (Confidencialidad, integridad y Disponibilidad).

- **Responsable del tratamiento:** persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.
- **Reutilización o reusó de datos:** Producto que se elabora a partir de los datos públicos, puede ser una visualización, una aplicación web, un servicio, un cuadro de mandos, una noticia o una información, un dibujo, una gráfica dinámica, entre otras cosas.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).
- **Segregación de tareas:** Reparto de tareas sensibles entre distintos servidores públicos para reducir el riesgo de un mal uso de los sistemas informáticos e información de manera deliberada o por negligencia.
- **Seguridad de la información:** Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- **Seguridad:** Medida tomada para reducir el riesgo
- **Sensibilidad:** Nivel de impacto que una divulgación no autorizada podría generar.
- **Servicio**: Cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.
- **Servidor Proxy:** Es un computador que funciona como intermediario entre una estación de trabajo de un usuario y el internet. Se instala por seguridad, control administrativo y servicio de caché, disminuyendo el tráfico de internet e incrementando la velocidad de acceso.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **SGSI Sistema de Gestión de la Seguridad de la Información:** Según [ISO IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)
- **SharePoint:** Sitio para almacenamiento de la información pública para uso interno de la institución.
- **Shareware:** Software de libre distribución que cuenta con un periodo de pruebas que puede variar entre 30 y 60 días.
- **Sistema De Gestión De Seguridad De La Información:** Parte del sistema de gestión general de una organización, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer,

implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

- **Sistema De Información:** Conjunto de datos, aplicaciones y equipos que de manera conjunta proveen a la empresa la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.
- **Sistema operativo:** Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.
- **SOC:** Los Centros de Operaciones de Seguridad se encargan de realizar un seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.
- **Software base:** Listado de software definido para ser instalado al entregar un computador. Dicho listado es definido por la Dirección TICs y planteado como aplicaciones mínimas para adelantar las funciones dentro de la entidad.
- **Software de aplicación:** maneja multitud de tareas comunes y especializadas que un usuario desea realizar, como contabilidad, comunicación, procesamiento de datos y procesamiento de textos.
- **Software libre:** Es software donde los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar o mejorar el software. Este tipo de software debe ser autorizado por las áreas de Tecnología e Infraestructura.
- **Software:** Información organizada en forma de sistemas operativos, utilidades, programas y aplicaciones que permiten que los computadores funcionen. Consiste en instrucciones y códigos cuidadosamente organizados escritos por programadores en cualquiera de los diferentes lenguajes de programación especiales. El software se divide comúnmente en dos categorías principales: Software del sistema: controla las funciones básicas (e invisibles para el usuario) de un computador y generalmente viene preinstalado con la máquina.
- **Soportes físicos:** Documentos en soporte físico (cartas, informes, normas, contratos) y en medios de almacenamiento físico.
- **Spam:** Se denomina correo electrónico basura (en inglés también conocido como junk-mail o spam) a una cierta forma de inundar la Internet con muchas copias (incluso millones) del mismo mensaje.
- **Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.
- **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.
- **Spyware:** El software espía es un software que se instala en un

dispositivo informático sin que el usuario final lo sepa. Dicho software es controvertido porque, a pesar de que a veces se instala por razones relativamente inocuas, puede violar la privacidad del usuario final y tiene el potencial de ser objeto de abuso.

- **Tecnología:** Corresponde a los equipos, sistemas de información, procesos y procedimientos utilizados para gestionar la información y las comunicaciones.
- **Teletrabajo:** Una forma de organización laboral, consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información para el contacto entre el trabajador y ETB, sin requerirse la presencia física del trabajador en un sitio específico.
- **Terceros:** Toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.
- **TI (Tecnología de la Información):** Conjunto de herramientas, procesos y metodologías (como codificación o programación, comunicaciones de datos, conversión de datos, almacenamiento y recuperación, análisis y diseño de sistemas, control de sistemas) y equipos asociados empleados para recopilar, procesar y presentar información. En términos generales, TI también incluye automatización de oficinas, multimedia y telecomunicaciones.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Titular de la información:** persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
- **Transacciones:** se deben identificar cuáles transacciones realiza el sistema, de qué manera las realiza y dónde se almacenan.
- **Transparencia:** Cualidad de la actividad pública que consiste en la apertura del sector público a la divulgación de información acerca de su gestión.
- **Transversales:** Son los procesos que se encargan de apoyar al negocio en temas estratégicos, administrativos y de operación.
- **Tratamiento de riesgos:** a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.
- **Trazabilidad:** Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.
- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- **TXT:** el archivo informático compuesto únicamente por texto sin formato.
- **Unidad de Conservación:** Medio utilizado para archivar la documentación.
- **Unidades de almacenamiento:** Dispositivos que se usan para guardar y localizar la información de forma ordenada para acceder a ella cuando se necesario. Pueden ser internos como el disco duro o externos como memorias USB, unidades de CD, unidades de DVD, unidades de Blu-ray

(BD), tarjetas de memoria SD.

- **USB (Universal Serial Bus):** Puerto Serial Universal del computador al cual se pueden conectar los periféricos.
- **Usuario informático:** Puede ser un humano o una computadora que tiene permisos de acceso a un sistema de información en el cual fue previamente agregado con algunos privilegios y ciertas restricciones.
- **Usuarios:** personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad, por ejemplo: servidores, contratistas, terceros, proveedores, entre otros.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Valor público:** Se relaciona con el fin último del uso de la tecnología en la relación del Estado, ciudadanos, usuarios y grupos de interés. El valor público se relaciona con el desarrollo social, la gobernanza, la garantía de derechos, la satisfacción de necesidades, la prestación de servicios de calidad y el mejoramiento de las condiciones de vida de la sociedad.
- **Valoración de riesgos:** Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- **Virus:** Un virus informático es un código malicioso que se replica copiándose en otro programa, documento o sector de arranque del computador y cambia el funcionamiento de este. El virus requiere que alguien, consciente o inconscientemente, disemine la infección sin el conocimiento o permiso del usuario o administrador del sistema.
- **VPN** (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.
- **Vulnerabilidad Crítica:** Una vulnerabilidad crítica es una característica o una falla de un software que permite ejecutar código de forma remota, obtener privilegios de administrador o filtrar datos sensibles de ese sistema.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOI/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.
- **Wan:** Wide Área Network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).
- **Wi•Fi:** Es un protocolo de red inalámbrica que permite a los dispositivos comunicarse sin cables de Internet. Es técnicamente un término de la industria que representa un tipo de protocolo de red de área local (LAN) inalámbrica basado en el estándar de red IEEE 802.11. Este es el medio más popular para comunicar datos de forma inalámbrica, dentro de una ubicación fija. Es una marca registrada de Wi-Fi Alliance, una asociación internacional de compañías involucradas con tecnologías y productos

LAN inalámbricos.

4. Marco Normativo y Documentación Técnica

Para consultar el Marco Normativo y Documentación Técnica aplicable a la presente política por favor remitirse al *Listado Maestro de Documentos DTIC*

5. Objetivos

5.1. Objetivo General

Establecer los lineamiento y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP por todos los colaboradores, funcionarios y contratistas, para proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información (grupos de valor, información, procesos, infraestructura de TI) de Empresas Públicas de Armenia ESP, teniendo en cuenta los objetivos de la entidad, la estructura definida, bajo el marco del Modelo Integrado de Planeación y Gestión, los procedimientos y los requisitos legales vigentes en la entidad.

5.2. Objetivo Especifico

En el marco de la Política *de* Seguridad y Privacidad de la Información se plantean los siguientes objetivos específicos:

- Establecer el ecosistema de seguridad y privacidad de la información con los involucrados de tipo Core, Directo e Indirecto.
- Establecer un modelo de gestión de gobierno del Sistema de Seguridad y Privacidad de la Información para Empresas Públicas de Armenia ESP.
- Establecer los componentes significativos asociados a la Política de Seguridad y Privacidad de la Información.
- Describir las buenas prácticas aplicables a las condiciones actuales de Empresas Públicas de Armenia ESP para la gestión de Seguridad y Privacidad de la Información.
- Definir los enfoques y lineamientos de la *P*olítica *de* Seguridad y Privacidad de la Información.
- Definir parámetros de estrategias de EIC (Educación, Información y Comunicación) para la gestión de la Seguridad y Privacidad de la

Información.

- Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basados en la norma ISO 27035.

6. Componentes de la Política *de* Seguridad y Privacidad de la Información

Esta Política de Seguridad y Privacidad de la Información describe las directrices, normas, lineamientos y buenas prácticas, con el propósito de gestionar la gobernanza del Sistema de Gestión de Seguridad y Privacidad de la Información, para el cuidado y protección de los activos de información de Empresa Publicas de Armenia *ESP*.

A continuación, se describen los componentes de esta política definida:

6.1. Principios de Seguridad y Privacidad de la Información

Los principios[2] definidos para la garantía de Seguridad y Privacidad de la Información son en el marco de la presente política son:

Autenticidad: Principio que garantiza veracidad en la autoría de la información. Sin embargo, no garantiza la veracidad del contenido de la información. La autenticidad garantiza la veracidad del autor, de quién produjo la información, sin importar si el contenido es verdadero o falso.

[2] Definición tomada y ajustada de: https://ostec.blog/es/seguridad-informacion/principios-basicos-de-la-seguridad-de-la-informacion/

Integridad: La integridad de la información hace referencia a que la información que se encuentra almacenada en los dispositivos o la que se ha transmitido por cualquier canal de comunicación **no ha sido manipulada por terceros** de manera malintencionada. Esto garantiza que la información no será modificada por personas no autorizadas.

Las personas con los privilegios para acceder a la información de propiedad de Empresas Públicas de Armenia ESP deben garantizar el uso de buenas prácticas para preservar la integridad de la misma. De la misma manera, la entidad debe garantizar el uso de buenas prácticas que permita resguardar y proteger la integralidad de la información contra modificaciones no autorizadas, realizadas con o sin intención, y en caso tal garantizar su recuperabilidad.

Confidencialidad: La confidencialidad, en el contexto de seguridad de la información, es la garantía de que determinada información, fuente o sistema esté disponible solo a personas previamente autorizadas. Eso significa que siempre que una información confidencial es accedida por un individuo no autorizado, intencionalmente o no, ocurre lo que se llama: violación de la confidencialidad. La violación de la confidencialidad, dependiendo del tipo de información filtrada, puede ocasionar daños inestimables a la empresa, sus clientes e incluso al mercado.

Disponibilidad:[3] Disponibilidad de la información Hace referencia a que Empresas Públicas de Armenia ESP debe garantizar siempre la disponibilidad de la información a las personas con los privilegios de acceso según el esquema de gobierno y seguridad de la información establecido en la entidad.

Estos privilegios de acceso establecen acciones como acceso para ver, acceso para modificar, acceso para compartir, acceso para elimina, así como su recuperabilidad, en caso de que ocurra un incidente de seguridad que cause su pérdida o corrupción. Es decir; permite que la información esté disponible cuando sea necesario.

[3] Tomado y modificado de: https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

Los principios anteriormente definidos fueron el resultado de la exploración de benchmarking realizada para establecer el estado del arte y las buenas prácticas en Seguridad y Privacidad de la Información.

6.2. Ecosistema de Involucrados Empresas Públicas de Armenia ESP

Empresas Públicas *de Armenia ESP* describe a continuación su ecosistema de involucrados:

- **Involucrado Core:** Fundamentales en la cadena de valor de Empresa Públicas de Armenia ESP, los necesarios para garantizar servicios.
- **Involucrado Directo:** Relevantes en el entorno de negocio, pueden ser pares, entidades que complementan servicios.
- **Involucrado Indirecto:** Involucrados en el proceso de regulación del sector, inspección, vigilancia y control.

Involucrados Core	Involucrados Directos	Involucrados Indirectos
• Consumidores (Establecimientos residenciales y Establecimientos comerciales) • Proveedores de materiales e insumos para garantizar servicios primarios • Colaboradores (funcionarios y contratistas) • Alcaldía de Armenia	• Pares (Empresas Públicas del Quindío) • Proveedores de insumos secundarios. • Entidades públicas del territorio. • Entidades privadas del territorio.	• Presidencia de la República • Congreso de la república. • Contralorías • Procuraduría • Entidades certificadoras de calidad. • Función Publica • Ministerios

Fuente: Elaboración Propia

6.3. Estructura de gobierno en Seguridad y Privacidad de la Información

La gestión de las competencias y capacidades en Seguridad y Privacidad de la Información requiere de parte de la entidad definir un conducto regular para la toma de decisiones, así como para la asignación y seguimiento de las responsabilidad y funciones que demanda este tema de vital importancia para garantizar la protección del Know-How de la entidad descrita en los activos de información.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con el comité de seguridad de la información (o quien haga sus veces) y del oficial de seguridad de la información.

Este componente define los roles y responsabilidades de la Seguridad de la Información, específicamente con respecto a la protección de los activos de información.

La gobernanza en Seguridad y Privacidad de la Información para la operación y cumplimientos de Empresas Públicas de Armenia ESP se describe en la siguiente estructura:

N°	Responsabilidad	Área/Procesos
1	Responsable de Gobierno y Gestión. – Revisar y proponer al gerente general, para su aprobación, la Política de Seguridad y Privacidad de la Información. – Supervisar la implementación de los lineamientos, procedimientos y planes asociados a la Política de Seguridad y Privacidad de la información. – Proponer estrategias y soluciones específicas para la incorporación de los controles necesarios para implementar las políticas establecidas y la debida solución de las situaciones de riesgo detectadas. – Reportar al Director TICs, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución. – Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones.	Comité Institucional de Gestión y Desempeño CIGD
2	Responsable de Garantizar Cumplimiento. – Aprobar *los* lineamientos actualizados y nuevos aplicables de Seguridad y Privacidad de la información. – Evaluar el proceso de gestión de seguridad de la Información. – Definir las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información. – Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información.	Gerencia General
3	Gestión estratégica y técnica en Seguridad y Privacidad de la Información - Gestión de la Política. - Gestión de Procedimientos e Instrumentos. - Gestión del Plan de Seguridad y Privacidad de la Información. - Garantizar el cumplimiento de los requerimientos de seguridad y privacidad de la información que demanda la presente política y demás documentos vinculantes normativos y técnicos de orden territorial y nacional. - Formulación de iniciativas y planes de contingencia sobre niveles de riesgos identificados y reportados. - Establecer mecanismos que permita la gestión de los incidentes reportados y la trazabilidad de los mismos. - Establecer canales de comunicación con proveedores de TI correspondientes para la garantía de cumplimiento de la política. - Socialización a los respectivos involucrados de las situaciones presentadas en gestión de incidentes. - Identificar riesgos asociados a la gestión de incidentes de	Dirección de Tecnologías de la Información y las Comunicaciones.

