Política de Gobierno y Gestión de TI

Empresas Públicas de Armenia ESP.

DIRECCIÓN TIC

Presentado por Ingeniero:

Cesar Iván López Bedoya
Director TICs

ARMENIA QUINDÍO.
30 de Noviembre de 2023

Tabla de contenido

1. Introducción ____ ***4***

2. Alcance ____ ***5***

3. Glosario ____ ***5***

4. Objetivos ____ ***26***

4.1. Objetivo General ____ **26**

4.2. Objetivo Especifico ____ **26**

5. Componentes de la Política de Gobierno y Gestión de TI ____ ***27***

5.1. Principios de Gobierno y gestión de TI ____ **27**

5.2. Ecosistema de Involucrados Empresas Públicas de Armenia ESP ____ **29**

5.3. Estructura de gobierno en Gobierno y gestión de TI ____ **29**

6. Enfoques de la Política de Gobierno y Gestión de TI ____ ***32***

Política General de Gobierno y Gestión de TI ____ **34**

Alcance/Aplicabilidad ____ 35
Nivel de cumplimiento ____ 35
Lineamientos Generales ____ 35

Enfoque Gobierno de TI ____ **39**

Lineamientos generales de Gobierno de TI ____ 39
Lineamientos sobre el Marco Operativo de Gobierno de TI ____ 39

Enfoque Gestión Humana ____ **41**

Lineamientos sobre la gestión de contratistas frente al gobierno y gestión de TI ____ 42
Lineamientos sobre las responsabilidades del Líder de Proyectos de TI ____ 42
Lineamientos sobre responsabilidades de los usuarios frente al gobierno y gestión de TI ____ 43

Enfoque Estrategia de TI ____ **45**

Lineamientos sobre la formulación de planes de gestión TI ____ 45
Lineamientos sobre la gestión de proyectos de TI ____ 46

Enfoque Servicios tecnológicos y Sistemas de Información ____ **47**

Lineamientos sobre gestión de recursos y servicios tecnológicos ____ 47
Lineamientos sobre gestión de software y sistemas de información ____ 50

Enfoque Datos e Información ____ **53**

Lineamientos sobre gestión y gobierno de la información ____ 53
Lineamientos sobre el respaldo de la información ____ 54

Enfoque Datos abiertos ____ **54**

Lineamientos sobre la captura, almacenamiento y manipulación de los datos ____ 55
Lineamientos sobre la calidad de los datos ____ 55
Lineamientos sobre la divulgación, acceso y uso de los datos abiertos ____ 55
Lineamientos sobre incentivos para el desarrollo de proyectos e iniciativas que promueva el uso de los datos abiertos ____ 56

Enfoque Uso, Apropiación y Capacidades institucionales ____ **56**

Lineamiento para el uso y apropiación de capacidades de TI. ____ 56

Lineamientos sobre la gestión de capacidades institucionales _____ 57

Enfoque Gestión de Proveedores de TI _____ 58

Lineamientos sobre gestión de la relación con Contratista Proveedores y/o terceros_____ 58

Enfoque Auditoria Gestión del Cambio y Mejoramiento Continuo _____ 60

Lineamiento sobre la Gestión de Cambios _____ 60

Lineamientos sobre la continuidad del negocio _____ 61

7. Instrumentos para la gestión de Gobierno y gestión de TI _____ 62

8. Parámetros de estrategias de EIC (Educación, Información y Comunicación) __ 62

9. Revisión y seguimiento al Sistema de Gobierno y gestión de TI _____ 63

10. Cumplimiento_____ 63

11. Declaración de publicación _____ 63

Este color indica que es información para complementar
Este color indica que es algo para analizar
Este color indica que es que se trabaja y se decide si se involucra o no
Este color indica que el texto aun requiere revisión.

1. Introducción

Hoy en día hablamos de la trasformación organizacional y la importancia de un pensamiento colectivo que lleve las organizaciones a un siguiente nivel, para entregar valor y beneficios agregados a la comunidad y grupos de interés. De igual manera cada día es más clara la responsabilidad de las entidades públicas en desarrollar acciones para construir y fortalecer territorios inteligentes para entregar bienestar, aplicando una filosofía de un gobierno abierto transparente, inclusivo y con apertura a decisiones colectivas.

Desde Empresas Públicas de Armenia ESP entendemos este propósito global, y nos conectamos con las acciones que nos lleve a garantizar en nuestro territorio un desarrollo sostenible y para esto es fundamental que trabajemos en estar conectado para ser pertinentes.

Para lograr todo esto es fundamental caminar hacia la transformación digital de nuestros procesos y operaciones. Llegar a eso requiere contar con estrategias de alto nivel que permitan la gestión efectiva a través de la habilitación y puesta en marcha de una Ruta de Madurez Digital que permita la gobernanza y gestión de los recursos y servicios tecnológicos, así como los sistemas de información, garantizando que la entidad pueda generar y entregar 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 gobierno y gestión de TI obedece también al cumplimiento de la normativa nacional en su política de Gobierno Digital y Seguridad Digital 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 gobierno y gestión de TI.
- Componente de gestión y gobierno en gobierno y gestión de TI.
- Lineamientos en el manejo y gestión de la Política de Gobierno y Gestión de TI desde Empresas Públicas de Armenia ESP.

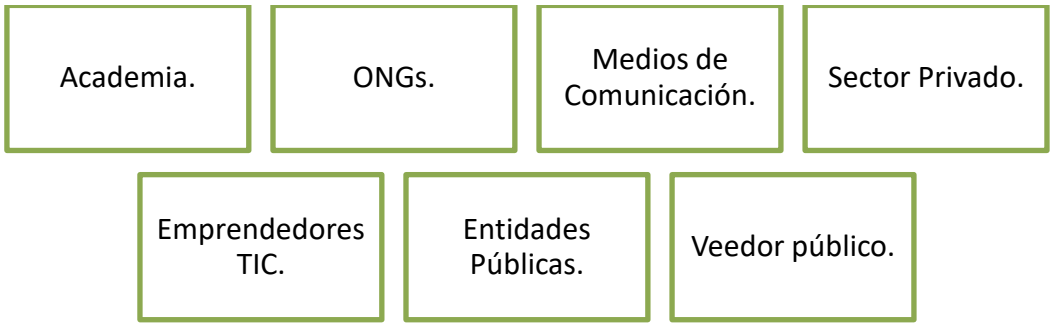
Contar con esta Política de Gobierno y Gestión de TI nos permite tener un conducto regular sobre la forma en que Empresas Públicas de Armenia ESP puede actuar y comportarse con el fin de gestionar los recursos y servicios tecnológicos, con los sistemas de información.

2. Alcance

Este documento contempla la descripción de lineamientos y conducto regular interno referente al Gobierno y Gestión de las Tecnologías de la Información en Empresas Públicas de Armenia ESP.

La Política de Gobierno y Gestión de TI es aplicable en toda la cadena de valor de TI que demanda Empresas Públicas de Armenia ESP, estableciendo acciones de atención para el gobierno, planeación, adquisición, instalación, manejo, y continuidad TI y destinación final de la Información, Sistemas de Información, Servicios Tecnológicos en la entidad.

La política interna 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 físico**: Significa ingresar a las áreas de misión crítica o instalaciones en general de un sitio de la entidad.
- **Acceso lógico**: En general, el acceso lógico es un acceso en red, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos. La mayoría de los accesos lógicos se relacionan con algún tipo de información.
- **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.
- **Acción correctiva:** Remediación de los requisitos o acciones que dieron

origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

- **Acción preventiva:** Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.
- **Aceptación de riesgo**: Decisión de asumir un riesgo.
- **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.
- **Actualidad:** Vigencia de la información.
- **Acuerdos de Confidencialidad:** Es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- **Acuerdos de Intercambio de información:** Es un contrato legal entre al menos dos entidades para compartir información o conocimiento para ciertos propósitos, donde se definen las responsabilidades de protección que se le deberá dar a dicha información.
- **Acuerdos de Niveles de Servicio:** Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho
- **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.
- **Adaptabilidad:** Define que todos los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior.
- **Administrador:** Toda persona responsable por la operación día a día de un sistema de cómputo o red de cómputo.
- **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.
- **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.
- **Alta Dirección**: Se considera Alta Dirección a los directivos con cargo más alto en una organización; el Presidente, el Gerente General y los Directores de las distintas áreas. En el caso de la Empresas Públicas de Armenia ESP se entiende como Alta Dirección a la integrada por la Superintendente y el Comité Directivo.

- **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.
- **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y para estimar el riesgo (Guía ISO/IEC 73:2002).
- **Anonimizar:** Proceso para remover datos personales de una base de datos, buscando la publicación segura de datos para reutilizarlos.
- **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.
- **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
- **Arquitectura Empresarial:** Conjunto de elementos organizacionales (estrategia, estructura, procesos más tecnología, personas) que se relacionan entre sí, garantizando la alineación desde los niveles más altos (estratégicos), medios (tácticos), hasta los más bajos (operativos), con el fin de optimizar la generación de productos y servicios que conforman la propuesta de valor entregada a los clientes.
- **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.
- **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.

- **Big data:** es un término en desarrollo que describe un gran volumen de datos estructurados, semiestructurados y no estructurados que tienen el potencial de ser extraídos para obtener información y usarse en proyectos de aprendizaje automático y otras aplicaciones de análisis avanzado.
- **Buzón:** espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros**.**
- **Calidad de datos:** La Guía Técnica de información G.Inf. 06 lo define como: es el ámbito enfocado en el aseguramiento de la calidad para garantizar la prestación de servicios de información e institucionales, a través de la identificación y propuesta de mejoras, la modificación del modelo operativo y la actualización y verificación del cumplimiento de los indicadores de calidad definidos para el dato
- **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 Datos Abiertos:** el inventario único de los conjuntos de datos puestos a disposición de la población, en el portal de internet datos.gob.mx, por las dependencias y entidades de la Administración Pública Federal, así como por las empresas productivas del Estado.
- **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.
- **Ciberespacio:** ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.
- **Cifrado:** Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave (llave criptográfica) necesaria para descifrarlos.
- **Cifrar:** Es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) que transforma la información, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta.

- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un cuerpo integrado por representantes designados por la Alta Dirección con el objetivo de garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- **Compatibilidad:** el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad.
- **Completitud:** Información plenamente diligenciada.
- **Comprensibilidad:** Entendimiento e interpretación adecuada de la información por parte de un usuario.
- **Computación en la nube (Cloud Computing):** Es un término utilizado para describir servicios proporcionados a través de una red por una colección de servidores remotos. Esta "nube" abstracta de computadoras proporciona una gran capacidad de almacenamiento distribuido y de procesamiento a la que se puede acceder desde cualquier dispositivo conectado a Internet que ejecute un navegador web.
- **Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.
- **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.
- **Consistencia:** Datos coherentes y libres de contradicción.
- **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.
- **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.
- **Credibilidad:** Información veraz y confiable para los usuarios.
- **Criterios para adquisición de tecnología:** condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología, como:
- **Criticidad:** Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
- **CSV (Valores separados por coma):** Formato abierto y sencillo para representar datos en formato de tabla, en columnas separadas por comas (o punto y coma, donde la coma es el separador decimal) y las filas son saltos de línea. Los campos que tienen una coma, un salto de línea o una comilla doble, deben cerrarse entre comillas dobles. Las extensiones que se utilizan son .csv y .txt.
- **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.
- **DAFP:** Departamento Administrativo de la Función Pública
- **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.
- **Dato Abierto:** 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 Personales:** información que contiene elementos que al unirse pueden caracterizar a un individuo, por ejemplo, número de cedula, dirección, tipo de sangre, teléfono, etc.
- **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.
- **Declaración de aplicabilidad**: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.
- **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 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.
- **Desarrollador**: Persona que apoya el desarrollo de alguna de las fases del ciclo de vida del desarrollo de software para la Empresas Públicas de Armenia ESP y que puede trabajar directamente para la Empresas Públicas de Armenia ESP (planta, contratista, estudiante en práctica) o través de una empresa externa.
- **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.
- **Desviación (Seguridad de la Información**): Malas prácticas adelantadas por las personas y que generan posibles incidentes o riesgos.
- **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.
- **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.
- **Dispositivo móvil:** Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria Son ejemplos de estos: celulares inteligentes, tabletas y portátiles
- **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.
- **Encriptación**: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.
- **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.
- **Estación de trabajo:** Área dispuesta por la Empresas Públicas de Armenia ESP para que cada colaborador pueda llevar a cabo sus actividades. Tales como oficinas, escritorios entre otros.
- **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:** 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 Gobierno y Gestión de TI 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
- **Freeware:** Software de libre distribución.
- **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.
- **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 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.
- **Habeas data:** Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
- **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**: Es una 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.
- **ICQ:** Programa de mensajería instantánea en línea desarrollado por Mirabilis LTD. Es usado como una herramienta de conferencia en la red para pláticas electrónicas vía teclado ("chatear"), mandar correos electrónicos y ejecutar transferencias de archivos, jugar juegos de computadoras, etc.
- **Impacto:** el costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad d la información.
- **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.

- **Interoperabilidad:** es la capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios digitales a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas TIC.
- **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)
- **IPS:** Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.
- **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 del tipo daemon (demonio), es decir, actúa como un proceso 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.
- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
- **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.
- **Lista blanca**: Es una lista o registro de entidades que, por una razón u otra, pueden obtener algún privilegio particular, servicio, movilidad, acceso o reconocimiento.

- **Llaves criptográficas:** Son códigos (algoritmos) que se generan de forma automática y se guarda en un directorio especial durante la instalación. 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.
- **Log**: es un registro oficial de eventos durante un rango de tiempo en particular. Se usa para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
- **Lugar seguro:** es aquel que protege el activo de información de acceso de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos son: cajón seguro con llave, oficina con llave, etc.)
- **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.
- **Metadato:** Los metadatos son "datos sobre datos" - es decir, los datos que describen los aspectos básicos de un conjunto de datos, por ejemplo, cuando se creó el conjunto de datos, cuál es la agencia responsable de la base de datos, el formato de los datos, etc.
- **MSPI:** Es el Modelo de Gobierno y gestión de TI definido por el Ministerio de Tecnologías de la Información – MINTIC.
- **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).
- **Norma:** Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **OEM:** Un fabricante de equipos originales (OEM) fabrica piezas o componentes que se utilizan en los productos de otra empresa. Un componente de OEM puede ser una pieza, un subsistema o software. Algunos ejemplos son los sistemas operativos y los microprocesadores en equipos. Por lo general, el fabricante de equipos no fabrica ni el microprocesador ni el SO. En su lugar, el fabricante de equipos compra estas piezas de otras empresas como OEM. En este sentido, OEM también puede ser un verbo: "comprar como OEM una pieza" de otra empresa.
- **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.
- **Personal:** Es aquella persona que tiene una relación con la Empresas Públicas de Armenia ESP directa o a través de un tercero, bajo cualquier tipo de vinculación Planta, contratistas, estudiantes en práctica, etc.
- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.
- **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.
- **Política:** actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.
- **Portabilidad:** Característica que garantiza que cualquier conjunto de datos esté representado en un Formato sin restricciones para la reutilización de este.
- **Principios de Seguridad de la información:** Confidencialidad, disponibilidad e integridad.
- **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.
- **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:** Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.
- **Red:** Es un sistema de comunicación que se da entre diversos recursos informáticos por medio de protocolos para permitir el intercambio de información.
- **Registro:** Documento que presenta resultados obtenidos o proporcionar evidencia de actividades desempeñadas.
- **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.
- **Relevancia:** Utilidad para los usuarios.
- **Reportes o salidas:** se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.
- **Requerimiento:** Necesidad de un servicio TIC que el usuario solicita a

través del mecanismo definido por la organización en los procedimientos normalizados.

- **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 de Seguridad TIC:** En Empresas Públicas de Armenia ESP el comité de seguridad de la información será el grupo encargado de realizar el seguimiento y monitoreo al Sistema de Gestión de la Seguridad de la información (SGSI).
- **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.
- **RFC:** Los documentos RFC (Request for Comments) han sido utilizados por la comunidad de Internet como una forma de definir nuevos estándares y compartir información técnica. Investigadores de universidades y corporaciones publican estos documentos para ofrecer mejores prácticas y solicitar comentarios sobre las tecnologías de Internet. Las RFC son administradas hoy por una organización mundial llamada Internet Engineering Task Force (IETF).
- **Riesgo Inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control
- **Riesgo residual:** Nivel restante de riesgo después del tratamiento del riesgo.
- **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 TIC:** Incluye los servicios profesionales para la instalación, mantenimiento, desarrollo, integración de software y adquisiciones, enajenaciones, arrendamientos y contratación de Hardware y soporte tanto de software como de hardware.
- **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:** 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.)
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen en la entidad.
- **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.
- **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.
- **Tecnología de la Información:** Se refiere al hardware y software operado por el organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad.
- **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.
- **Texto plano:** es un archivo informático que contiene únicamente texto formado solo por caracteres que son legibles por humanos, careciendo de cualquier tipo de formato tipográfico. También son llamados archivos de texto llano, simple o sin formato.
- **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.
- **Token**: Es un dispositivo que genera códigos de acceso que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
- **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.

- **Trasferencia de información:** Intercambio de información entre áreas internas de la Entidad o entre la Empresas Públicas de Armenia ESP y terceras partes.
- **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.
- **URL (localizador de recursos uniforme)**: Es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo con un formato modélico y estándar, que designa recursos en una red.
- **Usabilidad:** Significa facilidad de uso, atributo de calidad, que identifica el grado en que un producto puede ser usado por determinados usuarios para lograr sus propósitos con eficacia, eficiencia y satisfacción en un contexto de uso específico
- **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.
- **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.
- **XLS:** la extensión de archivo por defecto del formato propietario de Excel.
- **XLSX:** es la extensión de archivo de Excel, en su versión de formato abierto. Ésta cumple con la característica de seguir el estándar abierto Office Open XML.

4. Objetivos

4.1 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 el gobierno y gestión de componentes de las Tecnologías de la Información que permitan llevar la entidad a los ideales de Transformación y crecimiento organizacional, 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.

4.2 Objetivo Especifico

En el marco de la Política de Gobierno y Gestión de TI se plantean los siguientes objetivos específicos:

- Establecer el ecosistema de gobierno y gestión de TI con los involucrados de tipo Core, Directo e Indirecto.
- Establecer un modelo de gestión para el Gobierno y gestión de TI en Empresas Públicas de Armenia ESP.
- Establecer los componentes significativos asociados a la Política de Gobierno y Gestión de TI.
- Describir las buenas prácticas aplicables a las condiciones actuales de

Empresas Públicas de Armenia ESP para la gestión de Gobierno y gestión de TI.

- Definir los enfoques y lineamientos de la Política de Gobierno y Gestión de TI.
- Promover el uso adecuado de los recursos humanos, materiales y activos tecnológicos adecuados.
- Definir parámetros de estrategias de EIC (Educación, Información y Comunicación) para la gestión de la Gobierno y gestión de TI.
- Garantizar la continuidad de negocio frente a la operación demandada de las Tecnologías de la Información para el crecimiento tecnológico de Empresa Públicas de Armenia.

5. Componentes de la Política de Gobierno y Gestión de TI

Esta Política de Gobierno y Gestión de TI describe las directrices, normas, lineamientos y buenas prácticas, con el propósito de gestionar la gobernanza del Modelo de Madurez Digital definido para Empresas Públicas de Armenia ESP para lograr eficiencia y calidad en los servicios y tramites desde las Tecnologías de la Información.

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

5.1. Principios de Gobierno y gestión de TI

El Modelo de Arquitectura de TI establece que los principios[1] definidos para la garantía de Gobierno y gestión de TI son en el marco de la presente política son:

[1] Definición tomada de: https://www.mintic.gov.co/arquitecturati/630/articles-144767_recurso_pdf.pdf

Excelencia del servicio al ciudadano	Fortalecer de forma digital la relación de los ciudadanos con el Estado enfocándose en la generación de valor público sobre cada una de las interacciones entre ciudadano y Estado
Costo / Beneficio	El criterio de selección de un proyecto de TI debe priorizar el valor público por encima de su costo, de tal forma que se garantice que las inversiones en TI tengan un retorno definido por el beneficio.
Excelencia del servicio al ciudadano	Fortalecer de forma digital la relación de los ciudadanos con el Estado enfocándose en la generación de valor público sobre cada una de las interacciones entre ciudadano y Estado.
Costo / Beneficio	El criterio de selección de un proyecto de TI debe priorizar el valor público por encima de su costo, de tal forma que se garantice que las inversiones en TI tengan un retorno definido por el beneficio.
Racionalización	Optimizar el uso de los recursos de TI teniendo en cuenta criterios de pertinencia y reutilización, sin perjuicio de la calidad el servicio y de la operación de la entidad.
Estandarización	Definir un ecosistema tecnológico estandarizado para controlar la diversidad tecnológica, la complejidad técnica y reducir los costos asociados al mantenimiento de la operación.
Interoperabilidad	Utilizar los estándares que fortalezcan la plena interoperabilidad entre los sistemas de información e infraestructura tecnológica y que faciliten el intercambio de información entre las entidades y los sectores.
Co-Creación	Componer soluciones y generar servicios sobre lo ya construido y definido, con la participación de todos los interesados (internos y externos) para garantizar su máximo valor.
Calidad	Cumplir con los criterios y atributos de calidad definidos para los procesos y soluciones de TI construidas para la entidad.
Seguridad Digital	Establecer la seguridad y privacidad de la información teniendo en cuenta los lineamientos definidos en la Política de Gobierno Digital.
Sostenibilidad	Definir las acciones que propendan por el cumplimiento de los objetivos de desarrollo sostenible de las Naciones Unidas
Neutralidad tecnológica	Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes en la materia, fomentando la eficiente prestación de servicios, el empleo de contenidos y aplicaciones, la garantía de la libre y leal competencia mediante criterios de selección objetivos.

Foco en las necesidades	Las decisiones sobre el ecosistema tecnológico deben enfocarse en responder y dar solución las necesidades de la Entidad.
Vigilancia tecnológica	Realizar vigilancia tecnológica sobre las tendencias de la industria TI para evaluar su oportunidad en la solución a necesidades de la Entidad.

