INTRODUCCIÓN

Con la constante evolución de la tecnología, el sector público se ha visto en la necesidad de evolucionar hacia la cuarta revolución industrial, con el fin de generar valor en los procesos que se realizan dentro de las mismas entidades, en ese sentido, las TIC toman una gran relevancia dentro de la gestión de las entidades públicas, ya que se convierten en aliados fundamentales en el proceso de la transformación digital, tanto del estado como del país en general.

En este nuevo contexto, la política de Gobierno Digital se constituye en el motor de la transformación digital del Estado, permitiendo que las entidades públicas sean más eficientes para atender las necesidades y problemáticas de los ciudadanos y que éstos sean los protagonistas en los procesos de cambio a través del uso y apropiación de las tecnologías digitales.

Es por eso que el gobierno nacional a través del ministerio de tecnologías de la información MinTiC, ha venido promoviendo la política de gobierno digital, bajo el decreto 1008 de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”, esta política tiene como objetivo fundamental: “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”

En el contexto de la política de gobierno digital, se define adicionalmente como elemento transversal el ítem de “seguridad de la información”, el cual se implementa en las entidades públicas bajo la norma ISO 27001:2013 y tiene como línea base dar cumplimiento al modelo de seguridad y privacidad de la información MSPI, es decir, a través del modelo MSPI se implementa el sistema SGSI de las entidades territoriales.

El Modelo de Seguridad y Privacidad de la Información (MSPI), se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital reglamenta bajo el decreto 1008 de 2018.

MSPI para estar acorde con las buenas prácticas de seguridad debe de encontrarse en constante actualización; con el fin de reunir los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la

Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

En ese sentido, a través del modelo de seguridad y privacidad de la información “MSPI” se plantean las políticas de seguridad de la información de la alcaldía de Armenia, con el fin de proporcionar herramientas para la definición de los estándares y procesos internos de la entidad. En base a lo anterior, la Secretaría TIC debe ser impulsor de esta política, con el fin de asegurar que la información que se produce en la entidad se encuentre siempre disponible cumpla con los criterios de Confidencialidad, Integridad, Disponibilidad, Accesibilidad, Autenticidad, No Repudio, entre otros, mediante el resguardo de datos, la protección frente a accesos no autorizados, el control de acceso a otros sitios web, la adecuada utilización del correo electrónico de la Entidad, entre otros.

Así mismo, proporcionar hardware, software y equipos de comunicaciones en condiciones de seguridad y calidad; realizar revisiones periódicas de seguridad; y garantizar la propiedad de la Información y la buena manipulación de programas de software aplicativo.

Este documento describe las políticas, normas y lineamientos técnicos de seguridad de la información definidas por la alcaldía de Armenia para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables.

Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la Alcaldía de Armenia y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

ALCANCE

La presente política de seguridad informática de la Alcaldía de Armenia, aplican para los usuarios, contratistas, funcionarios de planta, personal de apoyo y terceros no vinculados directamente a la Alcaldía de Armenia, que utilicen los activos de información con los que cuenta la entidad.

Las excepciones al cumplimiento de las políticas de seguridad informática serán autorizadas única y exclusivamente por la Secretaría TIC (secretario TIC o profesional especializado de infraestructura tecnológica), cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos institucionales, y deberán ser documentadas formalmente.

Las políticas de seguridad informática serán objeto de evaluación semestral, aplicando mecanismos de autocontrol y autoevaluación a través de indicadores de gestión propuestos por el modelo de seguridad y privacidad de la información (MSPI), para garantizar el mejoramiento continuo.

Por último, debemos decir que la aplicación de las políticas propuestas en este documento obedece al interés por parte de la Alcaldía de Armenia, en diseñar, implementar y sostener el modelo de seguridad y privacidad de la información de acuerdo a las políticas, decretos, resoluciones y/o actos administrativos expedidos por las entidades de orden nacional.

GLOSARIO

- **Seguridad de la información (SGSI):** preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad (Editada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), 2006).

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad:** Condición que garantiza que la información consignada en un documento ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación (Ministerio de Tecnologías de la información y comunicaciones, 2017).

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la Alcaldía de Armenia**.**

- **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información:** Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocios, es también el conjunto total de procedimientos, operaciones, funciones y difusión de datos o información en una organización (Universidad del Cauca, 2017).

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

- **Administrador de Bases de Datos (DBA):** Persona responsable de los aspectos ambientales de una base de datos.

- **Amenaza:** Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Antivirus:** Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

- **Ataque:** Evento, exitoso o no, que atenta sobre el buen funcionamiento de los sistemas de información.

- **Backups:** Es una copia de seguridad de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida o robo.

- **Hardware:** Se refiere a las características técnicas y físicas de las computadoras.

- **IP:** Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP.

- **Plan de Contingencia:** Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

- **Redes:** Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

- **Servidores:** Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

- **Software:** Programas y documentación de respaldo que permite y facilita el uso del pc. El software controla la operación del hardware.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

MARCO NORMATIVO

Las políticas de seguridad de la Información de la alcaldía de Armenia se ciñen a la normatividad legal vigente colombiana, tal como se describe a continuación**:**

Legislación	Tema	Referencia
Ley 527 de 1999	"Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos"	El mensaje de datos es "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax".
Ley 1226 del 2008	"Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"	Se regula el manejo de la información para "todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada".
Ley 1273 del 2009	"Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones".	"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
		Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual

Ley 1581 de 2012	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	“todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que “Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”. El objeto de la ley es “regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información”.
Decreto 2573 del 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 113 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	El decreto tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.
Decreto 1008 de 2018	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la	Permite lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la Alcaldía de Armenia desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que

	parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"	traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos que puedan beneficiar a la entidad.
Resolución número 00500 de marzo 10 de 2021	"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"	La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.
Directiva presidencial No. 03 del 15 de marzo de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.	Con el fin de dar cumplimiento al artículo 147 de la Ley 1955 de 2019, "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", disminuir los costos de funcionamiento, acelerar la innovación, brindar entornos confiables digitales para las entidades públicas y mejorar sus procedimientos y servicios, se imparten las siguientes directrices

POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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

Para la Alcaldía de Armenia, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de

mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

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

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Alcaldía de Armenia.
- Garantizar la continuidad del negocio frente a incidentes.
- La alcaldía de Armenia a través de la secretaría TCI ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la Alcaldía de Armenia:

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los **empleados, proveedores, socios de negocio o terceros**.
- La alcaldía de Armenia protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- La Alcaldía de Armenia **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La Alcaldía de Armenia **protegerá su información** de las amenazas originadas por parte del **personal.**
- La Alcaldía de Armenia **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos.**
- La Alcaldía de Armenia **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Alcaldía de Armenia **implementará control de acceso** a la información, sistemas y recursos de red.
- La Alcaldía de Armenia garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Alcaldía de Armenia garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Alcaldía de Armenia **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Alcaldía de Armenia garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

Política y Controles de Organización Interna

Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información.

La Alcaldía de Armenia y su nivel directivo apoya la necesidad de contar con políticas de seguridad y privacidad de la información, la cual sirven como soporte y apoyo a los procesos institucionales. Por tal motivo se debe de tener en cuenta las siguientes recomendaciones:

- Creación de un comité de seguridad interdisciplinario conformado por representantes de la alta dirección de la entidad, quienes serán los encargados de tratar los temas concernientes a la seguridad de la información, formulando su propio reglamento, en el cual establecerán responsabilidades, funciones y periodicidad de las reuniones. Actuarán como invitados permanentes los administradores de los diferentes sistemas de información.

- Asignación de un responsable de la seguridad de la información (Oficial de seguridad) que vele por el cumplimiento de las políticas establecidas en este documento. En

concordancia con el articulo 3 y articulo 6 de la resolución 500 de 2021 del MinTIC, ““Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”, en la que las entidades públicas deben determinar y/o establecer acciones de talento humano para garantizar que la seguridad digital en las entidades.

- Aprobación bajo acto administrativo el documento de políticas de seguridad de la información.

- Realización de reuniones periódicas donde se verifique el cumplimiento de las políticas, donde verifiquen indicadores de gestión del modelo y control de riesgos con el fin de establecer mejoras en las políticas.

Con el fin de profundizar más a fondo en la organización de la información, la Alcaldía deberá establecer adjunto a las políticas de seguridad de la información, un documento de Roles y responsabilidades de seguridad de la información, con el fin de establecer compromisos en base a las mismas, por parte de los funcionarios de la entidad.

GESTION DE ACTIVOS

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información con los que cuenta la Alcaldía de Armenia.

Política para los servicios de procesamiento de la información

La Secretaría TIC, será la encargada de velar y custodiar los activos tecnológicos tangibles e intangibles con los que cuenta la entidad, así como la definición de los estándares para el desarrollo, adquisición y mantenimiento de la infraestructura tecnológica, todo lo anterior siguiendo las mejores prácticas internas y normatividad vigente.

Desarrollo de aplicativos

La Alcaldía de Armenia apoya el desarrollo propio o externo de aplicativos, más aún cuando el software que se requiere no se encuentra en el mercado o los costos de licenciamiento sobrepasan el presupuesto de la entidad, por tal motivo el desarrollo de aplicativos deberá ser autorizado por el comité operativo integrado por el secretario TIC, los líderes del proceso 18 y 17 así como también por las dependencias involucradas con la finalidad del mismo. Dicho software debe seguir las fases del ciclo de vida de los sistemas de información propuesta en

el dominio de arquitectura TI de la entidad y deberá ser testeado por los funcionarios de la Secretaría TIC y los funcionarios de las dependencias que utilizarán el mismo.

Control de cambios

Si una dependencia de la entidad requiere alguna modificación estructural o no, sobre el software y/o aplicativo, es necesario que la solicitud de modificación esté autorizada mediante escrito por los secretarios de despacho de las dependencias que utilizan el mismo, así como también de las personas responsables de la ejecución del proceso. Posteriormente el secretario TIC con el apoyo del comité operativo de su dependencia deberá realizar el análisis tanto técnico como económico con el fin de evaluar la operatividad y aplicabilidad del mismo, de conformidad con el procedimiento establecido.

Control de Versiones

El líder del proceso 18 será el responsable de gestionar el control de las distintas versiones de desarrollo de un software, de tal forma que se garantice la confidencialidad, disponibilidad e integridad de la información.

Publicación de Aplicativos

Para la publicación y puesta en marcha de aplicativos nuevos estos deben estar correctamente diseñados, evaluados de forma minuciosa para evitar la redundancia en las salidas de información, supervisados y autorizados por el comité operativo de la secretaría TIC y el responsable o líder del proceso de las dependencias donde utilicen el aplicativo.

Política de dispositivos móviles

La Alcaldía de Armenia no permite conectar a las redes wifi de la entidad a funcionarios y contratistas sus dispositivos móviles.

Controles

- Aunque no se permite el acceso a la red wi-fi de la alcaldía de Armenia a los funcionarios, desde sus dispositivos móviles, los diferentes funcionarios de las dependencias de la entidad podrán solicitar de manera escrita (firmada por el secretario de despacho) la solicitud a la secretaría TIC con el fin de suministrar la contraseña

- Las contraseñas de las redes Wi-fi se deben cambiar cada 3 meses, ya que la entidad está cambiando de personal (contratistas) constantemente.

