

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Nombre de la política / plan:	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Dependencia responsable:	Secretaría General
Fecha de aprobación de la política:	30 de enero de 2026
No. de acta del Comité Institucional de Gestión y Desempeño del AMB en que fue aprobada:	No. 01 de enero de 2026
Vigencia de la política / plan:	2026
Dimensión del MIPG a la que se asocia la política / plan:	Información y Comunicaciones

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Entidad: Área Metropolitana De Bucaramanga-AMB

MARCO DE REFERENCIA

El Área Metropolitana de Bucaramanga (AMB) reconoce la información como uno de los activos más valiosos y estratégicos para el cumplimiento de su misión institucional. En el desarrollo de sus funciones, la Entidad gestiona, almacena, procesa, custodia, intercambia y transmite información que resulta crítica para la toma de decisiones y para la prestación eficiente de sus servicios públicos. La exposición no autorizada, alteración o pérdida de esta información puede afectar la gestión pública, generar riesgos institucionales y vulnerar derechos de los ciudadanos. Por ello, la protección y defensa de los activos de información constituye una labor esencial para garantizar la continuidad operativa, el logro de los objetivos institucionales, el cumplimiento normativo y la confianza de las partes interesadas.

El marco normativo vigente establece que la seguridad y privacidad de la información deben alinearse con el habilitador de Seguridad y Privacidad de la Información definido en la Política de Gobierno Digital, conforme a lo dispuesto en el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector TIC. Esta disposición obliga a las entidades reguladas a desarrollar capacidades para implementar lineamientos que garanticen la protección de la información en todos los procesos, trámites, servicios, sistemas, infraestructuras tecnológicas y, en general, en los activos de información bajo su responsabilidad. Su objetivo fundamental es asegurar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Asimismo, el Decreto 2106 de 2019 establece en su artículo 16 que las autoridades que adelanten trámites y servicios por medios digitales deberán disponer de sistemas de gestión documental electrónica y archivo digital que aseguren la integridad, disponibilidad, autenticidad y trazabilidad de la información. En consecuencia, el AMB debe implementar y fortalecer una estrategia de seguridad digital que garantice la

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

adecuada protección de la información tratada mediante plataformas y medios electrónicos, en concordancia con las directrices del Ministerio TIC y del Archivo General de la Nación.

De igual forma, la Resolución 500 de 2021 que adopta los lineamientos, estándares y modelo para la estrategia de seguridad digital como habilitador de la Política de Gobierno Digital, establece la obligación de implementar el Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo establece lineamientos para la gestión de riesgos de seguridad de la información, la atención de incidentes de seguridad digital, la adopción de estándares y buenas prácticas, y la formulación de una estrategia integral de seguridad y privacidad de la información, aspectos que son plenamente aplicables al AMB para la vigencia 2026.

En cumplimiento de estas disposiciones y en coherencia con el Modelo Integrado de Planeación y Gestión – MIPG, el Área Metropolitana de Bucaramanga formula el Plan de Seguridad y Privacidad de la Información para la vigencia 2026, el cual define la hoja de ruta institucional para la gestión de riesgos, la protección de datos personales, el fortalecimiento del Sistema de Gestión de Seguridad Digital (SGSD) y la consolidación del Programa Integral de Protección de Datos Personales. Este plan establece acciones orientadas a prevenir, detectar, responder y recuperar frente a incidentes de seguridad digital, promoviendo un enfoque de mejora continua que permita garantizar la protección de la información generada, administrada y custodiada por la Entidad frente a amenazas internas y externas.

MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga se sustenta en el conjunto de normas, lineamientos y estándares que regulan la gestión de la información, la protección de datos, la seguridad digital y el Gobierno Digital en las entidades públicas colombianas. Este marco normativo constituye la base obligatoria para la planificación, implementación, seguimiento y mejora continua del Sistema de Gestión de Seguridad Digital (SGSD) y del Modelo de Seguridad y Privacidad de la Información (MSPI).