5.2. Ecosistema de Involucrados Empresas Públicas de Armenia ESP

Empresas Públicas describe a continuación su ecosistema de involucrados:

- **Involucrado Core:** Fundamentales en la cadena de valor de Empresa Públicas de Armenia, 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

5.3. Estructura de gobierno en Gobierno y gestión de TI

La gestión de las competencias y capacidades en Gobierno y Gestión de TI 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 en la implementación de mejoras que nos lleve al siguiente nivel en la transformación y escalabilidad del negocio.

Se deben definir claramente todas las responsabilidades en cuanto a la gobernanza y gestión de TI, en especial las relacionadas con el comité de MiPG de Gobierno Digital

Este componente define los roles y responsabilidades en Gobierno de TI, específicamente con respecto a la protección de los activos de información.

La gobernanza en Gobierno y Gestión de TI 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 Gobierno y Gestión de TI. – Supervisar la implementación de los lineamientos, procedimientos y planes asociados a la Política de Gobierno y Gestión de TI. – Proponer estrategias y soluciones específicas para la incorporación de los controles necesarios para implementar los lineamientos establecidos y la debida solución de las situaciones de riesgo detectadas. – Reportar al Director TICs, respecto a oportunidades de mejora en materia de Gestión y Gobierno de TI. – Arbitrar conflictos en materia de adquisición, habilitación, mantenibilidad y continuidad de soluciones y servicios de TI.	Comité MiPG
2	Responsable de Garantizar Cumplimiento. – Aprobar los lineamientos de la Política de Gestión y Gobierno de TI. – Evaluar el proceso de gestión y gobierno de TI. – Definir las estrategias y mecanismos para la continuidad del negocio desde el área de TI. – Facilitar los recursos requeridos para garantizar gobierno de TI.	Gerencia General
3	Gestión estratégica y técnica en Gobierno y gestión de TI - Gestión de la Política. - Gestión de Procedimientos e Instrumentos. - Gestión del Plan de Gobierno y gestión de TI. - Garantizar el cumplimiento de los requerimientos de gobierno y gestión de TI que demanda la presente política y demás documentos vinculantes normativos y técnicos de orden territorial y nacional. - Gestión estratégica y técnica de todos los enfoques de la política. - 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.	Dirección de Tecnologías de la Información y las Comunicaciones.

N°	Responsabilidad	Área/Procesos
	- Monitorear el estado, nivel de aplicación de la política en la entidad. - Organizar las actividades del Comité MiPG en materia de seguridad de la información. - Apoyar a los diferentes procesos institucionales en la adopción del Gobierno de TI definido para la entidad. - Compartir e intercambiar información acerca de nuevas tecnologías, productos que mejoren el desempeño del área de TI de Empresas Públicas de Armenia ESP.	
4	- Garantizar el cumplimiento legal de la Política de Gobierno y Gestión de TI 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 gobierno y gestión de TI. - Asesorar legalmente en las acciones de Gobierno y gestión de TI que se requieran en Empresas Públicas de Armenia ESP y determinar las pautas legales que permitan cumplir con los requerimientos legales en esta materia. - Determinar las consecuencias jurídicas que se podrán presentar sobre incumplimiento o desacato de las responsabilidades en la gestión de TI.	Dirección Jurídica y Secretaria General
5	- Incluir en el plan de capacitación anual temáticas asociadas a la gestión y gobierno de TI. (Ver Modelo de Transferencia de Capacidades de TI) - Fomentar la participación de los colaboradores (funcionarios y contratistas) y proveedores en las acciones de Educación, Información y Comunicación que definan. - Garantizar cumplimientos de los lineamientos, procedimientos y planes asociados a la Gobierno y gestión de TI del Talento Humano. - Notificar a todo el Talento Humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Gobierno y Gestión de TI y de todas las normas, procedimientos y prácticas que de ella surjan. - Apoyar en la resolución de conflictos interno asociados con violaciones u omisiones de la presente política.	Gestión del Talento Humano
6	Difusión de información de carácter público a grupos de interés referente a la presente política. - Diseño de estrategias de EIC para capacitar a los colaboradores y proveedores. - Difusión de material publicitario e informativo sobre las responsabilidad y gestión efectiva de incidentes que se presenten.	Dirección de Comunicaciones
7	Acompañar en la formulación y articulación de los documentos estratégicos de gestión y gobierno de TI: – Ruta de Madurez Digital. – Plan Estratégico de Tecnologías de la Información y las Comunicaciones. – Plan de Seguridad y Privacidad de la Información. – Plan de Gestión del Riesgos de Seguridad y Privacidad.	Dirección de Planeación Corporativa

N°	Responsabilidad	Área/Procesos
8	– Seguimiento al desempeño en la gestión y gobierno de TI. – 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 gestión y gobierno de TI 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 MiPG.	Dirección Control de Gestión
9	- Aplicar buenas prácticas en Gestión y Gobierno de TI. - 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 de Gobierno y Gestión de TI vigente, los procedimientos vinculantes y las normas asociadas.	Todos los procesos.

Fuente: Guía Roles y Responsabilidades del Modelo de Gobierno y gestión de TI. Elaborado por el MinTIC.

6. Enfoques de la Política de Gobierno y Gestión de TI

A continuación, se describen los lineamientos de cumplimiento para la Política de Gobierno y Gestión de TI de Empresas Públicas de Armenia ESP, clasificados en ## enfoques de aplicación.

Enfoques de la Política de Gobierno y Gestión de TI

Enfoque	Lineamientos	Referentes	Cantidad de Ítems
Política General de Gobierno y Gestión de TI	Lineamientos Generales.		34
Enfoque Gobierno de TI.	Lineamientos generales de Gobierno de TI.		8
	Lineamientos sobre el Marco Operativo de Gobierno de TI		16
Enfoque Gestión Humana	Lineamientos sobre la gestión de contratistas frente al gobierno y gestión de TI		8
	Lineamientos sobre las responsabilidades del Líder de Proyectos de TI		5
	Lineamientos sobre responsabilidades de los usuarios frente al gobierno y gestión de TI		
		Referente al uso de equipos de cómputo, dispositivos portátiles y móviles	9

Enfoque	Lineamientos	Referentes	Cantidad de Ítems
		Referente al uso de Software y Sistemas de Información	5
		Referente a la gestión de usuarios a nivel de base de datos	7
Enfoque Estrategia de TI	Lineamientos sobre la formulación de planes de gestión TI		4
		Referente a Inversiones y Costos de TI	3
	Lineamientos sobre la gestión de proyectos de TI		9
		Referente a la participación de los otros procesos.	7
Enfoque Servicios tecnológicos y Sistemas de Información	Lineamientos sobre gestión de recursos y servicios tecnológico.		7
		Referente a las adquisiciones de Recursos Tecnológicos	4
		Referente a la custodia de recursos tecnológicos	4
		Referente al control y mantenimiento de Infraestructura Tecnológica	6
		Referente a equipos y servicios de cómputo	4
		Referente al soporte de TI a los usuarios	3
	Lineamientos sobre gestión de software y sistemas de información		-
		Referente a la Adquisición y Custodia Software	9
		Referente al Desarrollo de software	13
		Referente a la educción y especificación de requerimientos	3
		Referente al diseño de software	3
		Referente a la documentación del software	4
		Referente a las pruebas de software y garantía de calidad	4
Enfoque Datos e Información	Lineamientos sobre gestión y gobierno de la información		1
	Lineamientos sobre el respaldo de la información		9
Enfoque Datos abiertos	Lineamientos sobre la captura, almacenamiento y manipulación de los datos		4
	Lineamientos sobre la calidad de los datos		3
	Lineamientos sobre la divulgación, acceso y uso de los datos abiertos		9
	Lineamientos sobre incentivos para el desarrollo de proyectos e iniciativas que promueva el uso de los datos abiertos		3
Enfoque Uso, Apropiación y Capacidades institucionales	Lineamiento para el uso y apropiación de capacidades de TI.		3

Enfoque	Lineamientos	Referentes	Cantidad de Ítems
	Lineamientos sobre la gestión de capacidades institucionales		3
Enfoque Gestión de Proveedores de TI	Lineamientos sobre gestión de la relación con Contratista Proveedores y/o terceros		8
		Referente a Servicios Tercerizados o en Outsourcing.	15
Enfoque Auditoria Gestión del Cambio y Mejoramiento Continuo	Lineamiento sobre la Gestión de Cambios.		10
	Lineamientos sobre la continuidad del negocio.		7
		TOTAL:	254

Política General de Gobierno y Gestión de TI

La Dirección TICs de Empresas Públicas de Armenia ESP, entendiendo la importancia de establecer e implementar un Modelo de Gobierno y Gestión de TI que permitiera desde la tecnología impulsar el crecimiento del negocio, hacia lo establecido hoy como la Transformación Digital.

Esta Política de Gobierno y Gestión de TI está en la ruta de lo establecido a nivel nacional por el Ministerio de las Tecnologías de la Información y las Comunicaciones que contempla un enfoque para el fortalecimiento de las capacidades de liderazgo estratégico de TI para gestionar y gobernar las Tecnologías de la Información (TI) de forma adecuada y de esta forma ofrecer mejores servicios a los ciudadanos cumpliendo con la Política de Gobierno Digital.

Para Empresas Públicas de Armenia ESP, la declaración de esta política busca establecer parámetros claros de gestión que den cumplimiento a la demanda de nuevas soluciones, acorde con las necesidades de los diferentes grupos de interés identificados.

Este Modelo de Gobierno y Gestión de TI es creado con la intención organizacional de definir las bases para gestionar de manera adecuada y efectiva, las acciones de TI que se realizan en la entidad.

Empresas Públicas de Armenia ESP ha decidido definir, implementar, operar y mejorar de forma continua el Modelo de Gobierno de TI, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios, así como los procedimientos, documentos de

trabajo, sistemas de información y recursos tecnológicos habilitados para los involucrados core.

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 describen lineamientos generales para el Gobierno y Gestión de TI en Empresas Públicas de Armenia ESP:

1. Los proyectos de tecnologías de información de cada proceso o áreas de Empresas Públicas de Armenia ESP, deben estar establecidos en el Plan Estratégico de TI como documento primario y oficial para el Gobierno del Modelo de Madurez Digital Empresas Públicas de Armenia ESP, cumpliendo con todos los requisitos en el mapeo de proyectos de TI.
2. Los recursos informáticos y de comunicaciones solo pueden ser utilizados por los usuarios y contratistas u otros usuarios que cuentan con la debida autorización de la Dirección TICs para su gestión en beneficio de la misión de la Entidad.
3. La Dirección TICs debe realizar la divulgación de la Política de Gobierno y Gestión de TI para conocimiento de todos los procesos y áreas de la entidad, incentivando el uso de racional y responsable de los recursos tecnológicos y sistemas de información por todos los involucrados en Empresas Públicas de Armenia ESP.
4. Todas las dependencias que requieran desarrollar proyectos que involucren el uso de recursos tecnológicos deben ser informados a la Dirección TICs y ser desarrollado bajo la estructura metodológica definida por Empresas Públicas de Armenia ESP, previa aprobación de la viabilidad de su ejecución.
5. Todas las solicitudes para mantenimiento y gestión de los equipos de cómputo y demás recursos de tecnologías incluidos servicio de voz y datos deben ser comunicados a través de la mesa de ayuda.
6. Dirección TICs realizará seguimiento periódico al estado y vida útil de los recursos tecnológicos para su debido reemplazo contemplando los lineamientos de depreciación tecnológica.