- La Secretaría TIC es la encargada de administrar la red Wi-fi, esta contará con todas las contraseñas Wi-fi de la entidad y podrá aplicar las restricciones de red que considere necesarias para salvaguardar los datos que genera la entidad.

- La secretaría TIC tendrá potestad de limitar la velocidad de conexión de los dispositivos conectados a las redes WI-FI, de acuerdo a la disponibilidad de red contratada, equipos conectados y capacidad técnica de los dispositivos de red.

- La secretaría TIC en cualquier momento podrá establecer restricciones de accesos a páginas webs no permitidas, que tengan contenido no permitido, o pongan en riesgo la navegación de los demás dispositivos conectados.

Política de teletrabajo

La Alcaldía de Armenia acorde a los retos de las nuevas tecnologías 4.0, deberá tomar medidas de seguridad para proteger los activos de información utilizados en materia de teletrabajo por parte tanto de los contratistas como de los equipos de la entidad.

Controles

- Los equipos utilizados para conectarse remotamente deberán contar con el cifrado de disco completo garantiza que, incluso si el dispositivo cae en las manos equivocadas, no se puede acceder a los datos de la alcaldía.

- Las contraseñas utilizadas para el cifrado de la información las asignará la secretaría TIC, previa autorización por parte del secretario de despacho de la dependencia que requiera e servicio.

- Se debe utilizar siempre una VPN para conectar trabajadores remotos a la red interna de la organización. Esto evita ataques de Man-in-the-Middle desde ubicaciones remotas

Política de medios de Almacenamiento externo

Tanto funcionarios públicos, como contratistas que hagan uso de algún activo de información de la entidad que contengan información confidencial de propiedad de la entidad en medios de almacenamiento externo, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

El medio de almacenamiento externo que conecte un funcionario en su equipo asignado es responsabilidad propia, por tal motivo la información que se encuentre allí y que por algún motivo sea modificada o borrada por accidente, no involucra ni compromete a la Secretaría TIC en ningún caso.

Controles

- Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido.

- Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta.

- No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Entidad, en lugares de acceso público como cibercafés, puntos vive digital o en equipos que no garanticen la confiabilidad, la integridad y la disponibilidad de la información.

- La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

- Tanto los equipos de cómputo de la entidad como los servidores del centro de datos deberán tener deshabilitadas la reproducción automática de dispositivos externos de almacenamiento removibles.

Políticas de creación y restauración de copias de seguridad

La Alcaldía de Armenia a través de la Secretaría TIC ha identificado los procesos operativos y misionales con infraestructura crítica que se manejan a través de los diferentes aplicativos de la entidad, los cuales son respaldados con copias de seguridad diarias, la frecuencia de estas copias fue debe ser definida por la Secretaría TIC.

Controles

- Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.

- Las copias de seguridad de los aplicativos Impuestos Plus, Finanzas Plus y SRF (sistema de recursos físicos) y pagina, se deberán de realizar diariamente y registrasen en las bitácoras correspondientes para cada uno de los aplicativos.

- La Secretaría TIC deberá definir y aplicar el modelo de conservación, restauración y eliminación de los archivos electrónicos, teniendo en cuenta siempre el programa de gestión documental de la entidad.

- Los servidores públicos deberán realizar copias de seguridad de sus archivos alojados en sus equipos de cómputo, si existiera dudas sobre el proceso, desde la secretaría TIC se brinda asesoría en el proceso.

- Los Administradores de las bases de datos realizaran pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente.

- La Secretaría TIC conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas.

Políticas para el manejo de carpetas compartidas

El usuario o funcionario de la administración municipal que autorice desde su equipo de cómputo el uso compartido de carpetas y/o dispositivos es responsable por las acciones y el acceso a la carpeta de la información compartida que se maneje allí.

Controles

- El usuario o funcionario de la Alcaldía de Armenia que autoriza la carpeta compartida debe de seleccionar los usuarios que realmente necesitan acceder a la información y verificar el acceso, controlando el tiempo en el cual estará expuesta la información

- El usuario o funcionario de la Alcaldía de Armenia que autoriza la carpeta compartida debe asegurarse que el usuario autorizado cuente con el antivirus autorizado por la secretaría TIC.

- La secretaría TIC a través de sus funcionarios brindará asesoría a la hora compartir correctamente las carpetas entre funcionarios, con el fin de restringir usuarios y permisos entre ellas.

Política de Antivirus

Todos los equipos de la entidad deben tener instalado, configurado, funcionando, actualizado y debidamente licenciado un antivirus, el cual será suministrado por la Secretaría TIC Municipal.

Controles

- El antivirus se deberá actualizar de forma automática con el fin de tener las bases de datos de las últimas actualizaciones de virus.

- Está prohibido que los usuarios desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus, ya que esta acción puede ocasionar riesgo total de contaminación de virus.

- Los funcionarios y contratistas de la administración municipal deben asegurarse de que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

- Los funcionarios y contratistas que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Secretaría TIC a través de la mesa de ayuda, con el fin de brindar el soporte técnico de correspondiente

- EI equipo de trabajo de la secretaria TIC es responsable por la actualización oportuna del software antivirus.

Dominio Armenia.com

Todos los equipos de propiedad de la Alcaldía de Armenia y que se encuentren en el centro administrativo municipal deben estar dentro del dominio, el cual será administrado desde la Secretaría TIC de la entidad.

Controles

- El personal de la Secretaría TIC de la Alcaldía Municipal, deberá asegurarse que los equipos de los funcionarios y que se encuentren en el centro administrativo municipal estén conectados al dominio Armenia.com.