N°	Responsabilidad	Área/Procesos
	seguridad - Contactar a las autoridades y/o grupos especializados en respuesta a incidentes para las labores de coordinación y apoyo. - Monitorear el estado, nivel de aplicación de la política en la entidad. - Organizar las actividades del Comité *Institucional de Gestión y Desempeño CIGD* en materia de seguridad de la información. - Estar en comunicación activa con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información. - Apoyar a los diferentes procesos institucionales en la adopción del sistema de gestión de seguridad de la información. - Mantener contacto con las autoridades en materia de ciberseguridad para conocer de primera mano indicios o alertas en materia de seguridad de la información y recibir el apoyo de grupos de respuesta ante incidentes de seguridad de la información. - Mantener contacto con grupos de interés especial en materia de seguridad de la información para asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa. - Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades. - *Diseño de estrategias de EIC para capacitar a los colaboradores y proveedores.*	
4	- Garantizar el cumplimiento legal de la Política de Seguridad *y Privacidad* de la Información en la entidad. - Trabajar de la mano con la Dirección TICs en la definición y gestión de los requerimientos estatuarios, reguladores y contractuales pertinentes en aspectos de seguridad y privacidad de la información. - Asesorar legalmente en las acciones de Seguridad y Privacidad de la Información que se requieran en Empresas Públicas de *Armenia ESP* y determinar las pautas legales que permitan cumplir con los requerimientos legales en esta materia. - Asegurar que los incidentes que involucren la fuga de información sensible son manejados con base en las regulaciones aplicables. - Determinar las consecuencias jurídicas que se podrán presentar sobre incumplimiento o desacato de las responsabilidades en la gestión de eventos e incidentes de TI. - Orientar y asistir en acciones de adquisición de evidencia forense requerida - Seguimiento y monitorio a eventos e incidentes.	Dirección Jurídica y Secretaria General
5	- Fomentar la participación de los colaboradores (funcionarios y contratistas) y proveedores en las acciones de Educación, Información y Comunicación que definan.	Gestión del Talento Humano

N°	Responsabilidad	Área/Procesos
	- Incluir en el plan de capacitación anual temáticas asociadas a Seguridad y Privacidad de la Información. - Garantizar cumplimientos de los lineamientos, procedimientos y planes asociados a la Seguridad y Privacidad de la Información del Talento Humano. - Notificar a todo el Talento Humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. - Apoyar en la resolución de conflictos internos asociados con violaciones u omisiones de la presente política.	
6	- Difusión de información de carácter público a grupos de interés referente a la Seguridad y Privacidad de la Información. - Difusión de material publicitario e informativo sobre las responsabilidad y gestión de la Seguridad y Privacidad de la Información ante los grupos de interés.	Dirección de Comunicaciones
7	- Acompañar en la formulación y articulación de los planes de Seguridad y Privacidad de la Información con la ruta estratégica del negocio.	Dirección de Planeación Corporativa
8	– Seguimiento al desempeño en la gestión de *acciones de Seguridad y Privacidad de la Información* – Realizar auditorías asociadas al cumplimiento de los establecido en esta política – Reportar a los responsables el estado de cumplimiento de los lineamientos, procedimiento y uso adecuado de los instrumentos de seguridad de la información establecidos por esta política y los documentos de estructura y gobierno vinculantes. – Recomendar acciones de mejora frente a los hallazgos y vulnerabilidades identificadas en las auditorias e informarlas al *Comité Institucional de Gestión y Desempeño CIGD*	Dirección Control de Gestión
9	– Caracterizar y clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad de los mismos, documentar y mantener actualizada la clasificación. – Definir los permisos de acceso para cada colaborador en su proceso teniendo en cuenta sus funciones y competencia. – Informar a la Dirección TICs cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles. – Proponer y/o implementar medidas de seguridad pertinentes para evitar vulnerabilidades e incidentes con los activos de información a su cargo. – Socializar y aplicar las cláusulas de confidencialidad pertinentes para el personal y proveedores a su cargo. – Apoyar y replicar la socialización de orientaciones que se presenten desde la alta dirección en materia de seguridad de la información. – Ejercer liderazgo y compromiso en la aplicación de la política de Seguridad *y Privacidad* de la Información.	Procesos propietarios de activos de información
10	– Informar a la Dirección TICs cuando detecte cualquier incidente de seguridad de la información. – Sugerir controles o contramedidas para el tratamiento de	Administradores de los Sistemas

N°	Responsabilidad	Área/Procesos
	incidentes que se presentes en seguridad y privacidad de la información. – Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios.	de Información y Plataforma de TI
11	- Aplicar buenas prácticas en Seguridad de la Información. - Asistir a los espacios de formación y capacitaciones citados. - Apropiar y cumplir con los establecido en los espacios de capacitación. - Conocer, divulgar, cumplir y hacer cumplir la Política *Interna* de Seguridad y Privacidad de la Información vigente, los procedimientos vinculantes y las normas asociadas. - Hacer buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones y responsabilidades, la relación de estos debe estar registrada en el Sistema de Inventarios de la EPA. - Cumplir con los lineamientos de gestión de seguridad y privacidad de la información. - Garantizar el buen manejo y custodia de la información almacenada en el equipo de cómputo y periféricos asignados. - Dar el adecuado uso y cumplimiento a los activos de información mapeados en la entidad. - Facilitar la revisión del equipo de cómputo, periféricos, sistemas de información y accesos asignados para el seguimiento de la adecuada gestión y uso según los establecido en la presente política - Mantener en buen estado los equipos de cómputo y periféricos que le sean asignados.	Todos los procesos.
12	– Abstenerse de acceder a espacios restringidos, manipular dispositivos e información que no estén en su rango de acceso y manipulación sin la previa autorización de manejo y gestión. – Para el acceso, excepcional a recursos y activos de información es fundamental la autorización de acceso de los responsables del activo, siguiendo los parámetros establecidos en esta política. – Cumplir *los lineamientos* de seguridad y privacidad de la información cuando se les autorice acceso a los activos de información institucionales. – Usar únicamente las redes de acceso a invitados, la cual restringe el acceso solo a internet. - Abstenerse de cualquier manipulación en los activos de información sin contar con las indicaciones y acompañamiento del responsable de la seguridad del activo de información comprometido.	Visitantes

Fuente: Guía Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información. Elaborado por el MinTIC.

7. Enfoques de la Política Seguridad y Privacidad de la Información

A continuación, se describen los lineamientos de cumplimiento para la Política *Interna* Seguridad y Privacidad de la Información de Empresas Públicas de Armenia ESP, clasificados en 08 enfoques de aplicación.

Enfoques de la Política de Seguridad y Privacidad de la Información

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
Política General	Lineamientos Generales.		14	Todos
Enfoque Gestión Humana	Lineamientos sobre la vinculación y desvinculación de servidores públicos		8	Subgerencia Administrativa | Gestión Talento Humano
	Lineamientos sobre la vinculación y desvinculación de los pasantes/practicantes		7	
	Lineamientos sobre la gestión de contratistas frente a la seguridad y privacidad de la información		8	
	Lineamientos sobre el control de acceso a servidores públicos, contratistas, pasantes y visitantes		6	
	Lineamientos sobre la circulación interna de servidores públicos, contratistas, pasantes y visitantes.		4	
	Lineamientos sobre los usuarios de la información		7	
	Lineamientos sobre el control de acceso del personal de vigilancia		6	
	Lineamientos sobre la seguridad para contexto de teletrabajo		*8*	
	Lineamientos sobre el acuerdo de Confidencialidad del personal vinculado laboralmente a la entidad		7	
	Lineamientos sobre los procesos disciplinarios en temas de Privacidad y Seguridad de la Información		3	
Enfoque Seguridad física, infraestructura TI y Dispositivos	Lineamientos sobre la seguridad física y del entorno		5	Subgerencia Administrativa | Gestión de Recursos
	Lineamientos sobre controles de acceso físico y a áreas restringidas.		8	
		Referente a Centros de cómputo y cableado.	9	
	Lineamientos sobre la gestión de seguridad de las redes		4	
		Referente a control de acceso a redes y servicios de red.	6	
		Referente a la separación de en las redes y redes inalámbricas	7	
	Lineamientos sobre el manejo y uso de recursos tecnológicos		--	

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
		Referente a la ubicación y protección de los equipos	2	
		Referente a la disponibilidad de equipo de cómputo.	8	
		Referente a los usos aceptables del servicio TI	16	
		Referente al uso y manejo de equipos de cómputo en su espacio de trabajo	6	
		Referente al uso y manejo de dispositivos móviles.	8	
		Referente a la seguridad de los equipos fuera de las instalaciones.	5	
Enfoque Software y Sistemas de Información	Lineamientos sobre Administradores de Software y Sistemas de Información		3	Dirección de las Tecnologías de la Información y las Comunicaciones
	Lineamientos sobre el control de contraseñas		12	
		Referente a la seguridad de las contraseñas	21	
		Referente a la protección de contraseñas	13	
		Referente al cambio de contraseñas	4	
	Lineamientos sobre el uso adecuado de Software y Sistemas de Información		--	
		Referente al manejo de los sistemas de información digitales.	6	
		Referente a uso del software legal y derechos de autor	4	
		Referente a el control de virus.	9	
	Lineamientos sobre el desarrollo del software para la Empresas Públicas de Armenia ESP		7	
		Referente al desarrollo seguro, pruebas y soporte.	7	
Enfoque Datos, Información y Almacenamiento	Lineamiento sobre la clasificación, uso y manejo de información confidencial		--	Dirección de las Tecnologías de la Información y las Comunicaciones
		Referente a la clasificación y	3	

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
		caracterización de la información		
		Referente al etiquetado y manejo de la información.	10	
		Referente a la confidencialidad de la información.	17	
		Referente a los controles criptográficos	*4*	
	Lineamientos sobre la gestión de almacenamiento		--	
		Referente al almacenamiento en equipos de cómputo y red local.	15	
		Referente al almacenamiento en la nube	3	
		Referente al borrado seguro de información	7	
		Referente a la transferencia de información en medios físicos.	6	
	Lineamientos sobre la propiedad de la información		--	
		Referente a la propiedad intelectual de activos de información	3	
		Referente a la gestión de activos de información.	7	
	Lineamientos sobre las copias de respaldo de información (Backup)		--	
		Referente al gobierno y gestión de las copias y respaldo de información (backup)	12	
		Referente al proceso de copias y respaldo de información (Backup)	19	
		Referente al registro de respaldo de información.	6	
		Referente a al respaldo de información para usuarios finales.	7	

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
Enfoque Canales de Comunicación	Lineamientos sobre el manejo de internet		--	Dirección de Comunicaciones
		Referente a la gestión del servicio de internet.	11	
		Referente a los usos aceptables del servicio	15	
		Referente a los usos no aceptables del servicio.	6	
	Lineamientos sobre el uso y manejo de correo electrónico		--	
		Referente a la gestión del servicio de correo electrónico.	25	
		Referente a los usos aceptables del servicio.	7	
		Referente a los usos NO aceptables del servicio.	20	
	Lineamientos sobre el uso y manejo de redes sociales		--	
		Referente a la gestión del servicio de cuentas de redes sociales de Empresas Públicas de Armenia ESP	8	
		Referente a los usos aceptables del servicio de Redes Sociales	4	
		Referente a los usos NO aceptables del servicio de Redes Sociales	16	
Enfoque Gestión Documental Física y Electrónica	Lineamientos sobre el manejo integral con gestión documental		4	Subgerencia Administrativa | Gestión de Recursos
	Lineamientos sobre el manejo de documentos electrónicos		--	
		Referente al manejo general de documentos electrónicos	6	
Enfoque Gestión de Riesgos e Incidentes	Lineamientos sobre el mapeo y caracterización		11	Todos los procesos
	Lineamientos sobre la priorización y diagnóstico preliminar		5	
	Lineamientos sobre la resolución y recuperación		8	
	Lineamientos sobre el cierre y seguimiento de incidentes		4	

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
Enfoque Auditoria Gestión del Cambio y Mejoramiento Continuo	Lineamientos sobre la gestión de evento en TI		--	Dirección Control Gestión
		Referente al registro de evento de TI	3	
		Referente al registro del administrador y del operador	2	
		Referente a la sincronización de relojes	1	
	Lineamiento sobre la Gestión de Cambios		10	
	Lineamientos sobre la continuidad del negocio		7	

Política General

La Dirección TICs de Empresas Públicas de Armenia ESP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para Empresas Públicas de Armenia ESP, la protección de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

Este sistema de gestión de seguridad de la información es creado con la intención organizacional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.

- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Empresas Públicas de Armenia ESP
- Garantizar la continuidad del negocio frente a incidentes.

Empresas Públicas de Armenia ESP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del Empresas Públicas de Armenia ESP y la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

Lineamientos Generales

A continuación, se establecen los 14 lineamientos de seguridad que soportan el SGSI de Empresas Públicas de Armenia ESP:

1. Empresas Públicas de Armenia ESP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
3. Empresas Públicas de Armenia ESP se compromete a fomentar y estimular la cultura y buenos hábitos en el uso y apropiación del personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.
4. Empresas Públicas de Armenia ESP protegerá la información generada, procesada resguardada por los procesos de negocio y activos de

información que hacen parte de los mismos.

5. Empresas Públicas de Armenia ESP protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
6. Empresas Públicas de Armenia ESP protegerá su información de las amenazas originadas por parte del personal.
7. Empresas Públicas de Armenia ESP protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
8. Empresas Públicas de Armenia ESP controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
9. Empresas Públicas de Armenia ESP implementará control de acceso a la información, sistemas y recursos de red.
10. Empresas Públicas de Armenia ESP garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
11. Empresas Públicas de Armenia ESP garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
12. Empresas Públicas de Armenia ESP garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
13. Empresas Públicas de Armenia ESP garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
14. Empresas Públicas de Armenia ESP garantizará la gestión de los riesgos de los activos de información considerando los niveles de tolerancia en la categorización de dicho activo.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Enfoque Gestión Humana

La Garantía de una buena implementación del Sistema de *Seguridad y* Privacidad de la Información está muy conectada al buen acompañamiento y gestión realizada al talento humano de la entidad contemplando acciones dirigidas a la transferencia, uso y apropiación de estos los lineamientos por parte de todo el personal, es allí donde podremos decir claramente que estamos en un proceso de incorporación de capacidades en seguridad y privacidad de la información.

Siendo consecuentes con esto, a continuación, se describen los lineamientos asociados a la Gestión Humana de Empresas Públicas de Armenia ESP para dar cumplimiento a lo establecido en el aspecto de Seguridad y Privacidad de la Información.

Estos lineamientos describen las condiciones de interacción, atención, cuidado, seguimiento y control del personal de la entidad.

Lineamientos sobre la vinculación y desvinculación de servidores públicos:

1. La seguridad de los recursos humanos debe ser gestionada desde el proceso de Gestión del Talento Humano y sus procedimientos vinculantes.
2. *La* Gestión del talento humano deberá garantizar procesos rigurosos de selección de personal que cumplan con las capacidades y competencias asociada a los perfiles requeridos y estos deberán establecer las condiciones mínimas de selección y vinculación en aspecto de seguridad y privacidad de la información.
3. Gestión del talento humano y Secretaria Jurídica y Administrativa son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales judiciales *y demás aplicables* y que se anexe la documentación requerida para la contratación.
4. La gestión del talento humano debe contemplar lineamientos que permitan la transferencia, capacitación, uso y apropiación de buenas prácticas y hábitos de seguridad y privacidad de la información.
5. Todo servidor público oficialmente vinculado deberá recibir una inducción sobre los lineamientos de Seguridad y Privacidad de la Información.
6. Todos los servidores públicos cuando sea el caso, que trabajan para Empresas Públicas de Armenia ESP deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y *P*rivacidad de la Información.
7. Al momento de la finalización de su relación laboral el servidor público debe cumplir con los requisitos del código único disciplinario en donde los servidores públicos aceptan la obligación legal de mantener la reserva de la información bajo su responsabilidad.

