Tabla de Contenido

1. Introducción

Considerando que la transformación digital viene avanzando en grandes velocidades y que la protección de los activos de la información y la gestión de riesgos asociados al entorno digital se han convertido en pilares fundamentales para el desarrollo y la eficiencia de la gestión pública. El Gobierno Nacional, por medio del Documento CONPES 3854 de 2016, adoptó la Política Nacional de Seguridad Digital, bajo la coordinación de la Presidencia de la República, con el objetivo de orientar y establecer los lineamientos estratégicos que deben seguir las entidades públicas y privadas del país.

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.

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.

Lo que se busca al adoptar esa Política es fortalecer las capacidades institucionales y operativas de los diferentes departamentos y secretarias de la Alcaldía de Armenia, para identificar, gestionar, tratar y mitigar los riesgos digitales que puedan comprometer la integridad, disponibilidad, confidencialidad y continuidad de los servicios que se prestan a la ciudadanía. Además, promueve la creación y adopción de mecanismos de resiliencia, recuperación y respuesta ante incidentes.

Para la secretaria TIC adoptar esta política representa un compromiso estratégico con el fortalecimiento institucional, la protección de la infraestructura tecnológica y la promoción de una cultura de seguridad digital. Todo ello con el propósito de asegurar la confianza en los servicios digitales, proteger los datos de los ciudadanos y contribuir activamente al crecimiento de la entidad.

2. Objetivo

Implementar la Política de Seguridad Digital, con el fin de fortalecer las capacidades institucionales para identificar, gestionar, tratar y mitigar los riesgos asociados al entorno digital, protegiendo los activos de información y los sistemas tecnológicos críticos de la entidad.

3. Alcance

La Política de Seguridad Digital en cumplimiento al documento del CONPES 3854 de 2016 y atendiendo a la normativa establecida por la Ley Estatutaria 1581 de 2012, la Ley 1266 de 2008, y la reciente Ley 2157 de 2021, la Alcaldía de Armenia aplica al tratamiento de la información digital y de los datos personales que administra la Alcaldía de Armenia, incluyendo la recolección, almacenamiento, uso, circulación, transferencia, actualización, supresión y reporte de datos en medios físicos o electrónicos, tanto por parte de servidores públicos, contratistas y terceros autorizados, como por las plataformas y sistemas de información de la entidad.

4. Marco Normativo

Legislación	Tema
CONPES 3854 de 2016	Define la Política Nacional de Seguridad Digital, orientando la gestión de riesgos digitales en entidades públicas y privadas.
Acuerdo 08 de 2019 (Concejo Municipal de Armenia)	Adopta el Plan de Desarrollo Municipal e incluye principios de transformación digital y fortalecimiento institucional.
Acuerdo 02 de 2018 (Concejo Municipal de Armenia)	Aprueba lineamientos de modernización administrativa y tecnológica en la administración municipal.
Decreto 1078 de 2015	Decreto Único Reglamentario del sector TIC. Incluye lineamientos para Gobierno Digital y seguridad de la información.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública. Garantiza la disponibilidad y seguridad de la información pública.
Decreto 113 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Ley 1581 de 2012	Ley Estatutaria de Protección de Datos Personales. Establece principios para el tratamiento responsable de datos personales.
Ley 1273 de 2009	Modifica el Código Penal para tipificar delitos informáticos, fortaleciendo la protección de la información y los sistemas.

Ley 1928 de 2018	Por medio de la cual se aprueba el Convenio de Budapest sobre ciberdelincuencia, lo cual fortalece la cooperación internacional para la lucha contra los delitos informáticos.
Norma Técnica Colombiana NTC ISO/IEC 27001 y 27002	Normas internacionales sobre gestión de seguridad de la información.
Ley 527 de 1999	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.
Ley 1266 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.
Ley 2157 de 2021	Por medio de la cual se dictan disposiciones generales del Habeas Data y se regula el reporte de información negativa en las centrales de riesgo crediticio.
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
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
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.