- La secretaría TIC municipal deberá designar un administrador de dominio, el cual aplicará las configuraciones necesarias para mantener la seguridad en todos los equipos de la administración municipal.

- Está prohibido que algún equipo de pertenencia de la Alcaldía de Armenia este por fuera del dominio Armenia.com

- Las políticas de generación de contraseñas para cada usuario y el administrador del dominio, por motivos de seguridad solo las conocerán los funcionarios de la Secretaría TIC.

- Las contraseñas de los equipos de los funcionarios serán suministradas por el administrador del dominio el cual es designado por la Secretaría TIC.

- Se realizarán controles a usuarios del dominio, con el fin de verificar si existen usuarios con permisos no autorizados y/o usuarios repetidos.

- Los equipos de cómputo comprados por la entidad deberán tener soporte a redes, con el fin de conectarlos al dominio Armenia.com.

Control de acceso a la información y los sistemas

El acceso a los recursos de información que provee la Alcaldía de Armenia, tales como internet, sistemas de información y redes avanzadas es suministrado a los usuarios de la Alcaldía de Armenia como herramientas de soporte para obtener la información necesaria para realizar de manera óptima sus actividades mediante el uso de herramientas tecnológicas, para lo cual debe cumplirse con los siguientes aspectos:

Controles

- Todo tipo de información que provenga, sea transmitida o recibida por un sistema computacional de comunicación es considerada parte de los registros oficiales de la Alcaldía de Armenia y, por ende, está sujeta a cumplir las normas y restricciones consignadas en este documento. Como consecuencia de esto, el usuario, deberá siempre asegurarse que la información contenida en los mensajes de e-mail y en otras transmisiones es precisa, apropiada, ética y constructiva.

- Los equipos, servicios, y tecnologías proporcionadas a los usuarios para hacer uso del Internet son en todo momento propiedad de la Alcaldía de Armenia. Por este motivo, la Alcaldía de Armenia se reserva el derecho a monitorear el tráfico de Internet, y retirar,

leer o verificar cualquier documento enviado o recibido a través de conexiones en línea y que sea guardado en los computadores de la Alcaldía de Armenia.

- El acceso a las bases de datos de los sistemas se realizará de conformidad con las políticas de acceso.

- Las pistas de auditoría deben permitir monitorear las conexiones a las bases de datos, las modificaciones al modelo de datos y las modificaciones a los datos, de manera directa o por medio de aplicativos.

- Las empresas externas contratadas por la Alcaldía de Armenia, para administrar y dar soporte a las bases de datos, deberán tener permiso autorizado por el director de sistemas para realizar cualquier modificación y/o actualización en las bases de datos de los aplicativos.

- La secretaría TIC se hace responsable del buen funcionamiento de los sistemas de información y de la seguridad en ellos, mas no se hace responsable del uso que les den a estos sistemas los funcionarios y contratistas que los utilizan, en ese sentido, la responsabilidad sobre el manejo de los aplicativos con los que cuenta la entidad es tácitamente del funcionario de planta y/o supervisor del contratista.

- La Secretaria de Hacienda y La Tesorería Municipal, deberá mantener informada a la Secretaria de las Tecnologías de la Información y Las Comunicaciones de la rotación de los funcionarios/contratistas de las áreas financieras y en el caso de las demás dependencias el responsable de dichas notificaciones será el jefe de cada una o en su defecto el funcionario de nombramiento de cada dependencia, con el fin de mantener actualizada la base de datos como la eliminación de cuentas de correos, claves de acceso entre otros de personas que ya no tengan vínculos con la institución y evitar accesos no autorizados.

- La secretaría TIC a través del plan de sensibilización y comunicación de seguridad deberá capacitar a los funcionarios de la entidad en el buen manejo de los sistemas de información y el uso responsable de los mismos.

Estrategia de preservación de archivos

La Secretaría TIC implementará las acciones para la protección y preservación de los archivos en el tiempo, teniendo en cuenta el entorno técnico para el buen funcionamiento del software y hardware. La entidad considera fundamental dicho proceso para la recuperación en el tiempo de la información almacenada en los diferentes aplicativos,

bases de datos, correo electrónico, páginas web y carpetas virtuales compartidas y servidores que poseen cada una de las dependencias de la Entidad.

Controles

- La Secretaría TIC implementará técnicas de preservación digital de los documentos de gestión documental teniendo en cuenta el programa de gestión documental de la entidad y la vida útil del hardware y software de la entidad.

- La Secretaría TIC, con la ayuda de los funcionarios que proveen los servicios del aplicativo de gestión documental deberán migrar los formatos antiguos de archivos (.doc, .xls, pdf) a formatos más modernos (.docx, .xlsx, pdf/A), con el fin de garantizar que la información se mantenga plena e inalterable en el tiempo.

- La dirección administrativa de Fortalecimiento Institucional DAFI deberá establecer los tiempos de permanencia de los archivos electrónicos y bases de datos de acuerdo a sus tablas de retención documental.

- El proceso de migración de documentos debe garantizar:

    - Independencia del dispositivo.
    - Debe ser representado de manera fiable en cualquier plataforma software o hardware.
    - Auto contenido: Debe contener todos los recursos necesarios para su representación.
    - Autodocumentado: Debe contener su propia descripción
    - Sin restricciones: No debe haber mecanismos de protección del fichero.
    - Disponible: Especificación accesible cuando se requiera.
    - Adoptado: Un uso amplio contra los riesgos de la preservación

- Cada vez que la Entidad obtenga nuevas versiones de software que involucren operaciones transversales, es importante por medio de la Secretaría TIC implementar un plan de migración en serie para facilitar la conversión en tiempo real.