1. Normatividad Nacional Aplicable

1.1. Protección de Datos Personales

- **Ley Estatutaria 1581 de 2012:** Régimen general de protección de datos personales.
- **Decreto 1377 de 2013 y Decreto 1081 de 2015:** Reglamentación parcial de la Ley 1581.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

- **Constitución Política de Colombia — Artículos 15, 20, 23 y 74:** Derecho a la intimidad, habeas data, acceso a la información, derecho de petición e información pública.

1.2. Transparencia, Acceso a la Información y Gestión Documental

- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- **Ley 594 de 2000:** Ley General de Archivos.
- Decretos reglamentarios:
 - **Decreto 1081 de 2015**
 - **Decreto 2578 de 2012**
 - **Decreto 4124 de 2004**
 - **Decreto 1100 de 2014:** Estos establecen lineamientos para la gestión documental, preservación digital y administración de archivos electrónicos.

1.3. Seguridad Digital, Gobierno Digital y TIC

- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC; regula Gobierno Digital, interoperabilidad, servicios ciudadanos digitales y seguridad digital.
- **Decreto 1008 de 2018 y Decreto 767 de 2022:** Lineamientos generales de la Política de Gobierno Digital y actualización del modelo.
- **Decreto 2106 de 2019:** Simplificación de trámites; exige seguridad, integridad, autenticidad y disponibilidad en expedientes y trámites electrónicos.
- **Decreto 1083 de 2015:** Normas sobre organización administrativa y Sistema de Control Interno; aplica a la gestión de riesgos y controles de información.

1.4. Normatividad Específica de Seguridad de la Información

- **Resolución 500 de 2021 — MinTIC:** Lineamientos y estándares para la estrategia de seguridad digital; adopta el Modelo de Seguridad y Privacidad de la Información (MSPI).
- **Resolución 746 de 2022 — MinTIC:** Fortalece el MSPI y define lineamientos adicionales.
- **Resolución 02277 de 2025 — MinTIC:** Actualiza y moderniza el MSPI 2025; establece obligaciones para entidades públicas.
- **Lineamientos de Gestión de Incidentes de Seguridad Digital — MinTIC 2025:** Esquema para detección, análisis, respuesta y reporte de incidentes.
- **Manual de Gobierno Digital — Módulo de Seguridad y Privacidad:** Documento técnico obligatorio para la implementación del MSPI.

1.5. Propiedad Intelectual y Derechos de Autor

- **Ley 23 de 1982:** Normas sobre derechos de autor.
- **Ley 44 de 1993:** Modifica la Ley 23 de 1982 y la Ley 29 de 1944.
- **Decisión Andina 351 de 1993:** Régimen común de derechos de autor y conexos.
- **Ley 527 de 1999:** Regula mensajes de datos, comercio electrónico y firmas digitales; establece SSF de certificación digital.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

2. Modelo Integrado de Planeación y Gestión – MIPG

El MIPG orienta la gestión institucional y transversaliza la protección de la información en las entidades públicas. Para la política y el plan de seguridad y privacidad, aplican:

2.1. Gestión del Conocimiento y la Información

Protección de la información como activo estratégico, asegurando su integridad, disponibilidad, privacidad y uso ético.

2.2. Control Interno

Obligación de implementar controles, auditorías y mecanismos de seguimiento y evaluación del SGSD y del MSPI.

2.3. Gestión del Riesgo

Identificación, análisis, valoración y tratamiento de riesgos asociados a seguridad digital, privacidad, ciberseguridad y continuidad operativa.

2.4. Gestión del Desempeño y Resultados

Asegura la calidad del servicio, cumplimiento legal y mejora continua del Sistema de Gestión de Seguridad de la Información.

2.5. Arquitectura Institucional y Talento Humano

Define roles, competencias y responsabilidades para servidores públicos y terceros respecto a seguridad y privacidad de la información.

3. Marcos, Estándares y Buenas Prácticas Internacionales

3.1. Estándares ISO

- **ISO/IEC 27001:2022** – Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002:2022** – Controles de seguridad.
- **ISO/IEC 27005** – Gestión del riesgo.
- **ISO/IEC 22301** – Gestión de continuidad del negocio.
- **ISO/IEC 27035** – Gestión de incidentes de seguridad.