5. Ámbito De Aplicación

Política De Seguridad Digital

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 digital 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 de seguridad digital asociados a los aplicativos misionales de la entidad 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 digital.
- 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 digital.
- Fortalecer la cultura de seguridad digital 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 TIC ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad Digital, 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 digital 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.**

6. Lineamientos generales para la implementación

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:

- Dando cumplimiento a la asignación de un responsable de la seguridad Digital de estas políticas serán autorizadas únicamente 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 el logro de los objetivos institucionales, y deberán estar **documentadas formalmente**. 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 digital.

- 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.

- Las políticas de seguridad digital serán **evaluadas cuatrimestralmente** mediante mecanismos de autocontrol y autoevaluación, a través de **indicadores de gestión propuestos por el MSPI**, con el fin de garantizar el mejoramiento continúo, atendiendo a la normativa propuesta.

- Considerando que la aplicación de esta política **responde al interés institucional** de diseñar, implementar y sostener el **Modelo de Seguridad y Privacidad de la Información (MSPI)**, conforme a la normativa nacional vigente.

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

CRONOGRAMA DE SEGURIDAD DIGITAL				
FASE MSPI	**ACTIVIDADES**	**META**	**PRODUCTO**	**RESPONSABLE(S)**
Diagnóstico	Realizar el Diagnóstico del modelo seguridad privacidad de la Información de la Alcaldía de Armenia	Establecer las fortalezas y debilidades que tiene la entidad en cuanto a la seguridad y privacidad de la información	Diagnóstico MSPI	Profesional Especializado
Planificación	Realizar Cronograma de actividades de todas las fases del modelo de seguridad y privacidad de la información MSPI	Establecer el cronograma de actividades correspondiente a la implementación del modelo de seguridad y privacidad de la información	Plan de seguridad y privacidad de la información	Profesional Especializado
	Actualizar Políticas de seguridad de la información	Diseñar y/o actualizar las políticas de seguridad y privacidad de la información de la Alcaldía de Armenia	Políticas de seguridad y privacidad de la información	Profesional Especializado

	Diseñar y/o actualizar los Procedimientos de seguridad de la información.	Actualizar los procedimientos de seguridad y privacidad de la información, con el fin de que sean normalizados.	Procedimientos de seguridad de la información.	Profesional Especializado
	Definir los Roles y responsabilidades de seguridad y privacidad de la información.	Lograr establecer los roles y responsabilidades en seguridad y privacidad de la información que incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Roles y responsabilidades de seguridad y privacidad de la información.	Profesional Especializado

	Realizar y/o Actualizar la matriz de activos de información	Crear un documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.	Matriz de Inventario de activos de información.	Profesional Especializado
	Con base a la matriz de inventario de activos de información, se identifican los riesgos de seguridad y privacidad de la información y seguridad digital	Identificación, Valoración y tratamiento de riesgo.	Plan de tratamiento de riesgos de seguridad y privacidad de la información y matriz de riesgos de seguridad y privacidad de la información y seguridad digital	Profesional Especializado
	Realizar piezas gráficas y material de promoción y sensibilización en seguridad de la	Crea un plan y/o Documento con el plan de comunicación, sensibilización y	Plan de sensibilización y comunicación de seguridad y	Profesional Especializado

	información en la Alcaldía de Armenia	capacitación para la entidad.	privacidad de la información	
	Realizar todas las actividades de identificación y planificación de la infraestructura compatible con el protocolo IPV6	Establecer el estado actual de la entidad en cuando a la implementación del protocolo IPV6 en la entidad.	Actualizar Plan de diagnóstico de IPv4 a IPv6.	Profesional Especializado
Implementación	Crear la declaración de aplicabilidad y el plan de control operacional	Establecer un Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Declaración de aplicabilidad y plan de control operacional	Profesional Especializado
	Realizar las actividades necesarias con el fin de dar seguimiento a el plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Implementación del plan de tratamiento de riesgos.	Profesional Especializado
	Definir y medir los indicadores de gestión de la	Documento con la descripción de los indicadores de gestión	Indicadores De Gestión.	Profesional Especializado

	implementación del modelo de seguridad y privacidad de la información	de seguridad y privacidad de la información.		
	Definir las actividades de transición hacia el protocolo IPV6 en la administración central departamental	Realizar un plan de transición del protocolo de IPV6 de la Alcaldía de Armenia	Plan de Transición de IPv4 a IPv6	Profesional Especializado
Evaluación de Desempeño	Con los datos obtenidos en la implementación, se debe realizar plan donde se evalúe el desempeño de la planificación e implementación del modelo MSPI	Crear documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Plan seguimiento MSPI	Profesional Especializado