- Cuando se adquieran nuevos equipos de almacenamiento y no acepten soportes de archivos antiguos, se debe realizan un procedimiento de verificación mediante MD5 dígitos de control, para asegurar la autenticidad e integridad de los soportes posterior al proceso de refreshing.

- La Entidad por intermedio de la Secretaría TIC y la dirección administrativa de Fortalecimiento Institucional DAFI deberán garantizar la disponibilidad e integridad de

los metadatos de los documentos y expedientes electrónicos, manteniendo de manera permanente las relaciones entre cada documento o expediente y sus metadatos.

- La Secretaría TIC a través del plan de tratamiento de riesgos deberá realizar un seguimiento a los riesgos identificados que afecten la disponibilidad, integridad y confidencialidad de los archivos.

Políticas de uso del correo electrónico

La Secretaría TIC es la encargada de definir los nombres, estructura y plataforma que se debe utilizar para la cuenta de correo Institucional de cada dependencia de la administración municipal

Controles

Administración del Correo Institucional

- El uso del correo institucional es de carácter corporativo, siendo responsabilidad de los secretarios y directores su administración y control.

- Los secretarios, subsecretarios y directores podrán delegar por escrito al funcionario que se encargará de la administración del correo.

- El tamaño del buzón, de los archivos enviados y del contenido del correo será definido por la Secretaría TIC.

Cambio de Contraseñas a Correos Institucionales

- En el mismo instante en que la Secretaría TIC cree y dé a conocer de la cuenta de correo Institucional designada para cada dependencia la persona a la que será entregada el correo será responsable si decide cambiar la contraseña.

- La confidencialidad y el uso del usuario y contraseña será responsabilidad de la persona a quien se le asigne.

Recepción e Intercambio de información

- El intercambio de información entre la entidad y terceros a través de correos electrónicos se hará única y exclusivamente por medio de los correos institucionales, y en ningún caso por medio de correos personales.

- El usuario responsable del correo institucional deberá evitar abrir los adjuntos de correos de origen desconocido a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.

- El correo institucional será de uso exclusivo para fines propios de la Entidad y en su uso se dará aplicación al código de ética; En consecuencia, es prohibido utilizar el correo institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

- La Alcaldía de Armenia a través de la secretaria de las Tecnologías de la Información y Las Comunicaciones se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad.

Exoneración de responsabilidades

- La Secretaría TIC definirá el texto de exoneración de responsabilidad que se debe incluir en los correos electrónicos, para proteger a la entidad de los contenidos de los correos electrónicos.

Políticas de acceso a internet e intranet

En el centro administrativo municipal el acceso a Internet e Intranet es permitido a todos los servidores públicos y contratistas para facilitar el desarrollo de los procesos y funciones propias de la Entidad, no obstante, los equipos de contratistas o personas ajenas a la entidad, deberán conectarse a una red distinta de la red local de la entidad, esta será suministrada por la Secretaría TIC.

Controles

Asignación IP: La Secretaría TIC deberá tener en un archivo el registro de asignación y control del direccionamiento IP de cada uno de los equipos conectados que forman parte de la red con acceso a internet de la Alcaldía municipal, el cual deberá contener la siguiente información:

1. Nombre del funcionario
2. Placa del equipo
3. Dependencia
4. Dirección IP

Finalidad del uso de internet: los canales de acceso a internet de la entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos de cada funcionario. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.
No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Alcaldía Municipal o de las personas.
La entidad se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

Uso de la Intranet

- Las cuentas de acceso a Intranet serán administradas por la Secretaría TIC y serán creadas para el personal de planta de la entidad y/o personal autorizado por el jefe de cada dependencia.

- Todos los contenidos que se publican en la intranet de cada una de las dependencias de la Alcaldía de Armenia, son responsabilidad del área que los emite.

- Toda la información que se publique en la intranet municipal, deberá cumplir con la ley 1581 de 2021 “Ley de tratamiento de datos personales”, además de cumplir con todas las leyes de derechos de copia y propiedad intelectual, no ir contra política o reglamento de la Alcaldía de Armenia y no ser usada para actividades comerciales o de lucro excepto cuando se trate de cumplir con fines institucionales.

- Para el uso de Intranet se deben observar las mismas normas de comportamiento definidas para el uso de internet

Políticas de publicación en el portal web

La Alcaldía de Armenia entiende el sitio web como un medio de comunicación con la comunidad, de manera que se brinde transparencia en los procesos que allí se adelantan. Ahora bien, la alcaldía de Armenia debe atender las políticas de transparencia y acceso a la información, entendidas en la ley 1712 de 2014 y resolución 0519 de del 2020, ya que desde allí se

establecen los lineamientos que en materia de publicación web los sujetos obligados deben de cumplir.

Controles

- La Secretaria de las Tecnologías de la Información y Las Comunicaciones como proceso de Gestión, tiene la responsabilidad de la operación de los servidores que albergan las páginas web, para lo cual; administra el servidor, se ocupa de la parte de programación y desarrollo utilizando tecnología estable en todo lo relacionado con Web y establece los estándares y lineamientos de diseño, publicación, comunicación y procedimientos de revisión para todas las páginas web institucionales, por lo tanto es la dependencia encargada de desarrollar, diseñar y mantener el portal de la Alcaldía de Armenia.

- La administración de los contenidos de las páginas institucionales estará a cargo de cada funcionario de cada dependencia, previamente designado por el secretario de despacho, quien será el encargado(a) de verificar los contenidos que pueden o deben ser publicados.

- Todos los contenidos que aparecen en los diferentes sitios, portales o páginas electrónicas de cada una de las instancias de la Alcaldía de Armenia con presencia en la página Web, son responsabilidad de la dependencia que los publica.