7. Dirección TICs realizará seguimiento periódico al estado y oportunidad de los sistemas de información según lo demanda el negocio para su debida actualización contemplando los lineamientos de obsolescencia tecnológica.
8. La Dirección TICs planificará las adquisiciones, la actualización, ampliación o desarrollo de las TICs de acuerdo a los criterios establecidos en esta política. La Dirección TICs hará la recopilación de las necesidades y propondrá el Plan Estratégico de Tecnologías de la Información y la Comunicaciones -PETI- con una vigencia operativa establecida a necesidad de la gestión.
9. Los Procesos y áreas de las sedes distintas a la principal, informarán a la Dirección TICs el estado de los equipos y necesidades TIC con el fin de velar porque los equipos y recursos informáticos se encuentren en condiciones operativas, según demanda de uso y consumo.
10. La Dirección TICs debe velar por la debida privacidad y confidencialidad de los datos registrados en los sistemas de información y en general en la plataforma e infraestructura tecnológica y solo se permitirá el acceso a información propia de los usuarios de la Entidad cuando sea solicitado de manera formal por una autoridad competente y con la respectiva justificación. Para más detalle consultar la Política Interna de Seguridad y Privacidad de la Información.
11. Todo proceso o área de Empresas Públicas de Armenia ESP que necesite adquirir, desarrollar e implementar sistemas de información debe incluirlo reportarlo a la Dirección TICs por medio de los instrumentos habilitados; En caso de ser necesario, solicitar acompañamiento para la formulación de la propuesta o solicitud, según los procedimientos establecidos. La omisión de este lineamiento, llevará a la no responsabilidad por parte de Empresas Públicas de Armenia ESP ante reclamos de cualquier proveedor de TI por los requerimientos que se generen como legalizar las licencias, ni tampoco de dar soporte o mantenimiento de ese producto.
12. Todo Sistemas de información en uso por Empresas Públicas de Armenia ESP deben cumplir con los requisitos de ley asociados al cumplimiento de derechos de autor, así como de conformidad a las condiciones pactadas en el contrato que se lleve a cabo entre las partes.
13. Toda actualización o mejora que se vaya a realizar a los sistemas de información en uso de Empresas Públicas de Armenia ESP debe cumplir con los estándares establecidos para el desarrollo y operación de los sistemas de información; los cuales deben estar documentados y evaluados en forma permanente por la Dirección TICs.
14. Todo sistema de información o aplicación que requiera actualización o mejora debe cumplir con la política detallada, con el procedimiento definido y debe tener ambiente de desarrollo, de pruebas y de producción los cuales serán adecuados por la Dirección TICs.

15. La interventoría de los contratos de soporte y mantenimiento de los sistemas de información o aplicación que se encuentren en producción y apoyen la gestión misional del Empresas Públicas de Armenia ESP debe estar a cargo de la Dirección TICs o su delegado.
16. Todos los procesos responsables de los sistemas de información a su uso para su gestión en Empresas Públicas de Armenia ESP son responsables del contenido y actualización permanente de los datos que capturan e ingresan a los aplicativos para ejecutar las funciones asignadas.
17. El mantenimiento de los equipos de cómputo, impresoras y periféricos demás recursos tecnológicos de propiedad de Empresas Públicas de Armenia ESP se deben realizar de acuerdo con los lineamientos establecidos por la Dirección TICs.
18. La Dirección TICs debe tener la administración, control y optimización de los canales tecnológicos que permitan Internet y WAN en todas las sedes de Empresas Públicas de Armenia ESP y debe seguir los estándares y procedimientos que definan para este asunto.
19. La Dirección TICs debe definir el esquema de las redes LAN y de la plataforma e infraestructura tecnológica en todas las sedes de Empresas Públicas de Armenia ESP y debe seguir los estándares y procedimientos que defina.
20. Toda ampliación y/o modificación del cableado estructurado debe realizarse con los lineamientos, estándares y procedimientos que la Dirección TICs establezca.
21. Todo proyecto relacionado con el cableado estructurado debe ser informado a la Dirección TICs y contar con su apoyo en cumplimiento de los lineamientos y procedimientos establecidos.
22. La Dirección TICs debe elaborar la política detallada de seguridad y privacidad de la información; como lineamientos y mecanismos de seguridad para proteger la información y velar para que se establezcan acciones de protección, detección de ataques informáticos y establecer los procedimientos de recuperación de los sistemas en caso de que ocurra un incidente.
23. La Dirección TICs debe proveer los lineamientos y mecanismos de seguridad para proteger la información y velar para que se establezcan acciones de protección, detección de ataques informáticos y la creación de procedimientos de recuperación de los sistemas en caso de que ocurra un incidente.
24. La Dirección TICs debe mantener actualizado para su uso y gestión el inventario de tecnologías de la información, el cual contempla Activos de Información y Sistemas de Información y Recursos tecnológicos.
25. La Dirección TICs es la responsable para adquirir, actualizar y administrar las licencias de uso de software.

26. Todo equipo de cómputo propiedad de Empresas Públicas de Armenia ESP contará únicamente con software licenciado, de uso libre comercialmente, términos de uso o algún documento que sirva de soporte legal.
27. Todas las Licencias del software adquiridas por Empresas Públicas de Armenia ESP a través de compra, donación o cesión son de uso exclusivo la Entidad.
28. Todo el software propiedad de Empresas Públicas de Armenia ESP debe ser usado exclusivamente para asuntos relacionados con las actividades de la entidad
29. Empresas Públicas de Armenia ESP, no se hace responsable del software ilegal que sea encontrado en algún equipo asignado a un funcionario; por lo tanto, toda la responsabilidad civil, económica y penal recaerá sobre el servidor público cuando se le haya comprobado su falta.
30. Todo computador que esté conectado o no a la red institucional debe tener instalado un único software antivirus y debe corresponder al Institucional.
31. La Dirección TICs establecerá protocolo de seguridad de la información para mantener libre de virus informáticos los equipos de cómputo
32. Esta rotundamente restringido la manipulación de los equipos de cómputo por parte del usuario para acciones de reparación, ampliaciones o actualizaciones de recursos informáticos.
33. Cada usuario con equipo de cómputo asignada es el responsable del cuidado de los recursos informáticos e insumos que le sean suministrados para la ejecución de sus funciones.
34. Cualquier situación no prevista en los presentes lineamientos será resuelta por La Dirección TICs de Empresas Públicas de Armenia ESP, algunas por su naturaleza requerirán de la aprobación explícita de Direccionamiento Gerencia.

El incumplimiento a la Política de Gobierno y Gestión de TI, 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 Gobierno y gestión de TI se refiere.

Enfoque Gobierno de TI

Este enfoque tiene el propósito de establecer las condiciones de operación para garantizar la adecuada gobernanza de TI en Empresas Públicas de Armenia ESP.

Lineamientos generales de Gobierno de TI

1. La Dirección de TICs es responsable de todas las acciones de TI desde su gobierno hasta la garantía de oportunidad y uso para garantizar la continuidad del negocio en su camino a la trasformación digital.
2. Empresas Públicas de Armenia ESP debe establecer el conducto regular para la toma de decisiones respecto al gobierno y gestión de las TI en la entidad.
3. Empresas Públicas de Armenia ESP establece que la Dirección TICs es el área responsable de la gestión y gobierno de las políticas nacionales en Gobierno Digital, Seguridad Digital y las demás consideradas bajo la competencia de TI, así como de garantizar el cumplimiento normativo que demande el sector TI para entidades públicas que cobije nuestra categoría de entidad.
4. Empresas Públicas de Armenia ESP deberá establecer un comité directivo para fortalecer la estructura de gobernanza de TI y toma de decisiones en alineación con la Política de Gobierno Digital y Seguridad Digital definidos por el MinTIC.
5. Dirección TICs debe definir mecanismos para la alineación estratégica del crecimiento y escalabilidad de TI con las megas y propósito de Empresas Públicas de Armenia ESP, articulando objetivos, metas, e indicadores en la línea de crecimiento que posea la entidad.
6. Dirección TICs deberá determinar mecanismos que permitan la gestión adecuada de riesgo de TI, mitigando los riesgos que se puedan presentar y siendo efectivos en la resolución de incidentes en TI.
7. Dirección TICs determinará los mecanismos para la gestión integral de los recursos tecnológicos de TI que posee Empresas Públicas de Armenia ESP
8. Dirección TICs determinará los mecanismos que permitan medir el desempeño y resultados en las acciones de TI en Empresas Públicas de Armenia ESP

Lineamientos sobre el Marco Operativo de Gobierno de TI

1. Dirección TICs debe establecer un marco de gestión y gobierno de TI basado en el diseño y habilitación de políticas, estrategias, modelos,

procesos, procedimiento, formatos de trabajo para la operatividad integral del área de TI, todo alineado con MiPG.

2. La Dirección TICs debe establecer una estructura de gobernanza en TI que defina el conducto regular para la toma de decisiones, según sus prioridades de oportunidad.
3. Dirección TICs debe definir y comunicar la estructura organizativa de TI que incluya:
    a. Esquema de Gobierno de TI.
    b. Cadena de Valor de TI .
    c. Mapeo de componentes de gestión de TI
    d. Mapeo de Funciones, roles y responsabilidades
    e. Mapeo de Procesos y procedimientos para el gobierno de TI.
4. La Dirección de TI debe establecer procesos y procedimientos que permitan determinar de manera continua la demanda de soluciones de TI para soportar las necesidades de áreas y procesos de Empresas Públicas de Armenia ESP.
5. Se debe trabajar continuamente en el desarrollo y fortalecimiento de la Arquitectura Empresarial de la Entidad.
6. La Dirección TICs debe garantizar y gestionar los siguientes planes:
    a. El Plan Estratégico de Tecnologías de la Información y las Comunicaciones a nivel Institucional.
    b. El Plan de Seguridad y Privacidad de la Información.
    c. El Plan de Gestión del Riesgo de Seguridad y Privacidad de la Información.
7. La Dirección TICs debe garantizar la oportunidad en el uso y acceso a las plataformas, servicios tecnológicas y sistemas de información que Empresas Públicas de Armenia ESP demande para cumplir su función.
8. La Dirección TICs debe definir, planificar, implementar y realizar seguimiento a los recursos tecnológicos y sistemas de información en propiedad y custodia de la entidad.
9. La Dirección TICs debe investigar, evaluar, definir, aprobar y monitorear la adquisición y renovación de bienes y servicios tecnológicos de Empresas Públicas de Armenia ESP, dando cumplimiento a los parámetros legales vigentes que apliquen.
10. La Dirección TICs debe investigar, evaluar, definir, aprobar y monitorear la adquisición y renovación de software y sistemas de información de Empresas Públicas de Armenia ESP, dando cumplimiento a los parámetros legales vigentes que apliquen.