3.2. NIST

- **NIST Cybersecurity Framework (CSF)**
- **NIST SP 800-30, SP 800-53 y SP 1800:** Marcos para identificación, protección, detección, respuesta y recuperación ante eventos de seguridad.

3.3. COBIT

Marco para gobierno y control de TI que complementa el MSPI y la gestión estratégica de la seguridad.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

4. Lineamientos Técnicos MinTIC para el MSPI

- Documento maestro del **Modelo de Seguridad y Privacidad de la Información – MSPI 2025**
- Manual de Gobierno Digital – Seguridad y Privacidad
- Lineamientos de gestión de incidentes de seguridad digital (2025)
- Estrategia de Seguridad Digital – MinTIC

1. OBJETIVO

Fortalecer la confidencialidad, integridad, disponibilidad y privacidad de los activos de información del Área Metropolitana de Bucaramanga, mediante la gestión eficaz del riesgo y la implementación de estrategias y controles de seguridad digital que reduzcan las amenazas y vulnerabilidades a niveles aceptables.

El Plan establece la hoja de ruta para consolidar el Sistema de Gestión de Seguridad y Privacidad de la Información, garantizar la continuidad operativa de los servicios institucionales, dar cumplimiento a los requisitos normativos aplicables y asegurar un entorno confiable, seguro y alineado con el MSPI, el MIPG y los estándares internacionales vigentes.

2. OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital del Área Metropolitana de Bucaramanga
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a ejecutar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

3. PROPÓSITO

El Plan de Acción de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga (AMB) aplica a todo el modelo de operación por procesos de la Entidad y orienta la ejecución de las actividades necesarias para garantizar la protección de los activos de información, en cumplimiento de la normativa vigente en materia de seguridad digital y gestión de datos personales.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Este plan incorpora las acciones requeridas por el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Seguridad Digital, el Programa Integral de Protección de Datos Personales, y las necesidades identificadas por las diferentes áreas del AMB en materia de seguridad y privacidad. De igual forma, articula los lineamientos técnicos y de gestión establecidos en:

- El Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública, en lo relacionado con la gestión institucional.
- El Capítulo 1 del Título 9 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector TIC, que reglamenta la Política de Gobierno Digital.
- La Resolución 500 de 2021, que adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la Política de Gobierno Digital.
- La Resolución 2277 de 2025, que actualiza el Anexo 1 del MSPI y sus lineamientos técnicos.
- Los principios y requisitos de la NTC/ISO/IEC 27001, como referencia para el fortalecimiento del Sistema de Gestión de Seguridad de la Información.

4. GLOSARIO

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27000).

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Sistema de Gestión de Seguridad de la Información – SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Confidencialidad: Propiedad según la cual la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: Propiedad que garantiza que la información es precisa, completa y no ha sido modificada de manera no autorizada.

Disponibilidad: Propiedad que asegura que la información y los servicios asociados están accesibles y utilizables cuando los usuarios autorizados los requieren.

Privacidad: Derecho de las personas a que su información personal sea tratada conforme a los principios y reglas establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012).

Dato Sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (Ley 1581 de 2012).

Titular de la Información: Persona natural cuyos datos personales son objeto de tratamiento.

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión.

Incidente de Seguridad de la Información: Evento identificable en un sistema, servicio o red que indica una posible violación de la política de seguridad, una falla de controles o una situación que compromete la confidencialidad, integridad, disponibilidad o privacidad de la información.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Gestión de Incidentes de Seguridad Digital: Conjunto de actividades destinadas a prevenir, detectar, analizar, contener, recuperar y reportar incidentes que afectan los activos de información o la infraestructura tecnológica.

Continuidad del Negocio: Capacidad de una organización para continuar operando durante y después de un incidente disruptivo.

Recuperación ante Desastres (DRP): Conjunto de procedimientos técnicos y administrativos orientados a restaurar sistemas, servicios e infraestructura tecnológica tras un incidente mayor.

Política de Seguridad de la Información: Declaración formal de la alta dirección que define la orientación y el compromiso para proteger los activos de información.