8. Todo el personal vinculado a la Entidad debe aceptar formalmente el cumplimiento de *todas* las *P*olíticas de operación institucionales y los procedimientos del sistema integrado de planeación y gestión.

Lineamientos sobre la vinculación y desvinculación de los pasantes/practicantes:

1. Los estudiantes en condición de pasantes o practicantes deberán vincularse a la entidad siguiendo los procedimientos establecidos desde Gestión del Talento Humano.
2. El director del proceso a donde sea vinculado el practicante o pasante será el responsable de asignar el supervisor.
3. Cualquier acto que realice el pasante/practicante en la entidad deberá estar aprobada previamente por el supervisor, este será el encargado de asignar las responsabilidades y realizar seguimiento al cumplimiento de las mismas según su propósito de vinculación.
4. Después de completado el proceso de vinculación y argumentando necesidad de uso, el supervisor deberá solicitar por medio de la mesa de ayuda la creación, actualización y eliminación de cuentas de usuario y asignación de privilegios de uso de equipos de cómputo para el cumplimiento de las actividades que le sean asignadas.
5. Todo pasante/practicante oficialmente vinculado deberá recibir una inducción sobre los lineamientos de Seguridad y Privacidad de la Información.
6. Todos los pasantes/practicante cuando sea el caso, que trabajan para Empresas Públicas de Armenia ESP deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información.
7. Todo pasante/practicante oficialmente vinculados deberá aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de *S*eguridad y *P*rivacidad de la Información.

Lineamientos sobre el control de acceso a servidores públicos, contratistas, pasantes y visitantes:

1. Todo el personal de la entidad (servidores públicos) deberán estar debidamente identificados mientras se encuentren realizando labores dentro o fuera de las instalaciones de Empresas Públicas de Armenia ESP.
2. Portar una identificación ajena a la suya, será considerado como suplantación de identidad y deberá notificarse a Gestión del Talento Humano.
3. Los contratos *con* proveedores deben describir claramente las condiciones asociadas a la propiedad, confidencialidad y no divulgación de la información.

4. Gestión del Talento Humano deberá actualizar en la periodicidad que lo considere el listado de personal contratista y pasante que se encuentre vinculado a la entidad y compartirlo con las áreas de las diferentes sedes de Empresas Públicas de Armenia ESP.
    a. Dicho listado deberá describir nombre completo, identificación, área primaria de vinculación y supervisor.
5. Empresas Públicas de Armenia ESP será la responsable del tratamiento de los datos personales del personal vinculado (vigente o retirado) y podrá hacer de los mismos únicamente para las finalidades establecidas en La Política de tratamiento de datos personales aprobada por la entidad y publicado en la página web *www.epa.gov.co*.
6. Los contratistas que realicen actividades en cualquiera de las instalaciones de la entidad deberán estar debidamente identificado y portando los atuendos y utensilios que les exige la normatividad para tal fin.

Lineamientos sobre la circulación interna de servidores públicos, contratistas, pasantes y visitantes:

1. El Área de Talento Humano, es el responsable de solicitar, actualizar y retirar los carnés de los servidores públicos y pasantes. Los supervisores de contratos son los responsables de solicitar y devolver los carnés al área de *Gestión del* Talento Humano de los contratistas a su cargo.
2. Cualquier servicio externo contratado que involucre intervención en espacio de cualquiera de las sedes de Empresas Públicas de Armenia ESP, deberá contar con acompañamiento permanente hasta que se finalice el servicio prestado.
3. Todo ingreso de servidores públicos, contratistas y pasantes en horario no hábil, debe ser notificado previamente al proceso pertinente de la administración municipal, dado el caso que sean las otras sedes de la entidad, será referencia al proceso correspondiente.

Lineamientos sobre los usuarios de la información

1. Usar la información de Empresas Públicas de Armenia ESP únicamente para propósitos del negocio autorizado y en cumplimiento de sus responsabilidades.
2. Abstenerse de compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial con personal fuera de los rangos de acceso y privilegios establecidos.
3. Abstenerse dejar apuntes y/o almacenar en lugares visibles las contraseñas de acceso a los sistemas de información y plataformas de TI de la entidad.

4. Apropiar y acatar los lineamentos de clasificación y categorización de los activos de información.
5. Restringir el acceso a los equipos de cómputo, portátiles y demás periféricos que permitan el acceso a activos de información mientras no estén en uso y al momento de ausentarse de los mismos.
6. Toda impresión que se realice sobre información confidencial o de cuidado especial deberá ser recolectada al momento de generarlas.
7. Bajo ninguna circunstancia está permitida:
    - La divulgación, cambio, retiro o eliminación no autorizada de información de la Entidad, ya sea que esté almacenada en medios físicos removibles, como USB, cintas magnéticas, entre otros.
    - La descarga, instalación y uso de software no licenciado en los recursos tecnológicos.
    - La copia de software licenciado a Empresas Públicas de Armenia ESP para utilizar en computadores personales, ya sea en su domicilio o en cualquier otra instalación y/o entregarlos a terceros.
    - La reserva, conservación, almacenamiento, generación de copias de ningún tipo de activos de información para uso fuera de los propósitos de la entidad.

Lineamientos sobre el control de acceso del personal de vigilancia:

1. El personal de vigilancia debe estar debidamente uniformado.
2. El personal de vigilancia debe asegurarse por medio de observación que ningún funcionario, contratista y visitante se encuentren en estado de ebriedad, bajo el efecto de sustancias alucinógenas, armado o en cualquier estado dudoso que pueda afectar la seguridad de la Entidad e informar cualquier novedad al área de Gestión del Talento Humano.
3. El personal de vigilancia debe solicitar a todos los visitantes un documento de identificación personal vigente, de preferencia con foto, con el fin de verificar los datos y solicitar confirmación telefónica con la persona o área que visita. Una vez realizada la verificación el documento de identificación será devuelto al visitante de forma inmediata.
4. El personal de vigilancia debe registrar la entrada o salida los equipos de cómputo, portátiles y demás equipos electrónicos en el libro de registro de elementos ubicado en la recepción.
5. Empresas Públicas de Armenia ESP bajo ninguna circunstancia se responsabiliza por los equipos de cómputo, portátiles, equipos electrónicos y otros objetos personales que ingresen a las instalaciones de la entidad. Por lo tanto, la custodia y cuidado de estos elementos es de total responsabilidad de su propietario.
6. El personal de vigilancia debe asegurar que ningún visitante salga de las instalaciones de la entidad con activos de información de la entidad, sin el

debido formulario de autorización que otorga el responsable del activo de información.

Lineamientos sobre la seguridad para contexto de teletrabajo:

- La entidad ha adoptado una política de teletrabajo que es conforme con los requerimientos de la Ley 1221 de 2008. La política institucional de teletrabajo se describe en el Sistema Integrado de y Gestión
- Gestión del Talento Humano es el responsable de realizar y/o coordinar la visita domiciliaria, pruebas de meritocracia y ofimática de los servidores públicos que se postulan a teletrabajo.
- Gestión del Talento Humano es responsable de realizar las pruebas de meritocracia del postulante a teletrabajo.
- Gestión del Talento Humano es el responsable de realizar la prueba de ofimática del postulante a teletrabajo. La evaluación de las pruebas de ofimática es responsabilidad La Dirección TICs.
- Gestión del Talento Humano es el responsable de realizar visita domiciliaria, para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar, sean las adecuadas en cuanto a iluminación, ruido, ventilación, puesto de trabajo, ergonomía y ubicación de los elementos del lugar donde realizaría el teletrabajo.
- Gestión del Talento Humano son los responsables de realizar visita domicilia para certificar que las instalaciones donde va a laborar el servidor público que se postula a teletrabajar sean las adecuadas en cuanto a equipo de cómputo, internet, red eléctrica, teléfono (fijo o móvil), software y antivirus instalado y debidamente licenciado.
- Es responsabilidad del teletrabajador, acatar la Política de Seguridad y privacidad de la Información establecida por la entidad.
- Es responsabilidad del teletrabajador cumplir con los controles técnicos que defina la Dirección TICs para garantizar la seguridad en las actividades de teletrabajo incluido:

    a. Utilizar únicamente los equipos autorizados por *EPA* para tener acceso a los sistemas de información e infraestructura tecnológica institucional.
    b. Asegurar su acceso Internet local con contraseña fuerte siguiendo los lineamientos de seguridad institucionales
    c. Conectarse a la red local institucional únicamente mediante conexión de red privada virtual autorizada para tal fin.
    d. Limitar el uso de familiares, amigos o desconocidos a los equipos de cómputo utilizados para las actividades de teletrabajo.
    e. Reportar a la mesa de servicio, cualquier comportamiento sospechoso o inusual que se detecte cuando se realicen actividades de teletrabajo

f. Conocer y estar alerta a los tipos de amenazas informáticas socializadas por la *Entidad EPA* para evitar ser víctima de estafas o software malicioso.
g. En caso de utilizar equipos de propiedad personal para las actividades de teletrabajo, cumplir con los lineamientos de seguridad que determine la Dirección TICs para este tipo de dispositivos.

Lineamientos sobre Compromisos de Confidencialidad del personal vinculado laboralmente a la entidad:

1. Empresas Públicas de Armenia ESP debe establecer compromisos de confidencialidad para el intercambio de información con terceros que manipulen, requieran o provean información física y/o digital de carácter reservado.
2. La Secretaria Jurídica y Administrativa deben definir los parámetros y condiciones de los compromisos de confidencialidad para el intercambio de información entre Empresas Públicas de Armenia ESP y los grupos de interés.
3. Los acuerdos compromisos de confidencialidad que consideren pertinentes las partes responsables deberán incluir, entre otros aspectos que consideren, compromisos adquiridos por las partes, penalidades por incumplimiento, alcances del manejo de los activos de información compartidos, destino final de la de la información suministrada entre las partes una vez se haya culminado el contrato o convenio.
4. El área de Gestión Documental es el responsable de proporcionar los lineamientos para el intercambio de información física con terceros.
5. La Dirección TICs es el responsable de proporcionar los lineamientos para el intercambio de información digital con terceros de manera segura con el fin de proteger la información de manipulación, modificación y divulgación no autorizada.
6. El área de Gestión Contractual es el responsable de realizar el acompañamiento a las diferentes áreas de la entidad para que se garantice la inclusión de los compromisos de confidencialidad en los contratos o convenios que lo requieran.
7. Todo personal que labore en Empresas Públicas de Armenia ESP deberá firmar como parte de sus términos y condiciones iniciales de vinculación, un compromiso de Confidencialidad (Consultar registro GTH-R-026). Este compromiso ~~o~~ debe incluir la aceptación de la Política interna de Seguridad y Privacidad de la Información, el tratamiento de la información de la entidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen, reglamenten o complementen, así como el Decreto 1377 de 2013. Este documento debe ser archivado de forma segura por el área de Talento Humano y Contractual, según sea el caso.

Lineamientos sobre los procesos disciplinarios en temas de Privacidad y Seguridad de la Información

1. Cualquier incidente de seguridad y privacidad de la información presentados en la entidad deberá tener el tratamiento adecuado y establecido en el protocolo de gestión de incidentes del procedimiento de seguridad y privacidad de la información, con el fin de determinar sus causas y responsables.
2. Teniendo en cuenta los resultados presentados en el reporte de incidentes, se tomarán acciones y se realizará la respectiva notificación y traslado ante las instancias responsables.
3. Cualquier violación a los lineamientos de la *P*olítica de *S*eguridad y *P*rivacidad de la *I*nformación cometida por el personal de la entidad será aplicable lo establecido en la ley, el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.

Enfoque Seguridad física, infraestructura TI y Dispositivos

Este enfoque tiene el propósito de establecer las condiciones de operación para garantizar seguridad y privacidad de la información en temas de uso y privilegios de acceso a infraestructura física, la infraestructura TI y los dispositivos electrónicos en Empresas Públicas de Armenia ESP.

Lineamientos sobre la seguridad física y del entorno

1. El horario autorizado para recibir visitantes en las instalaciones de Empresas Públicas de Armenia ESP es de 8:00 am a 6:00 pm. En horarios distintos se requerirá de la autorización del director de proceso correspondiente.
2. Las credenciales de acceso a los sistemas de video vigilancia de todas las áreas que hagan parte de Empresas Públicas de Armenia ESP son de carácter estrictamente personal e intransferible; los operadores, servidores y contratistas de Empresas Públicas de Armenia ESP no deben revelar éstas a terceros ni utilizar claves ajenas.
3. Todas las entradas que utilizan sistemas de control de acceso deben permanecer cerradas y es responsabilidad de todo el personal y terceros autorizados evitar que las puertas se dejen abiertas.
4. La Gerencia General es la responsable de establecer y divulgar los lineamientos de seguridad física y seguridad de los servidores públicos, pasantes, contratistas y visitantes que laboren o visiten la entidad.

5. Los dispositivos portátiles, así como toda información confidencial de Empresas Públicas de Armenia ESP, independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales el personal o terceros responsable no se encuentre en su sitio de trabajo.

Lineamientos sobre controles de acceso físico y a áreas restringidas

1. La Dirección TIC deberá definir procedimientos e instructivos para proveer el acceso físico y lógico a los recursos físicos e informáticos, así como el perfilamiento de los usuarios autorizados para el cumplimiento de sus funciones, en las distintas sedes de la Empresa.
2. En las áreas seguras, en ninguna circunstancia se puede fumar, comer o beber.
3. Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un colaborador del proceso.
4. Capacitar al personal de limpieza sobre las precauciones mínimas a seguir durante el proceso de limpieza y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.
5. Todas las puertas exteriores deben ser cerradas con llave o estar aseguradas de otra forma durante las horas no hábiles.
6. Bajo ninguna circunstancia está permitido el ingreso de dispositivos móviles (Tablet, celulares, cámaras digitales, etc.) a áreas catalogadas como restringidas.
7. Toda área con acceso restringido debe disponer de controles de acceso especiales. El acceso a estas áreas debe ser únicamente para personal autorizado.
8. El personal responsable y encargados de áreas de acceso restringido deben asegurar que los controles de acceso como llaves de seguridad o cerraduras con claves maestras sean cambiadas cuando el control haya sido comprometido.

Referente a Centros de cómputo y cableado

1. El acceso al centro de cómputo de la Entidad está a cargo de La Dirección TICs, la cual es la responsable de enrolar, asignar tarjetas de acceso y dar los permisos de acceso según el caso, con el fin de garantizar la seguridad de los activos.
2. El acceso y mantenimiento de los centros de cableado es responsabilidad del Dirección TICs.
3. La Dirección TICs debe disponer en todo momento para el centro de

cómputo de un sistema de control de acceso, sistema de control de temperatura y humedad, un sistema de detección y extinción de incendios, un sistema de alimentación eléctrica ininterrumpida (UPS) y un sistema de vigilancia y monitoreo.