- El nombre de dominio "www.armenia.gov.co" y todos aquellos que sirvan para acceder de forma directa al sitio oficial de la Alcaldía de Armenia son de titularidad exclusiva de la Alcaldía de Armenia. La indebida utilización de los mismos supondría una infracción de los derechos conferidos por su registro y será perseguido por los medios previstos en la Ley.

- Ningún contenido del portal WEB se puede copiar con fines comerciales, ni se puede copiar y utilizar en otros sitios WEB.

- Para la publicación imágenes, videos y audios en las páginas sociales a las que pertenece la Alcaldía de Armenia oficialmente, es indispensable contar con la autorización pertinente, cumpliendo así con la ley de tratamiento de datos personales.

Políticas de adquisición y mantenimiento de software y hardware

Toda adquisición de recurso tecnológico de la alcaldía de Armenia deberá contar con la revisión y aprobación previa de los requerimientos técnicos mínimos definidos, por parte de la Secretaría TIC, el proceso deberá ser supervisado por el líder del proceso 18 (infraestructura tecnológica).

Política de software

La Secretaría TIC deberá proteger la propiedad intelectual propia y de terceros. El software registrado con derechos de autor, el cual no se podrá copiar sin previa autorización del propietario.

Controles

- Todo proceso de cambio de Software deberá contar con un plan de contingencia, de tal forma que se garantice la continuidad de los procesos, la salvaguarda e integridad de la información.
- La secretaría TIC a través del directorio Activo de la entidad deberá restringir la instalación de software en los equipos de cómputo de la administración municipal, lo anterior con el fin de evitar faltas a la propiedad intelectual de los propietarios de los mismos.

- Aunque la secretaría TIC supervisa y controla la instalación de software en los equipos de la entidad, es de aclarar que indebida instalación de algún software en equipos de propiedad de la administración municipal sin la debida autorización de la secretaría TIC, son faltas graves a las políticas de seguridad y por lo tanto la oficina de control disciplinario podrá tomar las acciones correspondientes al funcionario que tiene el equipo de cómputo en su inventario.

Adquisición de equipos tecnológicos

La Secretaría TIC deberá verificar las características y el estado de todos los equipos tecnológicos que ingresan a la Alcaldía de Armenia, como parte de adquisiciones que haga la entidad, previo al ingreso a bienes y suministros

Controles

- Todos los dispositivos adquiridos deben contar con la garantía de fábrica. Esta debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento.

- Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

- Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

- Cuando los dispositivos tecnológicos como computadores e impresoras sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros se encuentre en Colombia.

Mantenimiento Preventivo y Correctivo

La secretaría TIC es la única dependencia autorizada para realizar el mantenimiento preventivo y correctivo de los equipos de cómputo de la entidad, a través de los funcionarios contratados para tal fin.

Controles

- Los funcionarios que no pertenezcan a la secretaría TIC no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos.

- El Servidor Público que requiera soporte técnico debe dar aviso a la Secretaría TIC a través de la mesa de ayuda, para que allí el encargado envíe el personal especializado a diagnosticar el equipo; en caso de que se presente un daño mayor, el funcionario deberá autorizar el envió del equipo a la Secretaría TIC, autorizado al personal de dicha dirección para que realice lo necesario para el mantenimiento correctivo.

- Cuando el equipo de cómputo necesite ser formateado por alguna razón, el funcionario a cargo del equipo deberá firmar una autorización por escrito (formato de autorización formateo) y realizar la copia de seguridad de los datos que en su equipo se alojan, para que este luego pueda restaurar los archivos.

Responsabilidad del uso del recurso tecnológico

La secretaría se responsabiliza del buen funcionamiento de los equipos de cómputo de la entidad, pero lo que se haga desde lo equipos mismos es responsabilidad exclusiva de los funcionarios que trabajan con ellos a diario.

Controles

- El recurso tecnológico asignado a cada funcionario será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización del jefe inmediato y registro de la novedad en la minuta de vigilancia.

- Los Servidores Públicos a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garantizar la seguridad física del recurso tecnológico y salvaguardar la información.

- Los servidores públicos deben dar aviso de inmediato a bienes y suministros, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.

- Los servidores públicos deben comunicar de manera inmediata a el departamento administrativo de fortalecimiento institucional DAFI cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos etc.

- La Secretaría TIC recomienda a los usuarios que no deben consumir alimentos en áreas cercanas al recurso tecnológico.

- La Secretaría TIC será la responsable de Administrar las hojas de vida del recurso tecnológico, en la cual se registre todos los componentes con sus seriales, placa del equipo y el software instalado con su número de licencia respectiva.

- Aunque la Alcaldía de Armenia los equipos se encuentran licenciados con diferentes tipos de sistemas operativos, estos deben de tener activados las actualizaciones automáticas para mantener los equipos seguros.

Legalidad del Software

Desde la secretaría se vigila a través recursos humanos y tecnológicos la legalidad del software instalado en la entidad, pero los funcionarios que tienen equipos de cómputo de la entidad deben asumir responsabilidades en el uso de los mismos.

Controles

- Todo software instalado en equipos de la Entidad será autorizado o instalado por la Secretaría TIC, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

- El funcionario que tiene asignado el equipo de cómputo asumirá la responsabilidad por el software instalado en el computador que le sea asignado o que esté utilizando. Toda aplicación que esté instalada debe estar debidamente licenciada.

- La Secretaría TIC será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

Política de seguridad de escritorio limpio y pantalla limpia

Todos los funcionarios públicos, incluidos contratistas deberán conservar el puesto de trabajo y la pantalla del equipo de cómputo limpia de documentos, archivos o dispositivos de almacenamiento removibles.