MSPI – Modelo de Seguridad y Privacidad de la Información: Marco establecido por el MinTIC (Resolución 500 de 2021 y Resolución 2277 de 2025) que orienta la gestión de la seguridad y privacidad en entidades públicas.

MIPG – Modelo Integrado de Planeación y Gestión: Modelo de gestión del Estado colombiano que integra políticas de gestión y desempeño institucional, incluyendo la Seguridad Digital como parte de su dimensión de Gestión con Integridad.

Tercero Autorizado: Persona natural o jurídica, contratista o proveedor, que accede a información institucional bajo condiciones y controles definidos por la entidad.

5. ALCANCE

El presente documento aplica a todo el modelo de operación por procesos del AMB y da cumplimiento a lo dispuesto en el Decreto 1083 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, y en el Capítulo 1 del Título 9 del Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”. Asimismo, se articula con el Modelo de Seguridad y Privacidad de la Información establecido en la Resolución 500 de 2021 y su actualización en la Resolución 02277 de 2025, manteniendo alineación con la norma NTC/IEC ISO 27001.

6. ESTADO ACTUAL DE AMB RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El Área Metropolitana de Bucaramanga (AMB) se encuentra en un proceso de fortalecimiento progresivo de su Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), en cumplimiento de los lineamientos establecidos por el Modelo de

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Seguridad y Privacidad de la Información (MSPI) de la Política Nacional de Gobierno Digital. No obstante, la entidad evidencia la necesidad de consolidar una línea base clara que permita dimensionar su estado actual y orientar la planeación estratégica del Plan de Seguridad y Privacidad de la Información (PESI).

En este contexto, el AMB reconoce la importancia de realizar el autodiagnóstico del MSPI, el cual constituye un insumo fundamental para identificar brechas, capacidades existentes y niveles de madurez en materia de seguridad digital. Asimismo, se requiere evaluar el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2022, con el fin de establecer el grado de adopción de buenas prácticas internacionales y priorizar acciones de mejora.

Actualmente, la entidad cuenta con avances parciales relacionados con prácticas de control interno, gestión documental y componentes tecnológicos; sin embargo, se requiere avanzar hacia un enfoque integral y sistemático que permita implementar el Ciclo de Gestión del MSPI (Planear, Hacer, Verificar y Actuar – PHVA). La adopción de este ciclo permitirá fortalecer la gobernanza de la seguridad de la información, garantizar la identificación y tratamiento de riesgos, y asegurar la continuidad operativa de los servicios institucionales.

Adicionalmente, los resultados disponibles del Autodiagnóstico de Gobierno Digital y de la Medición FURAG evidencian oportunidades de mejora en aspectos como gestión de riesgos de seguridad, formalización de lineamientos, capacidad de respuesta ante incidentes y protección de datos personales. Estas brechas refuerzan la necesidad de una planificación estratégica que permita a la entidad evolucionar hacia niveles superiores de madurez y cumplimiento.

En síntesis, el AMB cuenta con bases iniciales para la gestión de la seguridad y privacidad de la información, pero requiere consolidar un diagnóstico integral, fortalecer su marco normativo y operativo, y avanzar de manera estructurada en la implementación del SGSPI conforme a los lineamientos nacionales e internacionales aplicables.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información Ministerio de tecnologías de la información y las comunicaciones.

Asimismo, el Área Metropolitana de Bucaramanga debe avanzar en la ejecución de acciones que permitan consolidar una visión integral de la seguridad de la información, entendida como la interacción de múltiples componentes que actúan de manera coordinada para proteger no solo los sistemas tecnológicos, sino también los activos humanos, la infraestructura física, el desarrollo e implementación de software, la gestión del talento humano, la calidad institucional, la relación con proveedores y demás elementos críticos del funcionamiento organizacional.