11. La Dirección TICs deberá establecer un modelo que permita la transferencia y apropiación de Capacidades y competencias en TI al personal de Empresas Públicas de Armenia ESP para fortalecer el uso y apropiación en TI. Este modelo entre otras cosas permitirá:
    a. El Alcance en temáticas de formación en TI.
    b. El mapeo de necesidades de formación en TI.
    c. Las condiciones de selección de capacitadores y talleristas.
12. La Dirección TICs es la responsable de establecer las condiciones de operación y comportamientos permitidos por los usuarios en el uso de recursos tecnológicos y sistemas de información, así como la manipulación de activos de información.
13. La Dirección TICs deberá garantizar las condiciones de captura y custodia de los activos de información y niveles de confidencialidad de los datos, así como los datos abiertos.
14. Empresas Públicas de Armenia ESP es propietaria de todos los activos tecnológicos y de información adquiridos o capturados con base a las disposiciones aquí establecidas, esto a menos que se indique explícitamente lo contrario.
15. La Dirección TICs es la única área de Empresas Públicas de Armenia ESP autorizada para avalar la contratación de cualquier servicio tecnológico y/o sistema de información requerido, incluyendo, pero sin limitar, internet, servicios en nube, telefonía, impresión y otros servicios relacionados con tecnologías de información.
16. La Dirección TICs no será responsable de ningún recurso tecnológico o sistema de información que esté por fuera de los parámetros establecidos en las políticas aquí consagradas.

Enfoque Gestión Humana

La Garantía de una buena implementación de la Ruta de Madurez Digital 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 gobierno y gestión de TI.

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 Gobierno y gestión de TI.

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

Lineamientos sobre la gestión de contratistas frente al gobierno y gestión de TI

1. Para la vinculación de contratistas es fundamental que la persona natural y jurídica realicen el procedimiento de vinculación de proveedores ante la entidad.
2. Empresas Públicas de Armenia ESP debe verificar y validar los documentos de vinculación entregados.
3. Los contratos de prestación de servicios donde se quiera acceso a la gestión de activos de información, el supervisor del mismo deberá establecer cuáles son los permisos de acceso que entrega y el alcance de privilegios.
4. El supervisor del contrato deberá realizar la solicitud de cuentas de usuario a las plataformas o herramientas que requiera el contratista mediante la Mesa de Ayuda, para lo cual debe proporcionar los datos del contratista y del contrato.
5. Si el contrato establece que la Entidad debe proporcionar el equipo de cómputo, el supervisor del contrato debe realizar la solicitud a la Dirección TICs para que se verifique su disponibilidad y proceda a su entrega. El equipo de cómputo proporcionado al contratista debe quedar a cargo del supervisor del contrato.
6. Para los contratos con personas jurídicas, en el caso de requerirse, el supervisor debe realizar la solicitud de la cuenta de usuario proporcionando los datos del contrato y de las personas que tendrán a cargo dichas cuentas de usuario.
7. Al momento de terminar el plazo de ejecución del contrato, el supervisor del mismo debe solicitar la suspensión de la cuenta(s) de usuario asociada(s) al contrato. Si se asignó equipo de cómputo al contratista, el supervisor debe realizar la devolución del bien en el estado en el que se le entregó
8. Todo contratista oficialmente vinculado 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 gobierno y gestión de TI.

Lineamientos sobre las responsabilidades del Líder de Proyectos de TI

1. El líder de proyectos de TI debe apoyar los proyectos presentados y aprobados por el Gobierno de TI, partiendo de la definición de la arquitectura de la solución y estructurándolos desde los componentes de la solución.

2. El líder de proyectos de TI debe reportar al Director TICs el estado de los proyectos actuales en las sesiones requeridas. El líder deberá entender el objetivo de cada proyecto, cual es el valor que promete generar y por qué es importante para Empresas Públicas de Armenia ESP.
3. Apoyar al líder del área beneficiaria en la evaluación técnica y financiera y de factibilidad de los proyectos para su correcta priorización a nivel institucional, la cual está basada en la contribución de beneficios de cada proyecto.
4. Estimar los esfuerzos y recursos humano, tecnológicos y financieros que se requieran para la ejecución del proyecto de TI con el propósito de presentarlo en las sesiones de Comité MiPG.
5. El Líder de Proyectos no requiere conocer el detalle técnico del área beneficiaria, pero si debe comprender como se conecta la tecnología en la solución que están queriendo encontrar, entender los objetivos y situaciones problémicas, y la forma en que estos impactan Empresas Públicas de Armenia ESP en toda su Cadena de Valor.

Lineamientos sobre responsabilidades de los usuarios frente al gobierno y gestión de TI

Referente al uso de equipos de cómputo, dispositivos portátiles y móviles

1. Mantener limpios los espacios donde se encuentren ubicados los servicios tecnológicos.
2. No se permite la realización de modificaciones a la configuración de los servicios tecnológicos asignados, sin el conocimiento y la debida autorización de la Dirección TICs.
3. No se permite la conexión o desconexión de hardware de los equipos de cómputo, sin autorización de la Dirección TICs.
4. Los equipos de cómputo asignados no son para realizar actividades ociosas en la Internet que puedan generar inconvenientes y saturaciones en el ancho de banda de la Empresas Públicas de Armenia ESP.
5. No se permite que a través de los servicios tecnológicos a los que se tiene acceso se generen ataques a otros equipos internos o externos.
6. Para acceder a los recursos de infraestructura de TI, los usuarios deben contar con una cuenta de correo y una clave de acceso, la cual es confidencial e intransferible. El dueño de la cuenta es responsable de mantener la confidencialidad de la contraseña, de hacer uso adecuado de la misma y de responder sobre todas las actividades que ocurran bajo su cuenta.
7. Los usuarios deben mantener limpias las áreas donde se encuentren los equipos de cómputo.
8. Cualquier incidencia sobre los equipos de cómputo y acceso a la red de datos, debe ser reportado a la Dirección TICs, para apliquen la solución pertinente.
9. No se debe conectar o desconectar hardware externos al equipo de

cómputo sin autorización de la Dirección TICs.

Referente al uso de Software y Sistemas de Información

1. No puede realizar instalaciones de software sin contar con la aprobación de la Dirección TICs.
2. Todo usuario que requiera el uso de una licencia de software deberá realizar la solicitud de manera anticipada ante La Dirección TICs a través de la mesa de ayuda, de acuerdo a los niveles de servicios establecidos en el proceso de licenciamiento.
3. Una vez aprobada la compra por parte de La Dirección TICs, es La Dirección TICs la responsable de ingresar la solicitud de compra en el sistema designado para tal fin.
4. La Dirección TICs debe garantizar que la solicitud para la adquisición y/o renovación del software o licencia sea coherente con el ejercicio presupuestal. Dado el caso de requerir la compra o renovación de un software o licencia que no fue presupuestado, el área solicitante, debe justificar la razón por la cual no fue incluido en presupuesto, adjuntar la autorización del Director del proceso pertinente y buscar los recursos económicos requeridos.
5. Es responsabilidad de cada área solicitante, en caso de identificar componentes de Sistemas de Información, software e infraestructura de TI, en solicitudes cuya naturaleza no sean de tecnología, notificar a La Dirección TICs para su respectivo análisis.

Referente a la gestión de usuarios a nivel de base de datos

1. La solicitud de creación, modificación, inactivación o retiro de cuentas de usuario para cualquier Software o sistema de información vinculado a Empresas Públicas d Armenia ESP, debe realizarse a la Dirección TICs por medio de la mesa de ayuda.
2. Para la creación de la cuenta de usuarios, es necesario y obligatorio tener el acuerdo de confidencialidad debidamente firmado y anexarlo escaneado a la solicitud.
3. La solicitud deberá contener la siguiente información: Nombre del software o sistema de información, privilegios que se le deben asignar al usuario (sobre objetos, del sistema, sobre roles).
4. Las cuentas de usuario de Base de Datos son de carácter confidencial y no pueden ser compartidas, cualquier mal uso de la cuenta será responsabilidad de la persona a la que se le asignó, no debe utilizar cuentas genéricas. Es responsabilidad de cada servidor público y/o contratistas hacer buen uso del usuario de base de datos.
5. La configuración y administración las cuentas de usuario de base de datos es responsabilidad del Administrador de Base de Datos de la entidad, el cual debe llevar el registro de las cuentas de usuario por base de datos: datos del usuario, fecha de creación, fecha de actualización, fecha de

eliminación, servidor público que realizó la solicitud.

6. El uso de los privilegios dados a cada usuario puede ser auditado cuando se considere necesario o por solicitud explicita del responsable técnico y/o funcional del sistema de información y/o la aplicación correspondiente.
7. La Dirección TICs deberá disponer de un registro con los usuarios y privilegios otorgados al personal de Empresas Públicas de Armenia ESP, este registro será de carácter confidencial y se deberá garantizar la privacidad y seguridad de dicha información.

Enfoque Estrategia de TI

Este enfoque tiene el propósito de establecer las condiciones de operación para la gestión estratégica en planes y proyectos de TI en Empresas Públicas de Armenia ESP.

Lineamientos sobre la formulación de planes de gestión TI

1. Dirección TICs debe coordinar y gestionar la formulación y definición de los objetivos y propósitos de TI a largo plazo que están alineados con las intenciones de continuidad y crecimiento del negocio de Empresas Públicas de Armenia ESP.
2. La Dirección TICs debe definir mantener actualizados y en seguimiento los Planes de gestión de TI establecidas bajo la Ruta de Madurez Digital
3. Dirección TICs de la mano con Dirección de Comunicaciones debe establecer estrategias y acciones de EIC (Educación, Información y Comunicación) para la difusión y socialización de los planes, modelos, programas que se definan en competencias de TI.
4. Dirección TICs definirá de manera anual los Planes Operativos Anuales que describan las acciones priorizadas de intervención para soportar la continuidad del negocio.

Referente a Inversiones y Costos de TI

1. Se debe crear y mantener el presupuesto para TI basado en el presupuesto por resultados y alineado a los planes estratégicos y operativos.
2. Se deben modelar y asignar los costos de las TI en base a los servicios de tecnologías que se prestan.
3. Se deben gestionar los costos procurando la racionalización de los recursos y considerando al costo total de propiedad a los activos.

Lineamientos sobre la gestión de proyectos de TI

1. La Dirección TICs debe establecer el estándar para la gestión de programas y proyectos que serán llevados por la Dirección TICs a través del ciclo de vida del proyecto y los procesos relacionados.
2. La Dirección TICs debe establecer una metodología estandarizada para la gestión de proyectos de TI. Dicha metodología deberá tener los debidos procedimientos, guías, manuales e instrumentos de trabajo.
3. Todo proyecto de TI deberá estar registrado en el banco de proyectos de TI vinculado al Plan Estratégico de TI – PETI-.
4. La Dirección TICs debe generar un Acta de Constitución del Proyecto en base al enunciado del trabajo del proyecto emitido.
5. La Dirección TICs apoyará al área promotora del proyecto en gestionar el compromiso de las partes interesadas mediante un plan que incluya a todos los miembros de los equipos del proyecto, ejecutores y asesores para determinar los requisitos del proyecto y las expectativas de todas las partes involucradas y asegura el éxito del proyecto.
6. La Dirección TICs deberá incluir el desarrollo del plan para la dirección del proyecto y las actividades que forman parte de las áreas de conocimiento para la Gestión del Alcance, Gestión del Tiempo, Costos, Calidad, Recursos Humanos, Comunicaciones, Riesgos, adquisiciones y los interesados del proyecto.
7. La dirección TICs deberá garantizar la adecuada gobernanza y seguimiento del proyecto durante el proceso de ejecución, realizar el aseguramiento de la calidad, adquirir, desarrollar y dirigir el equipo del proyecto, gestionar las comunicaciones, realizar las adquisiciones y gestionar la participación de los interesados.
8. La Dirección TICs debe garantizar condiciones para garantizar el monitoreo y control del trabajo del proyecto, realizar el control integrado, validar el alcance del proyecto, controlar el alcance, controlar el cronograma, controlar los costos, controlar la calidad, controlar las comunicaciones, controlar los riesgos, controlar las adquisiciones, y controlar la participación de los interesados e Informar los resultados al comité estratégico del programa y a los patrocinadores.
9. La Dirección TICs al finalizar el proyecto es responsable de elaborar un informe de cierre para informar que los procesos definidos se han completado, realizando las actividades necesarias para asegurar el cierre de las adquisiciones y establecer formalmente que el proyecto o fase del mismo ha finalizado.