4. En el centro de cómputo y área de destinada al de control de operaciones, está prohibido realizar actividades que generen polvo, suciedad o partículas ya que pueden causar un mal funcionamiento de los equipos y generar falsas alarmas de incendio, dando como resultado el daño parcial o total de la infraestructura tecnológica y activos de información de la entidad.
5. No está permitido el ingreso al centro de cómputo y centros de cableado de líquidos, alimentos y material inflamable. Las áreas deben permanecer ordenadas, limpias y sin elementos que no correspondan con la operación del área.
6. Es responsabilidad de las personas autorizadas para el ingreso y mantenimiento del centro de cómputo y los centros de cableado mantener organizado los cables de voz, de datos y conexiones eléctricas (peinado).
7. La grabación de vídeo en las instalaciones del centro de cómputo con destino a terceras partes debe estar autorizada por el Director TICs.
8. Todo cambio dentro del centro de cómputo se debe tramitar a través del procedimiento de gestión de cambios establecido por la Dirección TICs. La autorización de ejecución de cambios en el centro de cómputo es responsabilidad de la Dirección TICs.
9. Mientras no se encuentren personas dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

Lineamientos sobre la gestión de seguridad de las redes

1. La Dirección TICs es la responsable de administrar y gestionar la red *de datos* de Empresas Públicas de Armenia ESP.
2. La Dirección TICs es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.
3. Empresas Públicas de Armenia ESP proporciona a los Colaboradores y Terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.
4. Se prohíbe conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por La Dirección TICs.

Referente a Control de Acceso a Redes y Servicios en Red

1. La Dirección TICs suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.
2. Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.
3. Toda actividad que requiera acceder a los servidores, equipos o a las redes de Empresas Públicas de Armenia ESP, se debe realizar en las instalaciones.
4. La conexión remota a la red de área local de Empresas Públicas de Armenia ESP debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por La Dirección TICs, que cuenta con el monitoreo y registro de las actividades necesarias.
5. La autenticación de usuarios remotos deberá ser aprobada por el jefe inmediato del usuario y bajo una solicitud con su respectivo formato a la mesa de ayuda de tecnología.
6. Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, se efectúa el seguimiento a los accesos realizados por los usuarios, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.

Referente a la separación en las redes y redes inalámbricas

1. Empresas Públicas de Armenia ESP debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.
2. Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.
3. Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.
4. Se deben establecer mecanismos de autenticación seguros para el acceso a la red.
5. Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.
6. La red inalámbrica será de uso exclusivo para usuarios de planta y contratistas con vínculo directo con Empresas Públicas de Armenia ESP. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación a la Mesa de Ayuda.

7. Para habilitar acceso a red inalámbrica se deberá hacer previa solicitud, justificación y autorización a la Mesa de Ayuda.

Lineamientos sobre el manejo y uso de recursos tecnológicos

Referente a la ubicación y protección de los equipos

1. La plataforma tecnológica (hardware, software) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.
2. Se debe garantizar control en el suministro eléctrico para eventuales incidentes que se presentes en donde se requiera su suspensión temporal en caso de emergencia. Así mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Referente a la disponibilidad de Equipos de cómputo

1. Todo dispositivo que requiera clave de acceso será entregado a la persona usuario y no podrá ser compartida, razón por la cual la responsabilidad de un posible mal uso recaerá sobre el servidor o contratista a quien se asignó dicho usuario y clave.
2. Empresas Públicas de Armenia ESP se reserva el derecho de monitorear el contenido y software instalado en los equipos de la Entidad para verificar el tipo de información, su uso y el licenciamiento del software instalado. De esta manera, contenidos de música, video, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del servidor o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
3. La Dirección TICs debe gestionar los mantenimientos preventivos y correctivos de la infraestructura del centro de cómputo y equipos de red.
4. Se deben realizar mantenimientos preventivos y correctivos a los equipos de cómputo de los usuarios, centros de cableado, periféricos, de comunicaciones y de seguridad de la entidad, de forma periódica según la programación establecida para cada vigencia.
5. Los equipos de cómputo y periféricos de Empresas Públicas de Armenia ESP deben conectarse a la red eléctrica regulada. En caso de no tener red eléctrica en el área, se debe disponer de un regulador externo.
6. Los equipos de cómputo de Empresas Públicas de Armenia ESP contarán con una herramienta de protección contra software malicioso instalado y permanentemente actualizado (tanto en su versión de software como su base de amenazas), la cual permitirá: i) activación toda vez que se inicie sesión en el dispositivo y debe permanecer siempre activo, ii) escanear en busca de amenazas en cualquier medio removible (pendrive, discos duros, etc.) cuando sea conectado a alguna estación de trabajo. iii)

detectar código malicioso y notificada automáticamente.

7. La Empresas Públicas de Armenia ESP dispondrá de una póliza que ampara los equipos de su propiedad en caso de daño o pérdida.
8. La empresa de seguridad es la encargada de ejercer vigilancia y control sobre los equipos eléctricos y electrofónicos de la entidad, que permanezcan en ella, o que ingresan o salgan de la misma.

Referente a los usos aceptables del servicio TI

Empresas Públicas de Armenia ESP asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los colaboradores y terceros de ser necesario. El uso adecuado de estos recursos se establece bajo los siguientes criterios:

1. Cada equipo de cómputo está configurado con el Hardware y Software básico necesario para su funcionamiento:
   - Sistema operativo: Windows o Linux.
   - Ofimática: Office 365 (Acces, Excel, OneNote, One Drive, Outlook, Power Point, Publisher, Word.)
   - Descomprimir Archivos: Winrar.
   - Antivirus.
   - Servicios en la nube Google Suite.
2. La instalación de software se encuentra bajo la responsabilidad la Dirección TICs y por tanto son los únicos autorizados para realizar esta actividad y toda solicitud debe realizarse por medio de la Mesa de Ayuda de Tecnología.
3. Si el Colaborador cuenta en su equipo de cómputo con aplicaciones diferentes a las antes mencionadas o con software no autorizado, se procederá a realizar la desinstalación sin previa autorización.
4. Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por La Dirección TICs.
5. La Dirección TICs es el responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en Empresas Públicas de Armenia ESP para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
6. Sólo el personal autorizado por la Dirección TICs podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de Empresas Públicas de Armenia ESP; las conexiones establecidas para este fin utilizan los esquemas de seguridad establecidos por la entidad.

7. Los Colaboradores y Terceros de la Entidad son responsables de hacer buen uso de los recursos tecnológicos de Empresas Públicas de Armenia ESP
8. No está permitido hacer uso de los equipos para para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros, Colaboradores y Terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por Empresas Públicas de Armenia ESP.
9. Cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación, o actualización de sus aplicaciones, deberá solicitarse por medio de la Mesa de Ayuda Tecnológica, y estas entraran a ser evaluadas por la Dirección TICs para su aprobación o denegación.
10. El software propiedad de Empresas Públicas de Armenia ESP, es para uso exclusivo de usuarios de planta y contratistas con vínculo directo con Empresas Públicas de Armenia ESP. Proveedores y/o contratistas no pueden instalar o hacer uso de las licencias propiedad de Empresas Públicas de Armenia ESP.
11. Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud a la Mesa de Ayuda, la cual respaldará la información y documentos que se consideren de las funciones asignas a su cargo.
12. Cada usuario debe ser responsable de sacar el respaldo respectivo de la información que maneja en su equipo de cómputo. La Dirección TICs sólo es responsable de respaldar y salvaguardar la información que se encuentra en los discos compartidos a través de los servidores del centro de cómputo. En caso de que algún usuario requiera ayuda con sus respaldos, deberá solicitarlo por medio de la Mesa de Ayuda, para que este le implemente el procedimiento más adecuado y su información pueda estar asegurada.
13. El usuario no deberá alterar el contenido físico y/o lógico del mismo incluyendo sus periféricos.
14. El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de estos.
15. En caso de que un equipo de cómputo presente un mal funcionamiento, el usuario responsable por el equipo de cómputo deberá reportarlo de inmediato a través de la Mesa de Ayuda. La Mesa de Ayuda hará una evaluación del equipo para determinar el tipo de daño y la reparación que se requiere.
16. De la evaluación que se realice del equipo de cómputo dañado, se determinará lo siguiente:
    - Si el equipo de cómputo está en garantía y el daño puede ser

procesado por garantía. En este caso lo enviará al proveedor donde fue adquirido el equipo para que este haga la reposición de la parte defectuosa y devuelva el equipo lo más pronto posible.

- Si el equipo de cómputo está fuera de garantía, se determinará si el equipo puede repararse internamente en el diario o si requiere de una reparación en un servicio técnico autorizado.
- Si el daño es por falla eléctrica, se determinará la parte que debe ser reemplazada, y si la reparación puede ser realizada en el diario o debe enviarse a una empresa de servicio técnico. Adicionalmente se reportará el particular a la dependencia correspondiente para que tomen las medidas pertinentes respecto al punto eléctrico que causó el problema.
- Si se determina que es por mal uso del mismo, se procederá con la reparación, pero se informará a la Dirección TICs para que el costo de la reparación del mismo sea descontado al usuario responsable del equipo de cómputo.

A tener en cuenta:

- Se recomiendan al personal y colaboradores de la entidad que restrinjan el uso de los equipos en almacenar o dejar registros sobre actividades y tareas personales, dado el caso que se requiera la información clasificada como personal almacenado en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como "PERSONAL".
- El uso de dispositivos como unidades de almacenamiento USB, CD's o cualquier otro, es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus.

Referente al uso y manejo de equipos de cómputo en su espacio de trabajo

1. Bloquear su computador o dispositivo móvil en los momentos que no se está utilizando y cuando deba retirarse de su puesto de trabajo.
2. Cerrar sesiones de usuario al finalizar su labor o cuando ya no sean utilizados los equipos de cómputo.
3. Activar bloqueos automáticos de dispositivos móviles y diferentes equipos de cómputo asignados, para evitar el acceso no autorizado y pérdida de información sensible.
4. Custodiar documentos impresos que contengan información sensible de Empresas Públicas de Armenia ESP., usuarios, proveedores, entre otros y deben ser retirados inmediatamente de impresoras y escritorios de

trabajo.

5. Clasificar la información impresa y almacenarla en cajas de acuerdo a los lineamientos asociados a la Gestión Documental, normalizado en el Sistema de Gestión Integrado.
6. Abstenerse de ingerir alimentos o bebidas en su entorno de trabajo, así como cerca de documentación física y medios magnéticos.

Referente al uso y manejo de dispositivos móviles

1. La Dirección TICs debe llevar un registro y control de todos los dispositivos móviles que posee la Entidad. Se debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de sus funciones laborales.
2. Se debe definir un procedimiento de formal de salida de dispositivos.
3. Los dispositivos móviles que son autorizados para salir de las instalaciones por Empresas Públicas de Armenia ESP deben ser protegidos mediante el uso e implementación de los controles apropiados para ello, como son: cifrado de información, políticas de restricción en la ejecución de aplicaciones, y de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, entre otros.
4. Todos los dispositivos móviles como celulares que almacenen información de Empresas Públicas de Armenia ESP deben contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave.
5. Todos los dispositivos móviles propiedad o de alquiler de Empresas Públicas de Armenia ESP pueden ser monitoreados y sometidos a la aplicación de controles en cuanto a tipo, versión de aplicaciones instaladas, contenido restringido y de ser necesario se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos.
6. El Colaborador o Tercero responsable del dispositivo móvil debe hacer periódicamente copias de respaldo, en caso de los portátiles deben conectar el quipo mínimo una vez por semana a la red, con el fin de que se ejecute la copia de respaldo de la carpeta destinada para esta función.
7. Todos los Colaboradores y Terceros son responsables de garantizar el buen uso de los dispositivos móviles en redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.
8. Los teléfonos móviles se deben utilizar exclusivamente para desempeñar funciones asignadas al cargo dentro de Empresas Públicas de Armenia ESP. La Dirección TICs se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del

mismo.

Referente a la seguridad de los equipos fuera de las instalaciones

1. Todos los equipos de cómputo deben ser registrados al ingreso y al retirarse de las instalaciones de Empresas Públicas de Armenia ESP.
2. Los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, deben contar con controles de seguridad que garanticen la confidencialidad de la información.
3. Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones de Empresas Públicas de Armenia ESP.
4. En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al Proceso de Gestión Administrativa y la Dirección TICs y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.
5. Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

Este Enfoque Software y Sistemas de Información

enfoque tiene el propósito de establecer las condiciones de operación para garantizar el adecuado uso y gestión del software y los sistemas de información adquiridos en Empresas Públicas de Armenia ESP.

Lineamientos sobre Administradores de Software y Sistemas de Información

1. La Dirección TICs de Empresas Públicas de Armenia ESP, será la única área autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de herramientas, aplicaciones y sistemas de información. En los casos donde otras dependencias requieran adquirir aplicaciones, el proceso debe llevar un visto bueno de la Dirección de Tecnologías de la Información y las Comunicaciones.
2. Para el desarrollo o mantenimiento del sistema de información que se realice por un tercero (contratista), se deben implementar los mecanismos necesarios para proteger la información almacenada en los sistemas de información, propendiendo por la integridad, confidencialidad y disponibilidad.
3. Se deben realizar revisiones anuales de los computadores y el software

que es instalado en los mismos, de tal manera que se ejecuten controles de instalación, ajustes a los perfiles de usuario, de tal manera que ningún usuario pueda adelantar instalaciones y la desinstalación correspondiente del software que no esté avalado por la Entidad.

Lineamientos sobre el control de contraseñas

1. Los perfiles de usuario y la contraseña tienen que ser asignados individualmente para soportar el principio de responsabilidad individual.
2. Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo la responsabilidad del rol asignado.
3. El usuario no debe compartir, escribir o revelar su contraseña con ningún colaborador.
4. Las contraseñas individuales no deben ser mostradas en texto claro. Todos los sistemas de procesamiento deben eliminar la visualización de contraseñas ya sea en pantallas o en impresoras.
5. Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.
6. La identificación del usuario y su contraseña no deben ser iguales.
7. Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo, apliance, impresoras, routers, switch, herramientas de seguridad, etc.).
8. Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.
9. Reportar a la Dirección TICs sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
10. Reportar a la Dirección TICs sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.
11. El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información debe estar autorizado por La Dirección TICs.
12. Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por lo tanto, se deben tener en cuenta las siguientes recomendaciones:

a. No utilizar el primer o segundo nombre, los apellidos, el nombre del esposo, el nombre de sus hijos, etc., en ninguna forma (reversado, diminutivos, etc.)

b. No utilizar otra información fácil de obtener acerca de Usted. Esto incluye: Placa o marca del carro, número del teléfono, marca, nombre del edificio, etc.

c. No use contraseñas que contengan sólo números o sólo letras.

d. No utilice palabras contenidas en el diccionario u otras listas de palabras. e. Use contraseñas fáciles de recordar para que no tenga que escribirlas.

e. No use el nombre del perfil de usuario en ninguna forma como, por ejemplo: reversado o duplicado.

f. Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

Referente a la seguridad de las contraseñas

1. Contener al menos doce (8) caracteres alfanuméricos.
2. Contener letras en mayúscula y minúsculas.
3. Contener al menos un número (por ejemplo, 0-9).
4. Contener por lo menos uno de los siguientes caracteres especiales: ,!$%^&*()_+|~-=\`{}[]:";'<>?,/.
5. Crear contraseñas que no puedan ser recordadas fácilmente y almacenarlas en un gestor de contraseñas
6. Usar generadores aleatorios en línea como http://passwordsgenerator.net/. La Protección de contraseñas.
7. Todas las contraseñas de nivel de usuario y de nivel de sistema deben cumplir con la política de construcción de contraseñas.
8. 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.).
9. En lo posible, los usuarios no deben usar la misma contraseña para diversas necesidades de acceso a Empresas Públicas de Armenia ESP.
10. 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.