Esto exige la implementación de estrategias que garanticen la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la entidad, incorporando tanto medidas técnicas como mecanismos organizativos, administrativos y procedimentales. En este sentido, la seguridad de la información debe ser asumida como un pilar transversal del modelo de operación del AMB, orientado a fortalecer la protección de los activos institucionales, mitigar riesgos y asegurar un entorno confiable y resiliente frente a las amenazas emergentes.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Ilustración 2 Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)



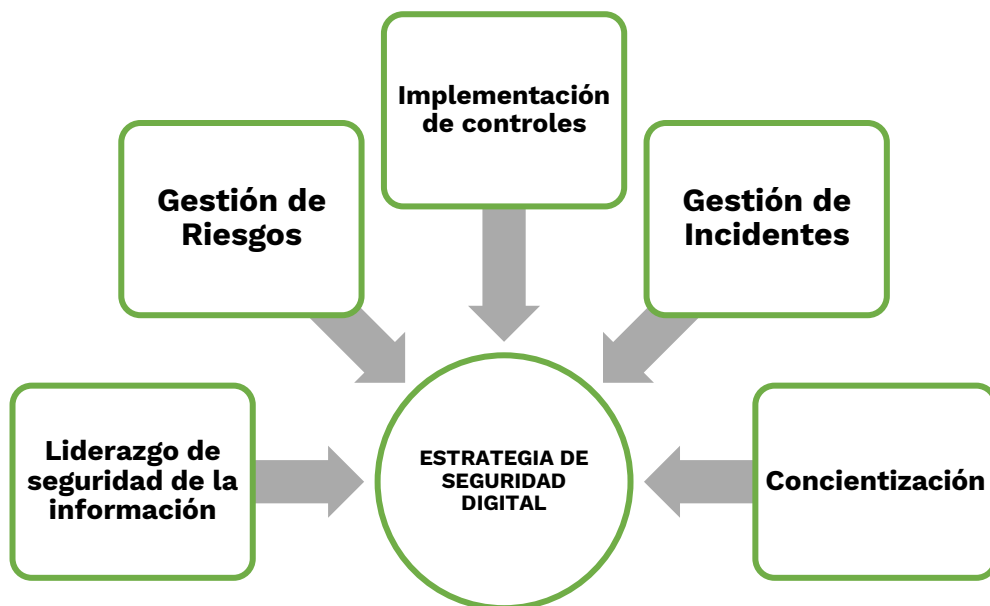
Fuente: Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información Ministerio de tecnologías de la información y las comunicaciones.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

El Área metropolitana de Bucaramanga establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos.

Por tal motivo, el AMB define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02



8. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MSPI y la resolución 500 de 2021

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad y privacidad de la información	Establecer el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

	fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo y apropiando al interior de la entidad las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

9. PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para cada estrategia específica, el Área Metropolitana de Bucaramanga define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Los proyectos deben estar relacionados tanto con el Manual de políticas como con la política de seguridad definida en la entidad, además estos proyectos deben corresponder a la implementación de controles que permita mitigar riesgos de seguridad de la información que la entidad haya identificado.

ESTRATEGIA / EJE	ACTIVIDAD	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	Actividad1: Aprobar por el comité de gestión y desempeño la política de seguridad de la información	Política de Seguridad y Privacidad formalizada, aprobada e implementada.

 ÁREA METROPOLITANA DE BUCARAMANGA BUCARAMANGA - FLORENCIANA - SION - PESQUEIRA	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