Referente a la participación de los otros procesos

1. Cada área o proceso debe asignar el Líder Técnico de Proyecto según la temática que corresponda para trabajar en conjunto con el líder de proyecto de TI designado por La Dirección TICs.
2. El Líder Técnico de Proyecto designado deberá apoyar, realizar recomendaciones y manifestar riesgos frente a las iniciativas presentadas

durante la fase de priorización y aprobación de los proyectos.

3. El proceso beneficiario debe garantizar la disponibilidad de los recursos financieros y humanos requeridos para la ejecución de los proyectos aprobados en comité.
4. El proceso beneficiario debe conocer e informar el estado y avance del proyecto que se encuentra en ejecución donde esté participando directamente.
5. El proceso beneficiario debe participar de manera activa y directa en las actividades que demande la continuidad del proyecto requeridas por los proyectos a ejecutar en alianza con La Dirección TICs.
6. El proceso beneficiario debe acatar las directrices de priorización y asignación de recursos para proyectos por parte del gobierno de TI.
7. El proceso beneficiario debe velar en conjunto con el líder de Proyecto de TI para que los beneficios y objetivos de los proyectos se mantengan durante la ejecución del proyecto y se materialicen.

Enfoque Servicios tecnológicos y Sistemas de Información

Este enfoque permite establecer los lineamientos y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP en la gestión de Servicios Tecnológicos y Sistemas de Información.

Lineamientos sobre gestión de recursos y servicios tecnológicos

1. La Dirección TICs es responsable de asignar, configurar, modificar y brindar asesoría sobre el uso y acceso a los servicios tecnológicos de Empresas Públicas de Armenia ESP.
2. La Dirección TICs debe configurar cada equipo con los servicios tecnológicos que demande cada procesos y área en su actividad para la entidad.
3. La Dirección TICs es la responsable de gestionar los servicios tecnológicos de la entidad, bajo ninguna circunstancia se entrega el control y gobierno a terceros.
4. La Dirección TICs deben establecer Acuerdos de Nivel de Servicio - ANS, para cada uno de los servicios que ofrece la Dirección TICs.
5. Todo servicio tecnológico, debe incluir una estrategia de gestión del cambio organizacional que permita la gestión del impacto y los intereses de los usuarios del servicio, que garanticen el uso y apropiación de este.
6. Gestión de Talento Humano debe formular e implementar con el apoyo de Dirección TICs un plan de transferencia de capacidades de TI por cada proyecto de implementación de los servicios tecnológicos, que fortalezca las competencias de los usuarios (funcionarios, contratistas y terceros), y garantice el uso y apropiación de la solución tecnológica.

7. La Dirección TICs, podrá modificar o suspender los servicios tecnológicos de manera parcial o total a uno o varios de los funcionarios, contratistas y terceros, cuando se requiera por motivos de seguridad, por mantenimiento de los servicios preventivo o correctivo, o por causas de fuerza mayor.

Referente a las adquisiciones de Recursos Tecnológicos

1. Toda la adquisición de infraestructura debe estar contemplada en el Plan de Compras de la entidad, el plan de gestión de la infraestructura tecnológica, el PETI y debe estar sujeta a los procedimientos establecidos por la Empresas Públicas de Armenia ESP. No obstante, de acuerdo con necesidades de la Entidad, será posible la adquisición de hardware que no estuviera inicialmente previsto.
2. Cualquier necesidad de adquisición de las dependencias deben ser gestionadas en coordinación con la Dirección TICs, previa validación de la infraestructura actual para identificar la disponibilidad de esta, el plan de gestión de la infraestructura tecnológica y no generar gastos a la entidad.
3. Las adquisiciones de la infraestructura deben generarse como una solución integral de la Empresas Públicas de Armenia ESP, se deben establecer como obligatorio la adquisición de las pólizas necesarias, velar por cubrir las necesidades de la adquisición de repuestos y el mantenimiento de la infraestructura.
4. La adquisición de la Infraestructura se debe priorizar en los fabricantes con presencia en el país y con capacidad de brindar soporte técnico garantizado. De igual manera, se pueden realizar adquisiciones por empresas distribuidoras nacionales e internacionales, debidamente autorizadas por los fabricantes y así poder garantizar el soporte técnico.

Referente a la custodia de recursos tecnológicos

1. La Dirección TICs es al responsable de la custodia de los activos fijos tecnológico, mediante los procesos establecidos y aprobados por el Sistema de Gestión Integrado.
2. La Dirección TICs es responsable de garantizar que los activos físicos tecnológicos estén protegidos de los riesgos del entorno físico y lógico.
3. La Dirección TICs, es quien define los activos físicos tecnológicos que deben ser dados de baja según lo establece los procedimientos aprobados en el Sistema de Gestión Integrado, por su nivel de obsolescencia, por no encontrarse aptos para su funcionamiento y por no poder realizarle un efectivo mantenimiento.
4. Los funcionarios, contratistas y terceros que tengan bajo su custodia los equipos de cómputo son responsables de su buen uso y deben atender la normatividad establecida por la Empresas Públicas de Armenia ESP. Los equipos de cómputo, pueden ser reasignados según las necesidades para

la ejecución de las actividades de cada uno de los funcionarios, contratistas o terceros de la entidad.

Referente al control y mantenimiento de Infraestructura Tecnológica

1. La Dirección TICs, debe elaborar, actualizar y mantener el plan de gestión de la infraestructura tecnológica de la Empresas Públicas de Armenia ESP.
2. Los mantenimientos preventivos o correctivos sobre la infraestructura tecnológica de la Empresas Públicas de Armenia ESP, deben ser planeados, coordinados, comunicados y ejecutados por la Dirección TICs.
3. La Dirección TICs, debe gestionar la configuración sobre cada uno de los componentes de la solución de TIC, como se establece en el procedimiento.
4. La Dirección TICs, debe realizar el monitoreo continuo de los servicios
5. tecnológicos y validar el cumplimiento de los ANS de cada uno de ellos.
6. Es de obligatorio cumplimiento la adquisición de las pólizas de garantía sobre toda la infraestructura tecnológica que se adquiera en la Empresas Públicas de Armenia ESP.

Referente a equipos y servicios de cómputo.

1. La asignación de los equipos de cómputo y el acceso a la red de datos, debe ser realizada por la Dirección TICs. La asignación debe ser a personal de la Empresas Públicas de Armenia ESP (funcionarios, contratistas o terceros).
2. Los usuarios, que requieran apoyo u orientación en el manejo y gestión de los equipos de cómputo asignados y la información que contengan, deben solicitar el mismo a la Dirección TICs.
3. Los equipos de cómputo y el acceso a la red de datos, no pueden ser utilizados para fines personales o de ocio. Las actividades a realizarse sobre estos equipos y la red deben relacionarse a los programas y proyectos administrativos y misionales de la Empresas Públicas de Armenia ESP.
4. La instalación de licenciamiento en cada uno de los equipos de cómputo debe ser realizado o autorizado por la Dirección TICs de la Empresas Públicas de Armenia ESP.

Referente al soporte de TI a los usuarios

1. La Empresas Públicas de Armenia ESP, por medio de la Dirección TICs, debe garantizar una única mesa de ayuda como canal oficial para atender los incidentes y requerimientos sobre los servicios de TIC de acuerdo con el catálogo de servicios de la Empresas Públicas de Armenia ESP y los Acuerdos de Nivel de Servicio - ANS establecidos para cada uno de ellos.
2. La mesa de ayuda, debe mantener informado a los usuarios solicitante de

la evolución de sus requerimientos. Si el requerimiento no puede ser implementado en los tiempos establecidos en los ANS, el usuario debe ser informado.

3. La Dirección TICs debe garantizar la resolución de incidentes y eventos de TI que se presenten, para ellos debe seguir los lineamientos establecidos en la Política de Seguridad y Privacidad de la Información.

Lineamientos sobre gestión de software y sistemas de información

La Dirección TICs es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo, actualizaciones e instalaciones del software de la Empresas Públicas de Armenia ESP. De igual manera, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de colocar en producción.

Referente a la Adquisición y Custodia Software

1. Toda adquisición de software debe estar contemplada en el Plan de Compras de la entidad, el PETI, alineado a la arquitectura de sistemas de información y debe estar sujeta a los procedimientos establecidos por la Empresas Públicas de Armenia ESP y deben ser aprobadas por la Dirección TICs. Es posible, que, por necesidad de la Entidad, se requiera la aprobación de la adquisición de software no previsto.
2. Cualquier necesidad de adquisición de las dependencias deben ser gestionadas en coordinación con la Dirección TICs, previa validación del software actual, la arquitectura de sistemas de información y la capacidad instalada, para identificar la disponibilidad de esta y no generar gastos a la entidad.
3. La adquisición de software debe realizarse a empresas, proveedora de productos de alta calidad y con respaldo técnico.
4. La adquisición de nuevo software, debe contar con una etapa de verificación (estudio previo) por parte de la Dirección TICs, para determinar que no existe una solución al interior de la entidad que cubra la necesidad, que el software es integrable con los sistemas existentes en la entidad y si la solución puede ser del mercado o a la medida.
5. La Dirección TICs es la responsable de la administración del software (sistemas operativos, aplicativos, utilitarios, administradores de bases de datos, lenguajes de programación, a la medida) de uso de la Empresas Públicas de Armenia ESP. De igual manera, debe mantener actualizado el inventario del software y su licenciamiento.
6. Los desarrolladores de loa Empresas Públicas de Armenia ESP y terceros, no deberán tener acceso a información de producción que contenga datos sensibles.
7. Se debe establecer un acuerdo previo con los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la

información manejada en el proyecto.

8. Los accesos al código fuente y los archivos del sistema, se debe encontrar restringido.
9. Las actualizaciones del software deben ser realizadas por los administradores de estos al interior de la Empresas Públicas de Armenia ESP, siguiendo las indicaciones establecidas en los controles de cambio debidamente documentados.