11. 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.
12. Las contraseñas no deben insertarse en los mensajes de correo electrónico, ni en ninguna otra forma de comunicación electrónica.
13. No revelar las contraseñas por teléfono a nadie, sin importar el mecanismo de presión que se ejerza.
14. No revelar la contraseña en cuestionarios o formularios de seguridad.
15. No insinuar o dar indicios del formato de una contraseña, por ejemplo: "mi apellido".
16. No escribir ni guardar las contraseñas en cualquier lugar de su oficina.
17. No almacenar contraseñas en un archivo de un sistema informático o dispositivos móviles (teléfono, Tablet) sin algún tipo de cifrado.
18. No utilizar la función "Recordar Contraseña" de las aplicaciones, por ejemplo: navegadores web.
19. Cualquier usuario que sospeche que su contraseña puede estar comprometida debe informar el incidente y cambiar todas las contraseñas.
20. Siempre que el Administrador de contraseñas asigne una contraseña, es responsabilidad del usuario cambiarla en su primer uso.
21. Las contraseñas débiles se caracterizan por los siguientes patrones:
    a. Cuentan con menos de 8 caracteres.
    b. Se encuentra en un diccionario, incluyendo un idioma extranjero, o existe en una lengua, dialecto o jerga.
    c. Cuentan con información personal como fechas de cumpleaños, direcciones, números telefónicos, o nombres de familiares, mascotas, amigos o personajes de fantasía.
    d. 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.
    e. Cuentan con patrones numéricos como aaabbb, qwerty, zyxwvuts o 123321.
    f. Cuentan con palabras comunes deletreadas hacia atrás, precedidas o seguidas por un número (por ejemplo, oterces,

secreto1 o 1secreto).

g. Utilizan alguna versión de “Bienvenido123”, “Contraseña123”, “Cambiame123”.

h. Generación una contraseña de forma manual.

Referente a la protección de contraseñas

1. Todas las contraseñas de nivel de usuario y de nivel de sistema deben cumplir con la política de construcción de contraseñas.
2. 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.).
3. En lo posible, los usuarios no deben usar la misma contraseña para diversas necesidades de acceso a Empresas Públicas de Armenia ESP.
4. 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.
5. 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.
6. Las contraseñas no deben insertarse en los mensajes de correo electrónico, ni en ninguna otra forma de comunicación electrónica.
7. No revelar las contraseñas por teléfono a nadie, sin importar el mecanismo de presión que se ejerza.
8. No revelar la contraseña en cuestionarios o formularios de seguridad.
9. No insinuar o dar indicios del formato de una contraseña, por ejemplo: "mi apellido".
10. No escribir ni guardar las contraseñas en cualquier lugar de su oficina.
11. No almacenar contraseñas en un archivo de un sistema informático o dispositivos móviles (teléfono, Tablet) sin algún tipo de cifrado.
12. No utilizar la función "Recordar Contraseña" de las aplicaciones, por ejemplo: navegadores web.
13. Cualquier usuario que sospeche que su contraseña puede estar

comprometida debe informar el incidente y cambiar todas las contraseñas.

Lineamientos sobre el uso adecuado de Software y Sistemas de Información

Estos lineamientos establecen las condiciones y restricciones para el manejo adecuado de los sistemas de información de Empresas Públicas de Armenia ESP.

Referente al manejo de los sistemas de información digitales

1. La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo es de la Dirección TICS.
2. Las estaciones de trabajo de la Empresas Públicas de Armenia ESP deben ser utilizadas únicamente por los empleados, proveedores o contratistas sólo para el desarrollo de las funciones normales de su trabajo.
3. Las bases de datos a las que se conectan los sistemas de información internos o los sistemas de información administrados por un operador tecnológico para la operación son de Empresas Públicas de Armenia ESP siempre y cuando la información y el sistema de información sea de propiedad de Empresas Públicas de Armenia ESP o en su defecto se definan las formas de utilización y propiedad dentro de las obligaciones contractuales correspondientes.
4. Solo podrán estar expuestas aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a de Empresas Públicas de Armenia ESP (ciudadanos y demás gente del común); las demás aplicaciones son de uso interno y su acceso desde fuera de la Entidad se debe realizar a través de conexiones seguras (VPNs) con previa autorización por parte de la Dirección TICs y del jefe inmediato, quien da el aval para dicho acceso.
5. En los casos donde la operación del Sistema de información de la Entidad sea administrada por un operador tecnológico externo (Contratista), las conexiones externas deben ser autorizadas por la Dirección de Tecnología y Sistemas de Información de Empresas Públicas de Armenia ESP.
6. En los casos donde los sistemas de información son administrados por un operador tecnológico y son propiedad de un tercero, estos deben cumplir con los lineamientos específicos de seguridad de la información descritos en el manual de seguridad de la información de Empresas Públicas de Armenia ESP.

Referente a uso del software legal y derechos de autor

1. Los usuarios solo podrán utilizar software legalmente adquirido y/o autorizado por Empresas Públicas de Armenia ESP.
2. En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable en donde se encontrase instalado dicho software; debido a que está atentando contra los derechos de autor.
3. En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información.
4. Los usuarios no pueden realizar copias de software que se encuentre instalado o sea desarrollado por Empresas Públicas de Armenia ESP, para su distribución.

Referente al control de virus

1. Los computadores personales deben mantener activo un software antivirus, Sistema Operativo, Microsoft Office, licenciados y actualizados y que su uso haya sido autorizado por el equipo de trabajo la Dirección TICs.
2. Los servidores de archivos, groupware y correo electrónico deben mantener activo un software antivirus.
3. Los computadores personales y servidores deben ser analizados contra virus periódica y automáticamente.
4. Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de Intraepa, debe ser revisada por un software antivirus antes de ser descargada y utilizada.
5. La Dirección TICs es responsable por la actualización oportuna del software antivirus.
6. Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus a las áreas encargadas.
7. Es responsabilidad de los usuarios tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.
8. El usuario debe asegurar que toda la información provenga de fuentes conocidas.
9. Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.

Lineamientos sobre el desarrollo del software para la Empresas Públicas de Armenia ESP

Empresas Públicas de Armenia ESP en el cumplimiento de sus responsabilidades debe establecer las condiciones para el desarrollo de software y sistemas de información que la entidad demande, a continuación, se definen los lineamientos a considerar:

1. Los mecanismos de seguridad definidos para una aplicación específica no deben ser alterados, pasados por alto o comprometidos.
2. Los controles de seguridad deben ser documentados y deben permitir probar su efectividad.
3. Todo software desarrollado no debe presentar nuevas vulnerabilidades o reducir el nivel de seguridad existente.
4. Cualquier software que use funciones privilegiadas del sistema operativo debe ser aprobado por el equipo de trabajo de la Dirección de Tecnologías de Información y Comunicaciones.
5. El desarrollo y mantenimiento de software debe dejar las adecuadas pistas de auditoría (Registro de eventos).
6. La Dirección TICs es responsable de efectuar pruebas para asegurar que se han cumplido los requerimientos de seguridad.
7. Todas las aplicaciones deben contar con documentación funcional, técnica y de usuario.

Referente al desarrollo seguro, pruebas y soporte

Empresas Públicas de Armenia ESP debe:

1. Establecer la metodología para el desarrollo integral de software y sistemas de información, contemplando el análisis, diseño, implementación, pruebas, integración, despliegue con su respectiva documentación.
2. Definir un procedimiento enfocado al Desarrollo y Mantenimiento de Software.
3. Garantizar el versionamiento de desarrollo de software.
4. Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
5. Asegurar la infraestructura tecnología necesaria para la puesta en producción de los sistemas de información, aplicaciones y portales, ya

sean nuevos o ajuste a los existentes.

6. Garantizar el soporte especializado a los sistemas de información, aplicaciones y portales a través de la Sistema de mesa de servicio.
7. Realizar monitoreo periódico del soporte especializado a los sistemas de información, aplicaciones y portales.

Enfoque Datos, Información y Almacenamiento

Este enfoque tiene el propósito de establecer las condiciones de operación para garantizar el adecuado uso y gestión de los datos e información que se captura en Empresas Públicas de Armenia ESP.

Lineamiento sobre la clasificación, uso y manejo de información confidencial

Estos lineamientos permiten asegurar que la información de Empresas Públicas de Armenia ESP es clasificada, con el fin de que sea tratada y protegida adecuadamente.

Referente a la clasificación y caracterización de la información

1. Toda la información de Empresas Públicas de Armenia ESP, debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.
2. Todos los procesos a través del Comité Interno de Archivo son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.
3. De acuerdo con la clasificación establecida por la entidad y el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:
    a. Acceso a la información sólo de personal autorizado.
    b. Llevar un registro formal de acceso a la información.
    c. Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Referente al etiquetado y manejo de Información

1. Todos los colaboradores y terceros cuando sea el caso deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.
2. Los directores, Jefes de Oficina, coordinadores de Grupo deben

establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

3. Todos los Colaboradores y Terceros cuando sea el caso de Empresas Públicas de Armenia ESP son responsables de la organización, conservación, uso y manejo de los documentos en los medios que son dispuestos por la Entidad.
4. Todas las dependencias de Empresas Públicas de Armenia ESP deben enviar al Archivo Central la documentación de forma ordenada y organizada, de acuerdo con los tiempos de retención establecidos en la Tabla de Retención Documental.
5. El Archivo Central de Empresas Públicas de Armenia ESP recibe las transferencias documentales de acuerdo con cronograma anual de transferencia *d*ocumentales.
6. Los archivos de Gestión de las oficinas de Empresas Públicas de Armenia ESP deben custodiar sus documentos de acuerdo con lo especificado en las tablas de Retención Documental.
7. La plataforma tecnológica usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.
8. Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por Empresas Públicas de Armenia ESP.
9. El etiquetado de información debe incluir la información física y electrónica. Las etiquetas de la información se deben identificar y reconocer fácilmente.
10. Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Referente a la confidencialidad de la información

1. Los documentos con esta información no pueden ser dejados desatendidos o inseguros.

2. Debe indicar el usuario dueño o fuente de información en la primera página o cubierta, o en algún repositorio central.
3. La divulgación de la información debe ser apropiadamente autorizada de acuerdo con los estándares de clasificación de la información por parte de los propietarios.

4. Reuniones relacionadas con el manejo de esta información deben llevarse a cabo en áreas de oficinas cerradas.
5. Prohibido el acceso o envió de información confidencial por medio de teléfonos, celulares u otros canales que dificulten garantizar custodio de la información.
6. Toda la información debe ser etiquetada con la clasificación respectiva para garantizar la confidencialidad de la misma.
7. El etiquetado debe ser fácilmente leíble a simple vista.
8. Antes de divulgarse verbalmente información clasificada como Restringida o Confidencial debe indicarse su clasificación.
9. El acceso o distribución de información de Uso Interno debe estar limitado a empleados u otros con la necesidad de conocerla o usarla para cumplir con sus funciones.
10. Documentos que contengan información confidencial deben ser impresos en un área segura o con la supervisión adecuada *y deben contener en el documento un indicador que establezca la confidencialidad del mismo.*
11. Distribución de información confidencial debe ser limitada a personas o grupos con la necesidad de conocerla o usarla para cumplir con sus funciones.
12. Los mecanismos de entrega utilizados para información Restringida deben contemplar confirmación de recibo.
13. Estas políticas aplican tanto a los originales como a todas las copias de la información.
14. Acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado. Esto incluye información confidencial almacenada externamente o copias de respaldo.
15. Las copias de respaldo de información confidencial deben ser protegidas de destrucción intencionada o accidental. Algunos métodos de protección pueden incluir contenedores a prueba de fuego, contenedores asegurados y almacenamiento externo.
16. Información almacenada por períodos prolongados debe ser revisada regularmente para verificar su legibilidad.
17. Las personas que tienen acceso remoto a la información de la Empresas Públicas de Armenia ESP son responsables por la seguridad de la información con los mismos niveles de control requeridos dentro de la Empresas Públicas de Armenia ESP.

Referente a los controles criptográficos

1. 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.
2. Verificar que todo sistema de información o software que requiera realizar transmisión de información reservada o restringida cuente con mecanismos de cifrado de datos.
3. Desarrollar y establecer estándares para la aplicación de controles criptográficos.
4. Asegurarse que los controles criptográficos de los sistemas de información utilizados cumplan con los estándares establecidos para garantizar la confidencialidad de la información.

Lineamientos sobre la gestión de almacenamiento

Estos lineamientos establecen las condiciones y restricciones de gestión del almacenamiento de la información de Empresas Públicas de Armenia ESP.

Referente el almacenamiento en equipos de cómputo y red local.

1. Cada proceso responsable de proteger los activos de información de Empresas Públicas de Armenia ESP suscritos a su velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.
2. El uso de carpetas compartidas se podrá realizar sobre privilegios y controles de acceso en cada uno de los equipos de cómputo de Empresas Públicas de Armenia ESP. Dado el caso que el colaborador no aplique los lineamientos sobre manejo de equipo de cómputo y recursos tecnológicos con acceso a información confidencial la Dirección TICS no se hace responsable de la pérdida o infiltración de la información.
3. Las carpetas compartidas sobre la infraestructura ofrecida por Dirección TICs como Google Drive, File server, SharePoint o el proveedor que considere, serán administradas por las áreas quienes velarán por el buen uso de la información y de las carpetas.
4. Dirección TICs debe documentar los permisos y accesos sobre la carpeta compartida, usando los siguientes criterios:

    a. Permisos de Lectura.

    b. Permisos de Escritura y modificación.

    c. Permisos de Control Total.

    Lo cuales serán documentados por la Dirección TICs a través de la Mesa de Ayuda. La información CLASIFICADA o RESERVADA, debe utilizarse en las carpetas destinadas en el file server, para que sean incluidos en las

Políticas de respaldo de información (Backup).

Para cada caso el área o proceso responsable deberá disponer de su documentación de permisos y acceso y solicitar el respectivo ajuste, cambio o adición a la Dirección TICs por medio de la mesa de ayuda.