Controles

- La Alcaldía de Armenia a través del comité de seguridad de la información y el líder del proceso 18 (infraestructura tecnológica) de la secretaría TIC remendará y vigilará a los funcionarios públicos que tengan equipos de la entidad, a que adopten buenas prácticas en el manejo y administración de la información física y electrónica a su cargo, conforme a su clasificación, con el fin de evitar el acceso a personas no autorizadas.

- Almacenar de forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) en cajones bajo llave, con el fin de evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

- Una vez culmine el proceso de impresión o copiado, los documentos deberán ser retirados por el funcionario responsable de forma inmediato.

- Conforme a los niveles de clasificación de la información de cada funcionario, los archivos o carpetas deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, evitando, por ejemplo, guardarlos en el escritorio del sistema de cómputo.

- Los funcionarios de planta, contratistas y terceros de la Alcaldía de Armenia serán los responsables del buen uso de la información tanto física como lógica, y del cumplimiento de los lineamientos determinados en esta política.

- La Secretaría TIC, será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado y así proteger los equipos contra accesos no autorizados.

CONTROL DE ACCESO

Este grupo de políticas hacen referencia a todas aquellas directrices mediante las cuales la Alcaldía de Armenia determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad de los lugares protegidos del centro administrativo municipal, todo esto relacionado con los accesos protegidos donde se encuentra la información y/o datos protegidos de la entidad, sin importar si estos accesos sean electrónicos o físicos.

Política de control de acceso y administración de contraseñas

Las tareas realizadas por los usuarios en cada uno de los sistemas de información de la Administración municipal, serán controladas por medio de la creación de cuentas de usuario en el dominio ARMENIA.COM de la entidad, los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles establecidos por la Secretaría TIC, adicionalmente los lugares protegidos donde se procesa grandes cantidades de información deberán contar con seguridad tanto física como electrónica.

Controles

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información:
1. Nombre completo del funcionario que utilizará el equipo y/o que pertenece el equipo en el inventario.
2. Cuenta de usuario del aplicativo mesa de ayuda para la notificación de contraseña.
3. Tipo de vinculación: (Personal de Planta o Prestación de Servicios).
4. En caso de solicitar acceso a aplicativos especiales se debe especificar por cada uno de ellos los permisos a los que va a tener derecho.
5. Los permisos especiales deberán ser solicitados por el supervisor o secretario responsable de la dependencia.

Cambio Forzoso de Todas las Contraseñas del Administrador

Siempre que se detecte un ingreso no autorizado a cualquier sistema de información, con la contraseña de administrador, el funcionario encargado de administrar los servicios en los servidores a cargo de la Secretaría TIC deberá cambiar inmediatamente cada una de sus contraseñas en el sistema, con el fin de que se viole la seguridad e integridad de los datos.

Cambios de Contraseñas Periódicas para el Administrador

El o el administrador (es) deben cambiar periódicamente la contraseña en el sistema (dominio de la gobernación del Quindío).

Control de Acceso al Sistema con contraseña Individual para cada Usuario: Se precisa que el control de acceso al cualquier equipo del centro administrativo municipal, se debe realizar por medio de usuario único, controlado por la Secretaría TIC a través del directorio activo, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

- La Secretaría TIC bloqueará desde el dominio el acceso a los equipos en los siguientes horarios: Lunes a viernes de 9:00 pm a 6:00 am del siguiente día. Sábados: de 4:00 pm en adelante. Domingos: Todo el día.

- Las personas que deseen trabajar en los horarios no permitidos deberán realizar la solicitud a través de la intranet, oficio que deberá tener el visto bueno del jefe inmediato.

- La secretaría TIC informará mediante circulares y capacitaciones del acceso a funcionarios a la entidad en horarios no permitidos, lo anterior con el fin de habilitar dicho usuario para trabajar en el horario.

- Los equipos que se encuentran en el dominio de la gobernación del Quindío se deberán bloquear cada cinco (5) minutos que pasen de tiempo de inactividad, lo anterior para evitar acceso no autorizado de alguna persona al equipo.

Entrega de Contraseñas a Usuarios
Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico o través de la mesa de ayuda.

Confidencialidad de las contraseñas

Las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los servidores públicos serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

Política de seguridad de control de acceso físico

El acceso a las instalaciones físicas de la Alcaldía de Armenia deberá ser supervisado por controles acceso físico y electrónico, que garanticen la integridad de la información que se maneja en las diferentes dependencias de la entidad.

Controles

Controles de acceso físico

- Para el ingreso a las instalaciones del centro Administrativo municipal se deberá inspeccionar por parte del personal autorizado a los visitantes de manera que se ejerzan controles físicos a todas las personas.

- Se deberá implementar controles de manera física y electrónica en los que se puedan registrar la fecha, el horario de ingreso o egreso de cualquier visitante, dichos controles se realizaran mediante torniquetes los cuales funcionan con control de acceso biométrico.

Controles de acceso físico a lugares protegidos

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico.

Estos controles de acceso físico deben tener, por lo menos, las siguientes características:

- Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso justificando propósitos específicos y autorizados e informando al visitante en el momento de ingreso, sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

- Deberá existir una bitácora de ingreso, en el cual se registre la fecha la hora de entrada y la hora de salida a los lugares restringidos (como data center).

- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

- Revisar y actualizar cada tiempo determinado (no mayor a 6 meses), los derechos de acceso a las áreas protegidas, los que debe ser documentados y firmados por el responsable del área organizacional de la que dependa y el comité de seguridad de la información.

- Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Oficina de Control Interno o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

Áreas protegidas

Para la selección y el diseño de un área protegida se tendrá en cuenta e riesgo o posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, y en lo posible se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas del centro administrativo municipal:

- Datacenter Principal.
- Centros de cableado de cada piso.
- Todas las áreas donde se almacene o procese información crítica de la Entidad.
- Área de Tesorería municipal

Se establecen las siguientes medidas de protección para áreas protegidas:

- Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

- Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información debe ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

- Ubicar las funciones y la infraestructura tecnológica de soporte, por ejemplo: impresoras, fotocopiadoras, scanners, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

- Agregar protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

Implementar mecanismos de control para la detección de intrusos:

- Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.

- Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

- Almacenar los materiales peligrosos o combustibles en lugares seguros, a una distancia prudencial de las áreas protegidas de la entidad.

- Los suministros, como implementos de escritorio, no debe ser trasladados, ubicados o almacenados en las áreas protegidas.

- Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

PRIVACIDAD Y CONFIDENCIALIDAD

Esta política contiene la descripción y los controles que la Alcaldía de Armenia realiza en el tratamiento de los datos personales. Dicha política está reglamentada conforme a la normatividad vigente.

Finalidad y tratamiento al cual serán sometidos los datos personales de los usuarios

En relación con la naturaleza y las funciones propias de la alcaldía de Armenia:

- El tratamiento de los datos se realizará con la finalidad de las funciones propias del departamento, en las disposiciones contenidas en la ley 1581 de 2012[1] (Ministerio de tecnologias de la información y comunicaciones, 2013) y el decreto 1377 de 2013[2] (Ministerio de tecnologias de la información y comunicaciones, 2013) demás normas que los modifiquen, adicionen, sustituyan o complementen.

- El tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, dependiendo del tipo de relación jurídica entablada con el municipio de Armenia (incluye, entre otros, funcionarios, ex-funcionarios, judicantes, practicantes y aspirantes a cargos).

- El tratamiento de los datos se realizará para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la practicante requiere para su funcionamiento de acuerdo a la normatividad vigente.

Derechos de los titulares de los datos personales

[1] "Por la cual se dictan disposiciones generales para la protección de datos personales"
[2] "Por el cual se reglamenta parcialmente la Ley 1581 de 2012"

- Conocer, actualizar y rectificar sus datos personales frente a la Alcaldía de Armenia, como responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

- Solicitar prueba de la autorización otorgada a la Alcaldía de Armenia como responsable y encargado del tratamiento de los datos personales, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.

- Ser informado por el municipio como responsable del tratamiento y encargado del tratamiento de los datos personales, previa solicitud, respecto del uso que le ha dado a los datos personales del titular.

- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la superintendencia de industria y comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la ley 1581 de 2012 y a la constitución.

- Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento

Procedimiento para ejercer los derechos

Consultas: Sobre la información de sus datos personales se absolverán en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible responder la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su solicitud, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.
Reclamos: Los Titulares o sus causahabientes que consideren que la información contenida en una base de datos del departamento debe ser objeto de corrección, actualización o supresión, o que adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante la Alcaldía de Armenia, a través de

cualquiera de los canales de comunicación con los que cuenta la entidad; y éste deberá contener la siguiente información:

- Nombre e identificación del Titular.

- La descripción precisa y completa de los hechos que dan lugar al reclamo.

  La dirección física o electrónica para remitir la respuesta e informar sobre el estado del trámite.

- Los documentos y demás pruebas que se pretendan hacer valer. En caso de que la Alcaldía de Armenia no sea competente para resolver el reclamo presentado ante el mismo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

- Si el reclamo resulta incompleto, la Alcaldía de Armenia requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el peticionario presente la información solicitada, se entenderá que ha desistido de aquél.

- El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo, y si no fuere posible responder en dicho término, la Alcaldía de Armenia informará al interesado los motivos de la demora y la fecha en que aquél se atenderá, sin llegar a superar, en ningún caso, los ocho (8) días hábiles siguientes al vencimiento del primer término.

Datos sensibles en el tratamiento de datos personales

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.

Y por su parte, la Ley 1266 de 2008 define los siguientes tipos de datos de carácter personal:

Dato público: Es el 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 presente

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 solo 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 a que se refiere el Título IV de la Ley 1266 de 2008.

Dato privado: Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular. La Ley 1581 de 2012, establece una categoría especial a los datos personales de los niños, niñas y adolescentes y prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos que por su naturaleza son públicos, la Corte Constitucional precisó que independientemente de la naturaleza del dato, se puede realizar el tratamiento de éstos "siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, niñas y adolescentes y se asegure sin excepción alguna el respeto a sus derechos prevalentes". Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Autorización del titular de los datos personales

Sin perjuicio de las excepciones previstas en la ley, en el tratamiento se requiere la autorización previa, expresa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

Casos en los que no se requiera autorización del titular de los datos personales

La autorización del titular no será necesaria cuando se trate de:

Información requerida por la Alcaldía de Armenia en ejercicio de sus funciones legales o por orden judicial.

Datos de naturaleza pública.

- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

- Datos relacionados con el registro civil de las personas.

Autorización de tratamiento de datos personales sensibles (Categorías especiales de datos)

El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.

En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:

- ❖ Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.

- ❖ Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles

Modo de obtener la autorización

Para efectos de dar cumplimiento a lo dispuesto en el artículo 9° de la Ley 1581 de 2012, la Alcaldía de Armenia estableció mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del Decreto reglamentario 1377 de 2013, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

La autorización será solicitada por la Alcaldía de Armenia de manera previa al tratamiento de los datos personales.

Prueba de la autorización

La alcaldía de Armenia conservará la prueba de la autorización otorgada por los titulares de los datos personales para su tratamiento, para lo cual utilizará los mecanismos disponibles a su alcance en la actualidad al igual que adoptará las acciones necesarias para mantener el registro de la forma y fecha y en la que obtuvo ésta. En consecuencia, la Alcaldía de Armenia podrá establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.