Referente al Desarrollo de software

1. El desarrollo de software a la medida se deberá efectuar a través de contratación de personal externo a la entidad y deberá ser supervisado por el área que suscriba el contrato, con el acompañamiento de la Dirección TICs.
2. Las áreas usuarias del software que se encuentre en desarrollo deben participar activamente desde el inicio hasta la terminación de todo el proceso.
3. La Dirección TICs debe velar que el software adquirido o desarrollado pueda integrarse con los sistemas de información existentes y que este orientado a la utilización de la plataforma de interoperabilidad del Estado.
4. La adquisición o desarrollo de Software deberá implementarse según lo establecido en el ciclo de vida, criterios de seguridad y de calidad en el desarrollo de software.
5. Las áreas usuarias del software en desarrollo son responsables, con la orientación de la Dirección TICs, de ejecutar las pruebas y posterior aprobación requeridas antes de la entrega definitiva y puesta en producción del software.
6. Se debe tener a disposición ambientes de desarrollo o pruebas representativas, previas a la implantación definitiva del software y ambientes de producción; es decir, de utilización definitiva claramente diferenciados.
7. Cuando se requiera realizar el desarrollo de un software nuevo, la Dirección TICs debe verificar, mediante un estudio o análisis previo, que la solución no va a generar duplicidad de tareas.
8. Los desarrollos realizados deben dar cabal cumplir con los requerimientos de desarrollo seguro establecidos por la Dirección TICs con la Política de Seguridad de la Información, definidas en la Empresas Públicas de Armenia ESP.
9. Los desarrollos de software realizados por los funcionarios, contratistas o terceros, en la ejecución de sus obligaciones será de propiedad intelectual de la Empresas Públicas de Armenia ESP, salvo si en sus obligaciones o alcance indica lo contrario.
10. No se permite, que los funcionarios, contratistas o terceros de la Empresas Públicas de Armenia ESP, realicen copias del software con el que se relacionan, o cedan autorización de acceso a terceros al software de propiedad intelectual o con licencia de uso de la Empresas Públicas de Armenia ESP.

11. Toda modificación de software crítico bien sea por actualizaciones o modificaciones, deberá ser analizada previamente en ambientes independientes de desarrollo y prueba, con el objetivo de identificar y analizar los riesgos de seguridad que acarrea dicha modificación.
12. La Dirección TICs, debe velar por la gestión de configuración y el control de versiones de los diferentes softwares, según lo establezca el procedimiento.
13. Los cambios de versiones deben ser planeados y acordados conjuntamente con el área usuaria y la Dirección TICs.

Referente a la educción y especificación de requerimientos

1. La Dirección TICs, debe garantizar la disponibilidad de una Mesa de Ayuda como canal único para dar correcta atención a los requerimientos de los usuarios de la Empresas Públicas de Armenia ESP de acuerdo con el catálogo de servicios de TIC ofrecido, para generar una respuesta oportuna, teniendo en cuenta los acuerdos de nivel de servicio ofrecidos.
2. De igual manera, proveerá información del estado de evolución del requerimiento al usuario solicitante. Si existe la posibilidad que durante la gestión del requerimiento no se dé cumplimiento a los Acuerdos de Niveles de Servicio, se debe comunicar al usuario solicitante.
3. La Dirección TICs, debe proveer a las áreas usuarias de instrumentos para la especificación de los requerimientos, según se define en el procedimiento.

Referente al diseño de software

1. Los niveles de confidencialidad del software, se definirá teniendo en cuenta la criticidad de la información que se gestione en este software. Los gestores de bases de datos, deben garantizar el nivel de protección adecuado.
2. Todo software crítico para la Empresas Públicas de Armenia ESP deberá incluir la generación de registros de auditoría, considerando como mínimo la identidad del usuario que lee, borra, escribe, o actualiza, el tipo de evento y la fecha y hora del evento. Estos registros deben ser protegidos contra la manipulación no autorizada.
3. En la etapa de diseño se deberá proyectar el rendimiento esperado, con el objetivo de no sobre dimensionar los recursos necesarios para el funcionamiento del sistema (ancho de banda, RAM, recursos del servidor, etc.).

Referente a la documentación del software

1. El diccionario de datos, o repositorio de metadatos, deberá mantener una descripción actualizada de las definiciones de datos.
2. Si el desarrollador incluye comentarios en el programa fuente, estos no deben divulgar información de configuración innecesaria.

3. Todo sistema desarrollado por la Empresas Públicas de Armenia ESP debe generar el protocolo de las condiciones de autenticación a la aplicación, el cual deberá ser revisado y aprobado por el equipo de seguridad de la información.
4. La documentación de los desarrollos deberá:
    a. Generarse durante el ciclo de vida de desarrollo y no postergarla hasta el final.
    b. Ser revisada por los usuarios finales del sistema en desarrollo.
    c. Actualizarse si el programa cambia alguna de sus funcionalidades.
    d. Almacenarse en un sitio centralizado (Servidor) administrado por la subdirección de desarrollo de aplicaciones.

Referente a las pruebas de software y garantía de calidad

1. Se deberán planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas antes y después, y criterios de aceptación del cambio.
2. Para propósitos de desarrollo y pruebas de software, se deberán generar datos de prueba distintos a los que se encuentran en el ambiente de producción.
3. En lo posible, las pruebas del sistema deberán incluir: instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores.
4. En lo posible, las pruebas deberán ser realizadas en forma automática, almacenando criterios y datos de pruebas en archivos, para permitir la verificación rápida y repetitiva.

Enfoque Datos e Información

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

Lineamientos sobre gestión y gobierno de la información

1. La Dirección TICs, con el apoyo de Gestión de Recursos deberá establecer una Arquitectura de Información Empresarial para Empresas Públicas de Armenia ESP la cual permita entre otras cosas definir:
    a. Modelo de Datos: Entidades y Vocabularios
    b. Inventario de activos de información.
    c. Normalización y caracterización de datos para integración entre Sistemas de Información.
    d. Ciclo de vida de los datos
    e. Análisis de la cadena de valor de información y entrega de datos

f. Diagrama lógico de datos, entre los otros necesarios en para el nivel de madurez de la entidad.

Lineamientos sobre el respaldo de la información

1. La Dirección TICs es responsable de establecer y garantizar el respaldo de la información de algo valor para la entidad.
2. La Dirección TICs es la única dependencia encargada de definir la periodicidad del respaldo de la información alojada en las carpetas compartidas, actualmente se realiza de forma diaria de acuerdo con los requerimientos de continuidad del negocio establecidos.
3. El respaldo diario de la información de las aplicaciones institucionales se realiza con la frecuencia que establezca el nivel de criticidad de los datos capturados según el proceso, este consiste en efectuar la copia de respaldo de la base de datos de producción y archivos adjuntos.
4. Cada usuario en su espacio de trabajo es responsable de garantizar y cumplir con los lineamientos de seguridad y privacidad de la información.
5. La Dirección TICs por medio del Modelo de Transferencia de TI deberá diseñar recursos pedagógicos que muestran los hábitos y buenas prácticas en temas de seguridad y privacidad de la información espacios ofimáticos, teletrabajo, trabajo en campo entre otros.
6. El respaldo deberá ser almacenado en la nube cumpliendo los parámetros de seguridad y privacidad que demanda la normatividad vigente.
7. La Dirección TICs es la responsable de convocar y seleccionar proveedores de TI que permitan la gestión del respaldo y seguridad de la información, en tal caso, la Dirección TICs realizará seguimiento y control al cumplimiento de los compromisos contractuales. El Proveedor seleccionado es el encargado de definir la estrategia, táctica y operatividad en copia de seguridad de la información.
8. La Dirección TICs deberá establecer los tiempos de retención de la información en medios electrónicos, esto aplicará para correos electrónicos y almacenamiento en la nube.
9. En términos de Correos Electrónicos deshabilitados o en inactividad, cada proceso con el apoyo de la dirección TICs deberá establecer la relevancia de respaldo de la información, sobre el resultado se establecerá la forma de proceder.

Enfoque Datos abiertos

Este enfoque tiene el propósito de establecer los lineamiento y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP apropiadas por todos los colaboradores, funcionario y contratistas, para habilitar y brindar acceso a la información de interés público, colocándola a disposición de los grupos de interés.

Lineamientos sobre la captura, almacenamiento y manipulación de los datos

1. Todo dato capturado deberá estar bajo cláusulas de permisividad de captura de los datos definidos en la Política e Privacidad y Uso de la Información.
2. Cada proceso es responsable de garantizar la privacidad y uso de la información capturada.
3. Empresas Públicas de Armenia ESP deberá garantizar sistemas de Información que permitan la calidad en la captura del dato.
4. Empresas Públicas de Armenia ESP, desde el proceso Dirección TIC, deberá garantizar la disponibilidad de los Sistemas de Información pertinentes y requeridos para cumplir con la captura, registro, seguridad y privacidad de los datos que captura.

Lineamientos sobre la calidad de los datos

1. Cada proceso deberá realizar la identificación de los activos de información bajo su responsabilidad.
2. Cada proceso deberá identificar y relacionar los datos generados por medio de los instrumentos y herramientas que sean necesarios.
3. 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.

Lineamientos sobre la divulgación, acceso y uso de los datos abiertos

1. La Dirección TIC será la encargada de generar, en los formatos correspondientes, el conjunto de datos abiertos para publicar.
2. Los datos abiertos generados por Empresas Públicas de Armenia ESP serán actualizados y/o publicados cada año, según corresponda cada caso y la agenda de publicación establecido en el plan de Datos Abiertos.
3. Los datos abiertos publicados serán los correspondientes al año de la vigencia anterior.
4. La divulgación oficial del conjunto de datos abiertos de Empresas Públicas de Armenia ESP, será divulgado por el portal www.datos.gov.co, plataforma oficial a nivel nacional.
5. Empresas Públicas de Armenia ESP publicará en su sitio web en la sección de transparencia la lista de datos abiertos actualizados para su fácil acceso y uso.
6. La Dirección TIC será la responsable de publicar los datos abiertos en la plataforma www.datos.gov.co
7. La Dirección de comunicaciones será la responsable de comunicar y

difundir por medio de los canales que vea pertinente la disponibilidad y actualización de los datos abiertos publicados en www.datos.gov.co.

8. La Dirección TIC deberá realizar seguimientos periódicos a los datos publicados para identificar el nivel de uso y acceso a estos.
9. La Dirección TICs de la mano con la Dirección de Planeación Corporativa deberá destinar recursos para promover e incentivar el uso de los datos abiertos con el propósito desarrollar proyectos e iniciativas para mejorar el desempeño e impacto de Empresas Públicas de Armenia ESP o fortalecer el bienestar del territorio de impacto la oferta de servicios públicos.

Lineamientos sobre incentivos para el desarrollo de proyectos e iniciativas que promueva el uso de los datos abiertos

Empresas Públicas de Armenia ESP debe establecer iniciativas y proyectos que promuevan el uso y apropiación de los datos abiertos, estas iniciativas podrán estar enmarcadas en:

1. Realizar maratones y eventos de innovación abierta, vinculando otras entidades públicas y/o privadas para fortalecer el territorio.
2. Promover programas de emprendimiento digital para el fortalecimiento una ciudad inteligente o la mejora de la gestión de Empresas Públicas de Armenia ESP en su gestión.
3. Fomentar la formulación de proyectos de TI que beneficien a los grupos de interés y consumidores.