5. Cada proceso, dirección o área tendrá un único administrador que será autorizado con permisos de lectura y escritura quien administrará las carpetas y será responsable a que usuarios otorgará permisos sobre esta.
6. El administrador de cada carpeta en su respectivo proceso y/o dirección deberá fijar el límite de tiempo durante el cual estará publicada la información y compartido el recurso en la infraestructura ofrecida por la Dirección TICs.
7. Los permisos de administrador serán gestionados por la Dirección TICs, a través de la mesa de ayuda de tecnología con el formato adjunto.
8. Cada administrador de las carpetas compartidas deberá realizar semestralmente una depuración de la información y notificar a la Dirección TICS los cambios realizados.
9. Se prohíbe el acceso a carpetas compartidas a usuarios que no tengan una vinculación directa con Empresas Públicas de Armenia ESP.
10. Se prohíbe el acceso a las carpetas compartidas a Colaboradores desde equipos de cómputo que no cuenten con antivirus corporativo actualizado.
11. Se prohíbe la publicación de archivo ejecutables (.exe, bat y dll entre otros) en las carpetas compartidas de Google Drive, File server, si el área requiere usar alguna de las extensiones mencionadas, debe justificarlo a la Dirección TICS para ajustar la política, como se defina según acuerdo por las dos áreas.
12. La Dirección TICS realizará monitoreo y revisiones periódicas, con el fin de velar por una correcta administración de las carpetas compartidas cada semestre.
13. Está prohibido el uso carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función del colaborador.
14. La Dirección TICs define que los nombres a los archivos y carpetas sean lo suficientemente significativo sin que sea demasiado extenso, y que no contengan nombres de los usuarios. Se establece como longitud máxima para un nombre de archivo, 256 caracteres (un carácter puede ser una letra, número o un símbolo).
15. Los permisos a las carpetas compartidas administrados por la Dirección TICS sobre los diferentes ambientes (Pruebas, Certificaciones y Producción) se autorizarán a través de una mesa de ayuda de tecnología.

Referente al almacenamiento en la nube

1. La información pública de las áreas de la institución debe utilizarse las carpetas destinadas en el Google Drive.
2. Para gestión de trabajo colaborativa en la operación cotidiana para uso interno de la institución podrá utilizarse en las carpetas destinadas en el Google Drive, para que sean incluidos en las Políticas de respaldo de información.
3. El único medio de respaldo de la información para los colaboradores es Google Drive, el cual será configurado por la Dirección TICs.

Referente al borrado seguro de información

1. La Dirección TICs es la responsable de gestionar el procedimiento de borrado seguro acorde al procedimiento establecido desde su competencia,
2. Los medios de almacenamiento que contengan información de Empresas Públicas de Armenia ESP y que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido por Empresas Públicas de Armenia ESP, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).
3. Todos los medios de almacenamiento que contengan información de Empresas Públicas de Armenia ESP y que salgan de la Entidad y que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por Empresas Públicas de Armenia ESP, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos alquilados, equipos para pruebas de concepto, equipos de proveedores, discos duros externos, etc.).
4. Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por Empresas Públicas de Armenia ESP para su uso dentro de la red corporativa, deben contar con su respectivo soporte.
5. Dado el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, éste hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente.
6. Al finalizar la vida útil o determinar que ya no son necesarios para las labores institucionales, los medios de almacenamiento de equipos de cómputo, medios de almacenamiento extraíbles como discos externos, discos ópticos u otros medios que puedan contener información institucional, deben ser sometidos a borrado seguro que impida su recuperación de información.

7. En caso de imposibilidad tecnológica de aplicar borrado seguro, los medios deben ser sometidos a destrucción siguiendo las políticas de manejo de residuos electrónicos institucionales.

Referente a la trasferencia de información en medios físicos

1. Cada proceso responsable y custodio de los activos de información que genera es responsable de garantizar el cumplimiento de los lineamentos descritos en la presente política.
2. Toda la información clasificada como CONFIDENCIAL o RESERVADA que se desee almacenar en medios removibles y que sean transportados fuera de las instalaciones de Empresas Públicas de Armenia ESP, debe cumplir con las disposiciones de seguridad indicadas por La Dirección TICs, específicamente aquellas referentes al empleo de técnicas de cifrado.
3. El transporte de los medios físicos se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma se evitar una afectación a la integridad y disponibilidad.
4. Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.
5. Cada proceso, dirección y/o área responsable debe informar trimestralmente a la Dirección TICs el estado del registro o cadena de custodia de los activos de información transportados.
6. Dirección TICs deberá establecer un procedimiento que permitan la efectiva gestión de dichos activos de información donde se contemplen condiciones de operación para la transferencia de información.

Lineamientos sobre la propiedad de la información

Estos lineamientos establecen las responsabilidades en la propiedad de los activos de información que se generan y gestionan en Empresas Públicas de Armenia ESP con el fin de resguardar los intereses de la entidad y los terceros implicados.

Referente a la propiedad intelectual de activos de información

1. Todo el material que es desarrollado por una persona natural o jurídica mientras tenga una vinculación como servidor o como contratista con de Empresas Públicas de Armenia ESP, se considera que los derechos patrimoniales son propiedad de la Entidad y que es de uso exclusivo de

la misma, por lo tanto, debe ser protegida contra un develado, descubrimiento o uso que menoscabe los intereses institucionales, misionales, reputacionales, económicos y en general cualquier perjuicio contra de Empresas Públicas de Armenia ESP, en los términos de la ley 23 de 1982 y sus normas reglamentarias y aquellas que la modifiquen.

2. La Dirección Jurídica y Secretaria General y Gestión del Talento Humano, deben realizar las tareas pertinentes para que en los contratos suscritos con empleados, contratistas, terceros y operadores tecnológicos se incluyan las cláusulas correspondientes que especifiquen los compromisos y cuidados que se debe tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad.
3. Con el fin de cumplir las leyes sobre propiedad intelectual, el área de Archivo Central y la Dirección TICs debe adelantar acciones para el guardado de archivos dentro de los equipos de la Entidad y en ese sentido, generar procesos para el borrado de archivos que no deban estar en los computadores, tales como archivos de video (mp4, avi, flv, etc.), archivos de audio (3gp, mp3, etc.), fotografías, etc. Hay que tener en cuenta que ciertos usuarios deben estar dentro de las excepciones, toda vez que el cumplimiento de sus funciones está orientado a la producción de dicho material, caso en el cual se debe documentar y adelantar las solicitudes correspondientes para poner en firme dicha excepción.

Referente a la gestión de los activos de información

1. Los activos de Información de Empresas Públicas de Armenia ESP deben ser identificados, clasificados y controlados para propender por su uso adecuado, protección y la recuperación ante cualquier desastre.
2. El Área de Archivo Central de la mano con la Dirección TICs serán los responsables de establecer las condiciones de gestión y clasificación de los activos de información por medio de la formulación de un Procedimiento para tal fin.
3. La Dirección TICs garantizará los medios electrónicos y recursos tecnológicos necesarios para apoyar la gestión integral y custodia de los activos de información.
4. Los propietarios de la información deben propender para que los custodios de los activos mantengan actualizado el inventario Matriz de Activos de Información y realicen las actualizaciones programadas una vez al año o cuando se requiera.
5. Es responsabilidad de los custodios y usuarios finales el adecuado uso

de los activos de información que de Empresas Públicas de Armenia ESP ha dispuesto para el cumplimiento de sus funciones u obligaciones.

6. Con el objeto de implementar los controles de seguridad de información, las áreas y procesos de Empresas Públicas de Armenia ESP que tienen la custodia de la información, en el marco de su función, se encargarán de proteger la información, y propender para que el propietario mantenga y actualice el inventario de activos de la información y proponer las mejoras correspondientes., para más información diríjase a la Declaración de Aplicabilidad.
7. En el caso de los operadores tecnológicos, se deben implementar los controles de seguridad necesarios para asegurar los activos de información y la información que están bajo responsabilidad de estos y están al servicio o son propiedad de Empresas Públicas de Armenia ESP.

Lineamientos sobre las copias de respaldo de información (Backup)

Estos lineamientos establecen las condiciones para el respaldo de información en medios físicos y electrónicos en Empresas Públicas de Armenia ESP con el fin de resguardar los intereses de la entidad y los terceros implicados.

Referente al gobierno y gestión de las copias y respaldo de información

1. El área de archivo central y la Dirección TICs debe formular e implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en cualquier espacio físico o virtual de la Entidad y su recuperación en caso de desastre.
2. La Dirección TICs, debe realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.
3. La Dirección TICs y el responsable de Seguridad de la Información junto a los propietarios de la información deben determinar los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de TI.
4. La Dirección TICs debe garantizar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico de Empresas Públicas de Armenia ESP.
5. Se debe definir y documentar un esquema de respaldo de la información.
6. El dueño de la información es responsable de definir claramente el periodo de retención de respaldos, en función de los requerimientos de las áreas funcionales.

7. Se debe tener en cuenta los lineamientos de la ley 594 de 2000 o cualquiera que la modifique, adicione o derogue.
8. Dirección TICs debe implementar controles para auditar el acceso y uso de datos por parte de los servidores o contratistas, a los sistemas de información en custodia y acompañamiento de la Dirección TICs.
9. Dirección TICs debe proveer los recursos necesarios para la implementación de los controles requeridos para la seguridad de las operaciones.
10. Dirección TICs debe definir e implementar un Plan de Continuidad y Contingencia de Negocio que propenda por la mitigación de los riesgos sobre la confidencialidad, integridad y disponibilidad de la información en los casos de incidentes seguridad.
11. Los usuarios responsables por respaldar la información también son responsables de facilitar la oportuna restauración de la información.
12. Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

Referente al proceso de copias y respaldo de información (Backup)

1. Se deben definir procedimientos para el respaldo de la información, que incluyan los siguientes parámetros:

    a. Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

    b. Definir un el procedimiento de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo a lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.

    c. Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración.
2. Cada Sistema de Información deberá contar con un sistema automático para la recolección de copias de respaldo.
3. Se debe verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de garantizar la integridad y

disponibilidad de la información.

4. Se deben extender los mismos controles de seguridad aplicados a los activos de TI en el sitio principal al sitio alterno.
5. Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros, según las condiciones descritas en los lineamientos del Enfoque Seguridad Física, Infraestructura TI y Dispositivos.
6. Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.
7. Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.
8. Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.
9. Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.
10. Al enviar Información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.
11. Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.
12. Dirección TICs debe garantizar controles para mitigar los riesgos inherentes a códigos maliciosos.
13. La Dirección TICs, a través del personal competente en administrador de Bases de Datos, de la Red y servidores, debe:
    a. Actualizar periódicamente las configuraciones de los Servidores para la correcta ejecución de las copias de respaldo.
    b. Efectuar las copias de información de los Servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones Básicas.
    c. Realizar un respaldo Diferencial semanalmente de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.
    d. Realizar un respaldo full mensual de los Servidores de Base de Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.
    e. Realizar un respaldo full anual de los Servidores de Base de

Datos, servidores Web, Sistemas de Información, Aplicaciones, Desarrollo y dispositivos de red.

f. Las copias de respaldo se deben realizar en horario no hábil, lo cual será verificado a través de Procesos Automáticos.

14. Una vez se verifique la correcta ejecución de las copias de respaldo, se debe retirar la cinta de Backup del robot de cintas.
15. Los dispositivos magnéticos que contienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra almacenada.
16. El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados.
17. Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores.
18. La Dirección TICs, cuenta con un responsable para gestionar la entrega o retiro de las cintas de Backup del sitio externo.
19. Las cintas de Backup con la Información actualizada, no deben permanecer más de una semana fuera del sitio externo.

Referente al registro de Respaldo de Información

1. Disponer de un procedimiento de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.
2. La Dirección TICs, a través del personal competente en administrador de Bases de Datos, de la Red y servidores, debe aplicar la siguiente Normativa:
    a. Llevar el registro de los Respaldos de Información realizada bajo los tiempos establecidos en el procedimiento.
    b. Registro del retiro de las cintas de Backup del sitio externo.
    c. Registro del ingreso de las cintas de Backup al sitio externo.
    d. Inventario de cintas de Backup.
    e. Comprobación de Integridad de la Información
3. La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en

el evento que se requiera para su utilización en casos de emergencia.

4. Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.
5. Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.
6. La Dirección TICs, a través del personal competente en administrador de Bases de Datos, de la Red y servidores, debe aplicar los siguientes lineamientos:
    a. Tener comunicación frecuente con los proveedores de TI para conocer el estado del Backup de los sistemas de información.
    b. Solicitar a los proveedores de TI los reportes y respectivas copias de seguridad sobre cada sistema de información al uso y servicio de Empresas Públicas de Armenia ESP.
    c. Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.
    d. Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.
    e. Realizar seguimiento a la configuración de las herramientas de ejecución de copias de respaldo de los Sistemas de Información de los proveedores para que automáticamente registre el éxito o errores en la ejecución.
    f. Validar la integridad y accesibilidad de las cintas magnéticas por lo menos cada cuatro meses.
    g. Mantener siempre una copia de la información de los Servidores, por lo menos con una antigüedad no superior a 24 horas.
    h. Se debe mantener un monitoreo frecuente sobre el rendimiento y alcance de la información en la Base de Datos para así asegurar la integridad de la información respaldada.

Referente al respaldo de Información para Usuarios Finales

1. Todos los usuarios son responsables de realizar los respaldos de información personal almacenada en los equipos asignados.
2. Toda la información relevante a las funciones del colaborador debe ser

almacenada en el Google Drive suministrado por la Dirección TICs.

3. La Dirección TICs, debe mantener los respaldos de información en condiciones adecuadas de medio ambiente, temperatura, humedad, y otros.
4. Ningún usuario puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.
5. Todos los Colaboradores y Terceros de Empresas Públicas de Armenia ESP deben dar estricto cumplimiento a esta política y el que haga caso omiso puede ser sujeto a acciones disciplinarias o civiles, incluyendo la terminación del respectivo contrato.
6. Se debe elaborar un plan de emergencia para todas las aplicaciones que manejen información crítica de la Entidad, el responsable de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
7. Es responsabilidad todos los Colaboradores y Terceros almacenar la información crítica asociada con su labor en el servidor de archivos establecido, para garantizar que la información está siendo respaldada.

Enfoque Canales de Comunicación

Este enfoque tiene el propósito de establecer las condiciones de uso y manejo de los canales de comunicación con colaboradores, consumidores y grupos de interés en Empresas Públicas de Armenia ESP.

Lineamientos sobre el manejo de internet

Estos lineamientos definen las condiciones para el buen uso del internet, con el fin de asegurar una adecuada protección de la información de Empresas Públicas de Armenia ESP.