	Definir las actividades que debe realizar la persona y/o organización que realice la auditoria del modelo MSPI	Realizar una auditoría independiente sobre la efectividad de la implementación del modelo de seguridad y privacidad de la información	Plan de Ejecución de Auditorias	Profesional Especializado
Mejora Continua	Con base en los resultados de la evaluación de desempeño se debe plantear el plan de mejoramiento.	Realizar un Plan de mejoramiento, con el fin de comenzar de nuevo el ciclo del modelo MSPI y corregir lo que haya lugar	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Profesional Especializado

Es considerable tener en cuenta que la **integración entre el MSPI, la Política de Seguridad Digital y el MIPG permite** a la Alcaldía de Armenia la consolidación de una cultura organizacional orientada a la protección de la información, alineando sus procesos tecnológicos con la **estrategia institucional y los marcos normativos nacionales** para fortalecer la **gestión del riesgo digital**, la **transparencia** y la **confianza en los servicios públicos digitales.**

Estableciendo el **Modelo Integra De Planeación Y Gestión** (**MIPG)** y teniendo en cuenta la dimensión de **"Gestión con valores para resultados"** que promueve una cultura organizacional centrada en **principios éticos, transparencia y orientación al logro de impactos reales en la ciudadanía**. De este modo se puede inferir que la Alcaldía de Armenia:

Transparencia y Confianza Digital: permite garantizar que los sistemas de información protejan los datos personales adoptando la normativa **Ley 1712 de 2014** y la **Ley 1581 de 2012.**

Cultura ética y responsabilidad institucional: Los servidores públicos tanto como de planta como contratitas deben aplicar conductas responsables para proteger las contraseñas y reportar incidentes, ya que deben actuar con integridad con el manejo de tratamiento de la información pública.

Orientación a resultados reales: Un **SGSI (Sistema de Gestión de Seguridad de la Información)** efectivo reduce interrupciones, pérdidas de datos y ataques, mejorando la continuidad del servicio público, promoviendo una **gestión basada en riesgos**, con indicadores que permiten tomar decisiones informadas y alineadas al propósito institucional.

Formación y conciencia: Capacitar a los servidores públicos en los riegos de seguridad Digital como parte de la gestión del conocimiento con enfoque en valores: actuar con prevención, cuidado y solidaridad institucional.

7. Criterios diferenciales para la Política de Seguridad Digital

La **secretaria Tic** de la Alcaldía de Armenia adoptara la implementación de la política de Seguridad Digital según como no lo indica la normativa y así de este modo dar cumpliendo a los lineamientos del **Modelo de Seguridad y Privacidad de la Información (MSPI)** y del **CONPES 3854 de 2016.**

La política podrá Identificar, analizar y valorar los riesgos que afectan la infraestructura tecnológica y la información institucional, Estableciendo medidas de tratamiento basadas en controles técnicos, administrativos y organizacionales, priorizando las acciones de mitigación y definir responsables dentro de los procesos misionales y de soporte facilitando la toma de decisiones informadas y alineadas a los objetivos estratégicos de la entidad.

Asimismo, esta política reconoce que la **gestión de riesgos de seguridad digital es dinámica**, por lo cual se establece su **evaluación periódica y actualización continua**, en concordancia con los principios de mejora del MIPG y de los sistemas de gestión de calidad adoptados por la entidad.

Elaborado por:	**Revisado por:**	**Aprobado por:**
Alejandra Zuluaga- Contratista secretaria TIC.	Juan Sebastián Herrera Pardo – Secretario TIC	Comité Institucional de Gestión y Desempeño realizado el día 31 de Julio del 2025 mediante acta No 03