Enfoque Uso, Apropiación y Capacidades institucionales

Este enfoque tiene el propósito de establecer los lineamiento y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP para gestionar el cambio y la transformación de la entidad acompañando la apropiación y habilitación de nuevas capacidades de TI en la entidad.

Lineamiento para el uso y apropiación de capacidades de TI.

1. La Dirección TICs debe establecer e implementas la estrategia de uso y apropiación de TI, de acuerdo con la caracterización de sus usuarios, ciudadanos y grupos de interés. Bajo estos parámetros se debe trabajar en:
    a. La identificación de los involucrados en la entidad.
    b. Todos los procesos y áreas deberán estar involucrados en estar involucrados.
    c. La alta dirección debe estar involucrada en todos los procesos para

gestión del cambio.

d. Se debe trabajar en alinear y establecer el diálogo que comunique una visión compartida entre los procesos.
e. El diseño de un plan de formación en competencias y capacidades de TI.

2. La Dirección TICs con el apoyo de Dirección de Comunicaciones debe desarrollar acciones de sensibilización y socialización de los proyectos o iniciativas de TI, a partir de la estrategia de uso y apropiación de TI. Bajo estos parámetros se debe trabajar en:
    a. Empoderamiento de las áreas y procesos para llevar a una efectiva toma de decisiones basadas en las competencias de TI que necesitan desarrollar para alcanzar esos ideales.
    b. Diseño de espacios virtuales y/o presenciales que permitan incorporar en la cultura organizacional buenas practicas de TI para el crecimiento y continuidad del negocio.
    c. Entender las dinámicas de cambio de la entidad y gestionar los impactos priorizando su nivel, de manera anticipada.
3. La Dirección TICs debe realizar el monitoreo, evaluación y mejora continua de la Estrategia de uso y apropiación de los proyectos de TI. Bajo estos parámetros se debe trabajar en:
    a. Desarrollar herramientas gerenciales y de aprendizaje que apalanquen el uso y la apropiación de las TI.
    b. Asegurar el uso y la apropiación de los sistemas de información y servicios tecnológicos desde la identificación de iniciativas estratégicas de TI para el negocio, hasta facilitar la dotación de tecnología y fomentar su acceso.
    c. Gestionar la transición que dé continuidad a la implementación de las estrategias hasta apropiar las TI como parte de las prácticas organizacionales.
    d. El diseño, aplicación y monitoreo de indicadores de impacto del uso y apropiación de las TI alineados a los de la cultura organizacional.

Lineamientos sobre la gestión de capacidades institucionales

1. La Dirección TICs debe definir e implementar buenas practicas para el uso eficiente del papel mediadas por TI.
2. La Dirección TICs debe desarrollar esquemas y herramientas de gestión de documentos electrónicos, con base en el análisis de los procesos de la entidad.
3. La Dirección TICs identifica y prioriza las acciones o proyectos a implementar para la automatización de procesos y procedimientos.

Enfoque Gestión de Proveedores de TI

Este enfoque permite establecer los lineamientos y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia ESP para la gestión efectiva y oportuna de la relación con Proveedores de TI y proveedores, para la gestión de incidentes de gobierno y gestión de TI.

Lineamientos sobre gestión de la relación con Contratista Proveedores y/o terceros

1. Empresas Públicas de Armenia ESP debe establecer para los contratistas, terceros y proveedores las mismas restricciones de acceso a la información que a un usuario interno.
2. El acceso a la información debe limitarse a lo mínimo indispensable para cumplir con la actividad asignada o contratada.
    a. Toda excepción de acceso a privilegios fuera del rango ya sea física como lógica a los activos de información, deberá ser analizada y aprobada siguiendo el conducto resultar establecido para la toma de decisiones y que figure como el Responsable de la Información y el Oficial de Seguridad de la Información de la entidad.
3. Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir con todas las políticas de su competencia.
4. El personal externo debe firmar un acuerdo de confidencialidad o un acuerdo de no-divulgación antes de obtener acceso a información de la entidad.
5. A los proveedores, solo se les dará acceso a los sistemas de información de la Empresas Públicas de Armenia ESP, únicamente bajo un requerimiento formal y previa aprobación del dueño o responsable del activo de información y solo cuando sea necesario.
6. En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violación de los contratos.
7. Todos los contratos deben incluir una cláusula donde se establezca el derecho de la Empresas Públicas de Armenia ESP de nombrar a un representante autorizado para evaluar la estructura de control interna del proveedor.
8. Los contratistas, proveedores y terceros deben comunicar los incidentes de seguridad de la información que detecten, al respectivo supervisor del contrato, para hacer el trámite o seguir el conducto regular. Los procedimientos de gestión de incidentes estarán basados en lo establecido en la norma ISO 27035.

Referente a Servicios Tercerizados o en Outsourcing

Los contratos o acuerdos de tercerización total o parcial de servicios, para la administración y/o control de sistemas de información, redes y/o plataformas tecnológicas de la Empresas Públicas de Armenia ESP, deben contemplar los siguientes aspectos:

1. Deben describir la forma en que se cumplirán los requisitos legales aplicables.
2. La Empresas Públicas de Armenia ESP como entidad contratante, es la que determina los lineamientos, políticas, manuales, estándares y demás parámetros de Seguridad de la Información que se deben aplicar, así como es quien aprueba cualquier ajuste o cambio de las mismas.
3. La Empresas Públicas de Armenia ESP ESO tiene el derecho de auditar cualquier aspecto de los servicios o actividades tercerizadas en forma directa o a través de la contratación de servicios ad hoc.
4. Deben establecer los medios de comunicación y socialización, para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad de la información.
5. Deben definir la forma o metodología con la que se mantendrá y comprobará la integridad y confidencialidad de los activos de la entidad.
6. Deben definir los controles físicos y lógicos que se utilizarán para restringir
7. y delimitar el acceso a la información sensible de la entidad.
8. Deben definir la forma o metodología que usaran para garantizar la disponibilidad de los servicios ante la ocurrencia de desastres.
9. Deben definir los niveles de seguridad física y del entorno que se asignarán al equipamiento tercerizado.
10. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.
11. Se deben establecer dentro de los acuerdos de confidencialidad o de no divulgación, el cumplimiento de las políticas de seguridad y de los respectivos controles de seguridad implementados en la entidad.
12. Se deben definir y determinar de niveles de disponibilidad aceptable.
13. Se deben garantizar ambientes aislados, si se ha contratado un servicio de procesamiento de la información de la entidad.
14. El proveedor debe y es responsable de informar de manera inmediata al supervisor del contrato de cualquier brecha o incidente de seguridad, que pueda comprometer los activos de información de La Empresas Públicas de Armenia ESP.
15. Cualquier contratista, proveedor o tercero de la entidad debe informar de violaciones a la seguridad de la información por parte de proveedores, al respectivo supervisor del contrato, para hacer el trámite o seguir el conducto regular.

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 para el Gobierno y Gestión de TI para el crecimiento y fortalecimiento de Empresas Públicas de Armenia ESP.

Lineamiento sobre la Gestión de Cambios

Estos lineamientos definen las condiciones que se deben considerar para la gestión del cambio en infraestructura, aplicaciones y sistemas de información y la continuad del negocio. en Empresas Públicas de Armenia ESP.

1. Los cambios en la infraestructura tecnológica y servicios de información en Empresas Públicas de Armenia ESP se deben realizar de acuerdo con el procedimiento establecido por La Dirección TICs.
2. Empresas Públicas de Armenia ESP debe establecer procedimientos para el control de cambios ejecutados en la entidad. Toda solicitud de cambio en los servicios de infraestructura y sistemas de información de Empresas Públicas de Armenia ESP, se debe realizar siguiendo el Procedimiento de gestión de cambios de TI.
3. La Dirección de TICs debe llevar una trazabilidad del control de cambios solicitados.
4. Se debe especificar los canales autorizados para la recepción de solicitudes de cambios, como la Mesa de Ayuda, correo electrónico o un oficio dirigido al Líder de Tecnología de la Información.
5. Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.
6. Se deben especificar en qué momento existen cambios de emergencia en la cual se debe garantizar que los cambios se apliquen de forma rápida y controlada.
7. Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los Colaboradores o Terceros que por sus funciones tienen relación con el sistema de información.
8. Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.
9. Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de

información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

10. Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

Lineamientos sobre la continuidad del negocio

Estos lineamientos establecen las condiciones para garantizar que los planes de continuidad de negocios se ejecuten de forma segura sin exponer la información de Empresas Públicas de Armenia ESP.

1. Empresas Públicas de Armenia ESP desde la Dirección TICs debe establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis.
2. Para Empresas Públicas de Armenia ESP su recurso más importante es el Recurso Humano y por lo tanto será su prioridad y objetivo principal protegerlo adecuadamente en cualquier evento.
3. Empresas Públicas de Armenia ESP deberá contar con un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos de la Entidad, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.
4. Empresas Públicas de Armenia ESP debe disponer de plan de continuidad que asegura la continuidad de las operaciones tecnológicas de sus procesos críticos, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.
5. Empresas Públicas de Armenia ESP deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:
    a. Identificación y asignación de prioridades a los procesos críticos de TI de Empresas Públicas de Armenia ESP de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
    b. Documentación de la estrategia de continuidad del negocio.
    c. Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
    d. Plan de pruebas de la estrategia de continuidad del negocio.
6. Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones y responsabilidades relacionados con el plan, deben estar incorporados y definidos en el Plan de continuidad.
7. La Dirección TICs se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

7. Instrumentos para la gestión de Gobierno y gestión de TI

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

- Política de Seguridad y Privacidad de la Información.
- Política de Servicios Ciudadanos Digitales
- Procedimiento de Gestión Estratégica y Gobierno de TI
- Procedimiento de Gestión de Infraestructura TI.
- Procedimiento de Gestión de la Información y Sistemas de Información de TI
- Procedimiento de Gestión de Fortalecimiento de Capacidades de TI.
- Procedimiento de Gestión de Proveedores de TI.

8. 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 informar los parámetros de comportamiento 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 y Gestión de TI de Empresas Públicas de Armenia ESP.
- Ambas asignaciones contarán con la participación activa y acompañamiento de la Dirección TICs para lograr asertividad y pertenencia en la información divulgada.

9. Revisión y seguimiento al Sistema de Gobierno y gestión de TI

La Gerencia General y el Comité de MiPG, deberá revisar periódicamente el desempeño y utilidad del Modelo de Madurez Digital establecido para 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 Modelo de Madurez Digital,
- Revisión a la presente Política de Gobierno y Gestión de TI.
- Revisión al seguimiento realizado por el área de Gestión Control.
- Revisión de las normas, procedimientos, estándares, controles, formatos y procedimientos.
- Acople del Modelo de Madurez Digital con el Sistema de Gestión Integrado de Empresas Públicas de Armenia ESP.
- Revisión del listado maestro de documentos.

10. Cumplimiento

Empresas Públicas de Armenia ESP en manos de la Dirección TICs, responsable del Modelo de Madurez Digital, velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la gobernanza y gestión de las tecnologías de la información. Para cada procedimiento los responsables de las áreas evaluarán la necesidad de adelantar procesos disciplinarios o legales.

Esta Política de Gobierno y Gestión de TI 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.

11. Declaración de publicación

La publicación de la *Política de Gobierno y Gestión de TI 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.