Referente a la gestión del servicio de internet

1. La Dirección TICs debe garantizar disponibilidad y buen servicio de conectividad a internet en todas las sedes de Empresa Publicas de Armenia
2. Empresas Públicas de Armenia ESP, en cabeza de La Dirección TICs dispone de un canal de Internet que apoya el cumplimiento de las funciones de los servidores públicos y pasantes.
3. El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas asignadas al servidor público, contratista o parte interesada. Ver ley 734 de 2002, por la cual se expide el Código Disciplinario Único. "Artículo 34, Deberes. Numeral 4: Deberes"

4. El acceso al servicio de Internet podrá ser asignado a las personas que tengan algún tipo de relación con la Entidad, ya sea como servidor público, contratista, pasante o miembro de un grupo de valor. La autorización de uso del servicio de acceso a internet para los visitantes de las instalaciones de la Entidad debe ser solicitada por los responsables de procesos o dependencias que visita la persona.
5. Todo usuario del servicio de Internet es responsable de informar a su superior o la mesa de ayuda de la Dirección TICs, el acceso vía Internet a contenidos o acceso a servicios que no le estén autorizados o no le correspondan para la ejecución de las funciones asignadas. El responsable de la dependencia o proceso debe coordinar con la Dirección TICs, el ajuste de los privilegios de acceso al servicio de navegación por Internet.
6. Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que él envíe desde las redes de datos de Empresas Públicas de Armenia ESP o se descargue desde Internet usando su cuenta de acceso.
7. La Entidad puede supervisar el uso y acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales. En los procesos verificación del uso apropiado del servicio de acceso a Internet se respetan los derechos a la intimidad y privacidad.
8. Cuando un servidor público, contratista o miembro de grupo de valor al que le haya sido autorizado el uso de una cuenta de servicio de Internet o de acceso a la red local finalice su relación con la Entidad, debe seguir los procedimientos definidos por la Dirección TICs para entregar su cuenta de usuario y accesos a servicios informáticos provistos.
9. Es responsabilidad de los servidores públicos, contratistas y pasantes, salvaguardar la información de entidad, cumpliendo con los criterios de integridad, disponibilidad y confidencialidad. Así mismo, deben velar porque la información de la entidad sea protegida de divulgación no autorizada.
10. Toda comunicación organizacional referente a noticias, circulares, documentos de Sistema de Gestión Integrado y similares tendrá como espacio central y principal de reposo la Intraepa *www.intraepa.gov.co.*
11. Empresas Públicas de Armenia ESP se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Referente a los usos aceptables del servicio

1. Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en

Empresas Públicas de Armenia ESP y no debe utilizarse para ningún otro fin.

2. Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información de Empresas Públicas de Armenia ESP.
3. La Dirección TICs, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
4. Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.
5. El navegador autorizado para el uso de Internet en la red de Empresas Públicas de Armenia ESP es el instalado por la Dirección TICs, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.
6. No se permite la conexión de módems externos o internos en la red de Empresas Públicas de Armenia ESP, previa solicitud autorizada por La Dirección TICs.
7. Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro de Empresas Públicas de Armenia ESP.
8. Todos los usuarios son responsables del uso de sus credenciales de acceso a las cuales les fue otorgado el acceso a internet.
9. Para realizar intercambio de información de propiedad de Empresas Públicas de Armenia ESP con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.
10. Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.
11. Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de Empresas Públicas de Armenia ESP.
12. Los colaboradores y tercero de Empresas Públicas de Armenia ESP no

deben asumir en Empresas Públicas de Armenia ESP, posiciones personales en encuestas de opinión, foros u otros medios similares.

13. Empresas Públicas de Armenia ESP, a través de la Dirección TICs, debe coordinar con los operadores tecnológicos que requieran acceso o interconexión a la infraestructura o a los activos de información de la Entidad para acceder a internet o a canales de comunicación externos, los controles que se deben seguir para dicha interconexión y operación.
14. En los casos donde la operación sea administrada por un operador tecnológico, éstos deben contar con los controles necesarios y conexiones seguras para el acceso a internet en las sedes de Empresas Públicas de Armenia ESP. La Dirección de Tecnología y Sistemas de Información o el supervisor del contrato debe realizar el monitoreo correspondiente.
15. La Dirección TICs se reserva el derecho de monitorear, hacer seguimiento y auditoría a los usuarios, para verificar que se haga un uso responsable y racional de los recursos y servicios tecnológicos de la Entidad.

Referente a los usos no aceptables del servicio

1. Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.
2. Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.
3. Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.
4. Todos los usuarios invitados que requieran acceso a internet dentro de las instalaciones de Empresas Públicas de Armenia ESP deben realizarlo por medio de la red pública habilitada y cumplir con los requerimientos que el portal solicita, una vez que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.
5. No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.
6. No se permite el acceso a páginas con contenido restringido como pornografía, anonimizadores, actividades criminales y/o terrorismo, crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p) o

páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración de contenidos de Empresas Públicas de Armenia ESP y las emitidas por los entes de control.

Lineamientos sobre el uso y manejo de correo electrónico

Estos lineamientos establecen las condiciones para el buen uso y manejo del correo electrónico en Empresas Públicas de Armenia ESP con el fin de resguardar los intereses de la entidad y los terceros implicados.

Referente a la gestión del servicio de correo electrónico

1. Empresas Públicas de Armenia ESP en cabeza de La Dirección TICs, dispone de un servicio de correo electrónico que apoya las actividades de los servidores públicos, contratistas y pasantes de la entidad.
2. Los servidores públicos, contratistas y pasantes son responsables de todas las actividades realizadas con la cuenta de correo asignada por la entidad. Toda la información transmitida a través de la cuenta de correo es responsabilidad del propietario de dicha cuenta.
3. El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con Empresas Públicas de Armenia ESP. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad de Empresas Públicas de Armenia ESP y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.
4. El área de Gestión de Talento Humano es el responsable de solicitar la creación, modificación y eliminación de las cuentas de correo para los servidores públicos y pasantes de la entidad.
5. El área de Gestión de Talento Humano es el responsable de solicitar la creación, modificación y eliminación de las cuentas de correo para contratistas.
6. Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar a la Dirección TICs a través de la Mesa de Ayuda y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM. En el caso de recibir correos con problemas de seguridad, se debe adelantar el procedimiento para gestión de Incidentes de seguridad.
7. Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados a la Dirección TICs a través de la mesa de servicio y serán tratados como incidentes de seguridad de la información.
8. El correo electrónico institucional deberá contener junto con la firma un mensaje de confidencialidad, que deberá ser aprobado por la Dirección de Comunicaciones.
9. Las cuentas de correo electrónico se asignarán de acuerdo con la

nomenclatura definida por la Dirección de Comunicaciones y Dirección TICs.

10. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por Empresas Públicas de Armenia ESP y deberán conservar en todos los casos Empresas Públicas de Armenia ESP saje legal corporativo.
11. Cuando un Proceso, Área o Dependencia, tenga información de interés institucional para divulgar, lo debe hacer a través de la Oficina de Comunicaciones de Empresas Públicas de Armenia ESP o la Intraepa *www.intraepa.gov.co.*
12. El único servicio de correo electrónico controlado en la entidad es el asignado directamente por La Dirección TICs, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
13. Cuando un Colaborador se retire de Empresas Públicas de Armenia ESP, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo corporativo, Talento Humano y Contratación debe notificar a la Oficina de Tecnologías y Sistemas de Información la desactivación de la cuenta.
14. Si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), la Oficina de Tecnologías de la Información y Comunicaciones actuará según sea el caso.
15. La Dirección TICs se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, mensaje será borrado.
16. Las cuentas institucionales (Ejemplo: Comunicaciones, atención al ciudadano, Soporte, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.
17. Las cuentas creadas en los dominios de Empresas Públicas de Armenia ESP serán bloqueadas automáticamente después de estar inactivas en un tiempo de noventa (90) días, para el des bloqueo de la cuenta se debe hacer a través de una mesa de ayuda de tecnología.
18. La información almacenada en los archivos de tipo .PST es responsabilidad de cada uno de los usuarios y cada usuario debe realizar la depuración periódica del buzón para evitar que alcance su límite.
19. Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.
20. Todos los usuarios de correo electrónico, el tamaño máximo para recibir o enviar mensajes es de 25 MB (incluyendo la suma de todos los adjuntos).
21. Todo Colaborador es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Colaborador o Tercero desconfíe del remitente de un correo

electrónico debe remitir la consulta a la Mesa de Ayuda.

22. Los mensajes y la información contenida en los buzones de correo son de propiedad de Empresas Públicas de Armenia ESP.
23. Todos los Colaboradores y Terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro de Empresas Públicas de Armenia ESP, para que de esta forma la Dirección TICs realicen el ajuste de permisos requerido.
24. El servicio de correo electrónico cuenta con las respectivas funcionalidades que ofrecer el proveedor para la gestión de cuentas corporativas.
25. Teniendo en cuenta que el correo electrónico es exclusivamente para uso institucional, de Empresas Públicas de Armenia ESP se reserva el derecho de monitorear el contenido. De esta manera contenidos de música, video, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del servidor o contratista podrán ser borrados sin previa consulta.

Referente a los usos aceptables del servicio

1. El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales, comerciales, propaganda, campañas, invitaciones y cualquier otro uso ajeno a los propósitos de la Entidad.
2. El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @epa.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
3. Todos los Colaboradores y Terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información de Empresas Públicas de Armenia ESP.
4. Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de Empresas Públicas de Armenia ESP.
5. Todos los Colaboradores y Terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.
6. Es responsabilidad del usuario etiquetar mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en la entidad.
7. Cada usuario se debe asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es

responsabilidad de quien envía mensaje de correo electrónico.

Referente a los usos no aceptables del servicio

1. Envío de correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de Solicitud de Cuentas de Usuario, establecido en Empresas Públicas de Armenia ESP.
2. Suministrar los datos de acceso o clave de la cuenta de correo asignada por la entidad.
3. Envío, reenvío o intercambio de correos no deseados o considerados como SPAM, cadena de mensajes o publicidad.
4. De ninguna manera se podrá utilizar la cuenta de correo asignada por la entidad, para actividades personales.
5. Participar en la transmisión correos spam (cadenas).
6. Suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.
7. Responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar a La Dirección TICs, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo de Empresas Públicas de Armenia ESP.
8. Registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales, casinos, concursos, sitios de citas o cualquier otro ajeno a las funciones y obligaciones que le correspondan en de Empresas Públicas de Armenia ESP.
9. Envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través de los correos corporativos autorizados.
10. Envío de contenidos vulgares, agresivos, insultantes, ofensivos, injuriosos, obscenos, violatorios de la propiedad intelectual o que atenten contra la integridad moral de las personas o instituciones, como tampoco información de agremiaciones.
11. Distribuir información de Empresas Públicas de Armenia ESP que no sea considerada de uso público a otras Entidades o ciudadanos, sin la debida autorización de propietario del activo de información.
12. Envío o intercambio de mensaje con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.
13. Envío o intercambio de mensaje que promuevan la discriminación sobre

la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

14. Envió de mensaje que contengan amenazas o mensajes violentos.
15. Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.
16. Divulgación no autorizada de información propiedad de Empresas Públicas de Armenia ESP.
17. Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.
18. Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.
19. Adulterar o intentar adulterar mensajes de correo electrónico.
20. Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado "Usos aceptable del servicio" de la presente política.

Lineamientos sobre el uso y manejo de redes sociales

Estos lineamientos establecen las condiciones para el buen uso y manejo de las redes sociales en Empresas Públicas de Armenia ESP con el fin de resguardar los intereses de la entidad y los terceros implicados.

Referente a la gestión del servicio de Cuentas de Redes Sociales de Empresas Públicas de Armenia ESP

1. Empresas Públicas de Armenia ESP en cabeza de La Dirección de Comunicaciones, es quien es responsable de definir y establecer la gestión y administración de las cuentas propias de Empresas Públicas de Armenia ESP, así como de seleccionar en las redes sociales en las que la entidad debería tener cuentas.
2. La Dirección de Comunicaciones, será el encardo de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en Empresas Públicas de Armenia ESP.
3. Dirección de comunicaciones establecerá los perfiles para la gestión de la administración de los perfiles paginas oficiales de la entidad.
4. El servicio de redes sociales debe ser empleado para servir a una finalidad de mercadeo, marketing, promoción y branding en relación con Empresas Públicas de Armenia ESP.
5. Los perfiles definidos en las redes sociales deberán contener imágenes que comuniquen la identidad de marca claramente y con la información de perfil que lo certifique como canal oficial.
6. El único servicio de redes sociales controlado en la entidad es el asignado directamente por La Dirección de Comunicaciones, el cual cumple con

todos los requerimientos técnicos y de seguridad necesarios ofrecidos por cada proveedor de perfil para la Entidad.

7. Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de Empresas Públicas de Armenia ESP.
8. Las cuentas de administración de los perfiles en cada red social serán gestionadas desde cuentas de correo electrónico con denominación @epa.gov.co.

Referente a los usos aceptables del servicio de Redes Sociales

1. El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con Empresas Públicas de Armenia ESP.
2. Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información de la Entidad.
3. Empresas Públicas de Armenia ESP facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar por parte de los Colaboradores y Terceros, sin embargo, es necesario hacer buen uso de forma correcta y moderada.
4. Responder adecuada y oportunamente los comentarios y solicitudes de la comunidad sobre las publicaciones y etiquetados de la Entidad.

Referente a los usos NO aceptables del servicio de Redes Sociales

1. Publicación de contenidos que no hayan sido previamente autorizados a través del procedimiento formal de publicación de contenidos.
2. Suministrar los datos de acceso o clave de la cuenta de usuario asignada por la entidad a terceros no autorizados.
3. Compartir contenidos y publicaciones ajenas a los intereses de la entidad o su actividad primaria con la comunidad.
4. De ninguna manera se podrán utilizar las cuentas de perfil de la entidad para actividades personales.
5. Participar en interacción de contenidos nocivos y ajenos a los intereses de la entidad.
6. Suscribirse en canales, perfiles u otras cuentas que no estén afines a los intereses de la entidad.
7. Publicación de mensajes o contenidos en páginas o perfiles de redes

sociales o cualquier otro ajeno a los intereses de la entidad.

8. Envío de contenidos vulgares, agresivos, insultantes, ofensivos, injuriosos, obscenos, violatorios de la propiedad intelectual o que atenten contra la integridad moral de las personas o instituciones, como tampoco información de agremiaciones.
9. Distribuir información de Empresas Públicas de Armenia ESP que no sea considerada de uso público a otras Entidades o ciudadanos, sin la debida autorización de propietario del activo de información.
10. Envío o intercambio de mensaje con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.
11. Envío o intercambio de mensaje que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.
12. Envió de mensaje que contengan amenazas o mensajes violentos.
13. Crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor.
14. Divulgación no autorizada de información propiedad de Empresas Públicas de Armenia ESP.
15. Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.
16. Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado "Usos aceptable del servicio" de la presente política.

Enfoque Gestión Documental Física y Electrónica

Este enfoque tiene el propósito de establecer las condiciones de manejo de los archivos documentales generados en Empresas Públicas de Armenia ESP con colaboradores, consumidores y grupos de interés en Empresas Públicas de Armenia ESP.

Lineamientos sobre el manejo integral con gestión documental

1. El acceso al archivo central estará autorizado por el gestor del área de archivo central, el cual coordinará el debido acompañamiento para garantizar la seguridad de los activos.
2. Empresas Públicas de Armenia ESP deberá garantizar las condiciones de seguridad física y ambiental de las áreas de almacenamiento de activos. Así mismo, contará con equipos de almacenaje adecuados que permitan

la fácil ubicación, correcta custodia y minimicen los riesgos de accidente y daño.

3. Empresas Públicas de Armenia ESP, desde la Subgerencia Administrativa, debe garantizar las condiciones de seguridad física y ambiental del área de archivo, tales como ventilación, iluminación, temperatura y humedad. Contará al igual con equipos de almacenaje adecuados para los diferentes tipos de formatos que maneja Empresas Públicas de Armenia ESP (papel, cintas, fotografías, disquetes, CD, DVD, memorias extraíbles).
4. El acceso a la unidad de correspondencia está restringido, solo se permite el acceso al personal designado desde el área de Gestión de Recursos. Toda la documentación que deba ser radicada se debe entregar en la ventanilla destinada para tal fin, ubicada en el tercer piso del Centro Comercial del Café para su respectivo trámite.

Lineamientos sobre el manejo de documentos electrónicos

Referente al manejo general de documento electrónicos.

1. El Área de Archivo central es la responsable de establecer las condiciones de arquitectura de datos, manejo y gestión de los documentos electrónicos generados por la entidad.
2. Las comunicaciones electrónicas en lo posible, deben ser concretas, precisas y completas.
3. Solamente se considera oficial un mensaje de correo electrónico que incluya el nombre y el cargo del funcionario de la Secretaria de donde lo envía.
4. Las comunicaciones oficiales y circulares de la Empresas Públicas de Armenia ESP deben ser escaneadas y enviadas desde el correo electrónico de quien los elabora al funcionario autorizado de manejar la cuenta de comunicados Generales, y deben estar debidamente firmadas por el Secretario de Despacho.
5. Se deben conservar los niveles de seguridad en el manejo de la información electrónica conforme a los parámetros definidos institucionalmente para tal fin.
6. Los mensajes deben ser redactados de forma clara y concreta, evitando el uso de MAYÚSCULAS sostenidas, que, según normas internacionales de redacción en Internet, equivale a gritar.

Enfoque Gestión de Riesgos e Incidentes

Este enfoque permite establecer los lineamiento y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP apropiadas por todos los colaboradores (funcionario y contratistas) y proveedores, para la gestión de incidentes de seguridad y privacidad de la información.

Lineamientos sobre el mapeo y caracterización

1. Identificar a la Dirección TICs como primer y único punto de contacto para reporte de incidencias.
2. El reporte de cualquier incidencia se realizará únicamente por los siguientes medios de comunicación:
    a. Mesa de Ayuda – Dirección TICs, accediendo al sitio web www.intraepa.gov.co.
    b. Correo electrónico: atic@epa.gov.co
    c. Extensión: 1512-1513
3. Cada proceso es responsable de notificar a la dirección TICs las incidencias identificadas en los servicios de TI.
4. Empresas Públicas de Armenia ESP., desde el proceso de Dirección TICs deberá garantizar canales y vehículos de comunicación que permitan efectividad y eficiencia en la identificación y registro de las incidencias.
5. Toda incidencia identificada deberá ser registradas y categorizada bajo las tipologías definidas en la presente Política Interna de Seguridad y Privacidad de la Información.
6. El reporte de cinco (5) o más incidente del mismo tipo dará pie para que se declare como un incidente masivo.
7. Si un incidente es catalogado como masivo, su gestión deberá seguir el siguiente conducto regular:
    a. La Dirección TICs deberá notificar a la gerencia general.
    b. La Dirección TICs bajo autorización de la gerencia general, deberá notificar a todos los procesos la incidencia masiva presentada.
    a. La Dirección TICs deberá activar el *Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.*
    b. La Dirección TICs deberá notificar bajo el carácter de “emergencia” a los proveedores directamente vinculados al incidente masivo.
8. La Dirección TIC deberá apoyar a los procesos en la definición de un lenguaje de modelado que permita el mapeo y relacionamiento de los datos. Esto puede ser un Modelo Entidad-Relación, un diagrama de datos, un modelo de arquitectura de datos.
9. Los incidentes que en su identificación den origen a cambios en los ítems de configuración del servicio de TI serán atendido por medio de una *Solicitud de Cambios* descrito en el *Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.*
10. Los incidentes de TI asociados a Seguridad de Información serán gestionados mediante el *Procedimiento de Gestión de Incidentes de*

Seguridad y Privacidad de la Información.

11. La Dirección TICs deberá registrar en una bitácora todos los incidentes reportados con sus respectivos estados resolutivos.

Lineamientos sobre la priorización y diagnóstico preliminar

1. La Dirección TICs será la encargada de diagnosticar y priorizar las incidencias reportadas por los procesos y de establecer la forma de darle resolución.
2. La Dirección TICs deberá establecer, por medio propio o con el apoyo de proveedores si lo requiere, el origen del incidente.
3. La Dirección TICs asignará y notificará a quien, por competencia y responsabilidad, deba trabajar en resolver el incidente presentado.
4. La Dirección TICs deberá escalar cada incidente, dado el caso de cada incidente, al especialista responsable de garantizar la solución tecnológica afectada. Si el incidente es asignado a un proveedor, se deberá hacer efectiva aplicando lo que establece la Política Interna de Gestión de Proveedores.
5. La Dirección TICs, deberá mantener informados a los involucrados el estado del incidente, teniendo en cuenta parámetros de tiempos para cada actualización del reporte, los niveles de escalamiento para comunicación y conocimiento son:

Nivel	Tiempo de atención	Acciones	Área ~~a~~ *para* informar	Propósito
0	De 0-60 minutos de transcurrido el incidente.	El delegado de TI notificará vía telefónica el resumen del incidente y el tiempo de atención estimado.	Proceso directamente implicado en el incidente.	Que las áreas implicadas conozcan cómo actuar ante posible incidente y exista una comunicación asertiva hacia terceros.
1	De 61-100 minutos de transcurrido el incidente.	El delegado de TI notificará vía correo electrónico con resumen del incidente y el tiempo estimado según clasificación del incidente. Con recomendaciones de conducta sobre la situación.	Proceso directamente implicado en el incidente, Proceso jurídico y secretaria general.	Que las áreas de implicadas sepan cómo actuar sobre el incidente reportado.
2	De 101-179 minutos de transcurrido el incidente.	El Director TICs notificará vía circular a los directores implicados con resumen del incidente y el tiempo estimado de resolución según reportes del	Proceso directamente implicado en el incidente, Proceso jurídico y secretaria general.	Preparar acciones de contingencia sobre procesos vitales de Empresas Publicas de Armenia.

Nivel	Tiempo de atención	Acciones	Área ~~a~~ *para* informar	Propósito
		proveedor del servicio.	Gerencia General	
3	De 180 minutos en adelante de transcurrido el incidente.	Luego de tres (3) horas de detención de la operación, el incidente se convierte en problema y se efectúan las actividades del procedimiento de gestión e problemas, el director TICs comunicará al gerente general y demás procesos la situación y posibles tiempo de atención del problema para la generación de planes de contingencia.	Nivel directivo de todas las áreas de la entidad, todas los procesos y comunicación al ciudadano.	Gestionar el protocolo de contingencia ante la operación.

Lineamientos sobre la resolución y recuperación

1. Empresas Públicas de Armenia ESP., deberá identificar las causas del incidente para proceder a la debida solución.
2. Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, implementar una estrategia que permita la toma de decisiones oportuna con el fin de evitar la propagación de incidentes ya así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información.
3. Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, definir e implementar acciones contención que permita la oportuna detección de incidentes y evitar propagación a niveles masivo que afecten la integridad de la información.
4. Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, realizar una erradicación y eliminación de cualquier rastro dejado por el incidente.
5. Empresas Públicas de Armenia ESP., deberá realizar pruebas después de garantizar la erradicación completa del incidente.
6. Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, restablecer la funcionalidad de los sistemas afectados, y realizar un fortalecimiento del sistema que permita prevenir incidentes similares en el futuro.
7. Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, definir una ruta de continuidad del servicio suficientemente probado en los diferentes escenarios, como apoyo en la restauración de los servicios, sistemas y aplicativos.
8. Empresas Públicas de Armenia ESP., deberá revisar procesos,

procedimientos, lineamientos, entre otros, con el fin de determinar modificaciones para prevenir futuros incidentes.

Lineamientos sobre el cierre y seguimiento de incidentes

1. Cuando el incidente haya sido resuelto se registrará en la bitácora de incidentes establecida por la Entidad.
2. Los procesos o áreas afectadas deberán aplicar encuesta y/o cuestionario de satisfacción para verificar el estado del servicio y el desempeño y acompañamiento en la resolución del incidente.
3. Si el incidente es catalogado como masivo, el proveedor de servicios de TI deberá entregar un informe sobre la gestión del incidente y las recomendaciones pertinente para evitar nuevos eventos. Este informe será reportado en el seguimiento que se realiza desde el calendario establecido por Empresas Públicas de Armenia ESP.
4. La Dirección TICs deberá consolidar anualmente la información registrada en la bitácora y generar un reporte sobre las incidencias e incidencias masivas presentadas en Empresas Públicas de Armenia con su respetivo reporte resolutivo. Este informe deberá dar respuesta a las siguientes métricas:
    a. Número total de incidencias.
    b. Número y/o porcentaje de incidencias graves.
    c. El número y/o porcentaje de incidencias asignadas de manera incorrecta.
    d. El porcentaje de incidencias gestionadas en el plazo acordado.
    e. Lecciones aprendidas y acciones de mejora para la siguiente vigencia.

Enfoque Auditoria Gestión del Cambio y Mejoramiento Continuo

Este enfoque tiene el propósito de establecer las condiciones para el manejo de los eventos en mejora continua y gestión del cambio que se deben llevar a cabo en todos los procesos para el crecimiento y fortalecimiento de Empresas Públicas de Armenia ESP.

Lineamientos sobre la gestión de evento en TI

Estos lineamientos definen las condiciones para el registro, clasificación y manejo oportuno para la gestión de eventos en tecnologías de la información generados desde Empresas Públicas de Armenia ESP.

Referente al registro de evento de TI

1. Todo acceso de usuarios a los sistemas, redes de datos y aplicaciones

de Empresas Públicas de Armenia ESP, deben poder ser registrados y con posibilidad de consulta por personal autorizado.

2. Los logs de eventos requeridos deben ser revisado con regularidad por el personal de peritaje capacitado y autorizado.
3. Cada evento de auditoria deberá disponer de una copia de respaldo para consultar en casos de incidentes.

Referente al registro del administrador y del Operador

1. Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información de Empresas Públicas de Armenia ESP deben estar debidamente registradas.
2. Los administradores de la infraestructura tecnología y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.

Referente a la sincronización de relojes

1. Todos los relojes de la infraestructura de procesamiento de información de Empresas Públicas de Armenia ESP deben estar sincronizados con la hora legal Colombiana.

8. Instrumentos para la gestión de Seguridad y Privacidad de la Información

Empresas Públicas de Armenia ESP ha diseñado un Modelo de Madurez para dar cumplimiento a las Políticas Nacionales de Gobierno Digital y Seguridad y Privacidad de la Información y específicamente en la gestión de Seguridad y Privacidad de la Información. A continuación, se muestran los documentos para la gestión de Seguridad y Privacidad de la Información:

- Política Interna de Seguridad y Privacidad de la Información.
- Procedimiento de Seguridad y Privacidad de la Información. | En proceso
    - Enfoque Seguridad del recurso humano. | En proceso
    - Enfoque Gestión de activos de información. | En proceso
    - Enfoque Control de acceso. | En proceso
    - Enfoque Seguridad física y del entorno. | En proceso
    - Enfoque Seguridad de las operaciones. | En proceso
    - Enfoque Seguridad de las comunicaciones. | En proceso

- Enfoque Adquisición, desarrollo soporte y mantenimiento de sistemas de información. | En proceso
- Enfoque Gestión de incidentes de seguridad de la información. | *En proceso*
- Enfoque Gestión de continuidad de negocio. | *En proceso*

- Plan de Seguridad y Privacidad de la Información.
- Plan de Tratamiento de Riesgos de Seguridad de la Información.
- Catálogo de activos de Información.
- Plataforma Mesa de Ayuda -Intraepa.

9. Parámetros de estrategias de EIC (Educación, Información y Comunicación)

Empresas Públicas de Armenia ESP establece:

- Para estrategias de EIC a los grupos de interés e involucrados externos esto estará bajo la responsabilidad de Dirección de Comunicaciones, quien deberá formular estrategias y tácticas que permitan la socialización de los enfoques y lineamientos para resguardar la seguridad y privacidad de la información a los activos de información de Empresas Públicas de Armenia ESP.
- Para fines específicos de Educación la Gestión de Talento Humano con el apoyo de Dirección TIC, diseñará planes de capacitación y entrenamiento para los funcionarios y contratistas de la Empresas Públicas de Armenia ESP según las necesidades de formación para cumplir con los lineamientos nacionales establecidos en la Política de Gobierno Digital y Política de Seguridad Digital de Empresas Públicas de Armenia ESP de Tecnologías de la Información y las Comunicaciones.
- Ambas asignaciones contarán con la participación activa y acompañamiento de la Dirección TICs para lograr asertividad y pertenencia en la información divulgada.

10. Revisión y seguimiento al Sistema de Seguridad y Privacidad de la Información

La Gerencia General y el Comité de MiPG, deberá revisar periódicamente el desempeño y utilidad del Sistema de Gestión de Seguridad de la Información (SGSI) de Empresas Públicas de Armenia ESP, con el fin de verificar su conveniencia, suficiencia y eficacia. Entre otras esta revisión debe contemplar:

- Análisis de las oportunidades de mejora y la necesidad de cambios del SGSI,
- Revisión a la presente política de seguridad y los objetivos de seguridad.
- Revisión al seguimiento realizado por el área de Gestión Control
- Revisión de las normas, procedimientos, estándares, controles, formatos y procedimientos.
- Acople del SGSI con el Sistema de Gestión Integrado de Empresas Públicas de Armenia ESP.
- Revisión del listado maestro de documentos.

11. Cumplimiento

Empresas Públicas de Armenia ESP en manos de la Dirección TICs, responsable del Sistema Integrado de Seguridad de la Información, velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

El incumplimiento de los lineamientos descritos en la presente política, serán tratados por medio del procedimiento de incidentes de seguridad de la información, teniendo en cuenta la naturaleza del incidente y los resultados de su peritaje por parte del personal pertinente en cuyo caso particular, los responsables de los procesos evaluarán la necesidad de adelantar procesos disciplinarios o legales.

Cuando el incidente de seguridad de la información no esté calificado como un delito informático, las acciones disciplinarias o legales se adelantan de acuerdo con la competencia del código único disciplinario en el caso de servidores públicos o mediante los criterios definidos en los contratos de prestación de servicios en el caso de contratistas.

Dado el caso que se categorice el incidente como delito informático sobre lo establecido en la normatividad vigente y el peritaje técnico, el área jurídica, tomado como base el peritaje técnico formulará los pliegos pertinentes para iniciar las acciones legales ante la respectiva autoridad competente.

Esta Política Interna de Seguridad y Privacidad de la Información deberá revisarse y actualizarse cada año o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.

12. Declaración de publicación

La publicación de la Política Interna de Seguridad y Privacidad de la Información de Empresas Públicas de Armenia ESP. se realizará en:

1. El Sitio Web www.epa.gov.co una vez sea aprobada.
2. El Sistema de Gestión Integrado disponible en la Intranet. https://intraepa.gov.co/

La presente política rige a partir de su publicación.