	Actividad: Definición y formalización de roles y responsabilidades del SGSI.	Documento con roles, responsables y niveles de autoridad en seguridad de la información, incorporado en la política.
	Actividad 3: Incluir el seguimiento a los temas de Seguridad de la Información en los comités de gestión de Desempeño	Actas de reuniones y seguimiento.
	Actividad 4: Elaboración y publicación del Manual de Políticas de Seguridad de la Información.	Manual de políticas institucional con lineamientos actualizados y evidencias de socialización.
	Actividad 5: Plan de Implementación del MSPI.	Documento de planificación con acciones, tiempos y responsables.
Gestión de riesgos	Actividad 1: Identificar, valorar y clasificar los riesgos de seguridad de la información asociados a los activos.	Matriz de riesgos de seguridad digital completa (activos, amenazas, vulnerabilidades, impacto y probabilidad).
	Actividad 2: Definir y ejecutar los planes de tratamiento de riesgos.	Planes de tratamiento de riesgos documentados con responsables y plazos.
	Actividad 3: Actualización del inventario de activos de información.	Inventario consolidado y clasificado de activos de información.
	Actividad 4: Monitoreo y revisión periódica de riesgos.	Informes trimestrales de revisión y seguimiento al tratamiento de riesgos.
Concientización	Actividad 1: Plan anual de sensibilización en seguridad de la información.	Plan anual de cultura, sensibilización y apropiación.
	Actividad 2: Jornadas de sensibilización a todo el personal.	Evidencias de actividades: listas de asistencia, presentaciones, memorias entre otras.
	Actividad 3: Transferencia de conocimiento mediante cursos en temas de Seguridad y privacidad de la información.	Certificaciones o constancias de participación del personal.
	Actividad 4: Medición del grado de sensibilización institucional.	Resultados de encuestas, análisis y plan de mejora
	Actividad 5: Campañas permanentes de buenas prácticas de ciberseguridad.	Piezas de campaña (afiches, correos, boletines, material gráfico entre otros).
Implementación de controles	Control 1: Política de respaldos de información.	Política formalizada y plan de respaldos implementado.
	Control 2: Procedimiento de Gestión de Cambios.	Procedimiento formal implementado y evidencias de aplicación.
	Control 3: Clasificación de la información.	Matriz de clasificación y lineamientos de manejo de datos.
	Control 4: Políticas de Desarrollo Seguro.	Lineamientos de desarrollo seguro institucional.

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

	Control 5: Implementación de solución WAF para protección de servicios web.	WAF desplegado, configurado y funcional.
	Control 6: Control de acceso lógico y fortalecimiento de autenticación.	Matriz de accesos y evidencias de controles aplicados.
	Control 7: Hardening de servidores, endpoints y aplicaciones.	Reportes de endurecimiento y configuraciones seguras aplicadas.
	Actividad 1: Definir y formalizar el procedimiento de Gestión de Incidentes.	Procedimiento de gestión de incidentes formalizado y publicado.
Gestión de incidentes	Actividad 2: Capacitar al personal en la gestión de incidentes.	Sesiones de capacitación realizadas y registradas.
	Actividad 3: Implementar un registro oficial de eventos e incidentes.	Bitácora o repositorio institucional de incidentes.
	Actividad 4: Realizar simulacros y pruebas de respuesta a incidentes.	Informes de simulacros y acciones de mejora.

10. CRONOGRAMA DE ACTIVIDADES / PROYECTOS

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

1. Liderazgo de Seguridad de la Información (Enero 2026)			
Proyecto	Actividades	Mes	Responsable
Actividad 1: Aprobación de la Política de Seguridad	Presentar política al Comité de Gestión; aprobación; publicación.	Enero	Dirección/Secretaría General / Miembros del Comité de Gestión y Desempeño
Actividad 2: Definir Roles y Responsabilidades del SGSI	Construcción, validación y formalización de roles.	Enero	Secretaría General
Actividad 3: Seguimiento en Comités	Incluir temas SGSI en agenda y generar actas.	Enero	Secretaría General
Actividad 4: Elaborar Manual de Políticas	Construcción, revisión y publicación	Enero	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
Actividad 5: Plan de Implementación del MSPI	Estructurar plan anual con actividades, responsables y tiempos.	Enero	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
2. Gestión de Riesgos (Enero – Diciembre 2026)			
Proyecto	Actividades	Meses 2026	Responsable

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

Actividad 1: Identificación y valoración de riesgos	Actualizar inventario; identificar activos; valorar riesgos.	Ene – Mar	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información / Dependencias Líderes
Actividad 2: Planes de tratamiento	Diseñar, priorizar y asignar responsables.	Mar – Jun	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
Actividad 3: Actualizar inventario de activos	Consolidación, clasificación y validación.	Ene – Feb	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
Actividad 4: Monitoreo y revisión	Seguimiento trimestral a riesgos y tratamiento.	Mar, Jun, Sep, Dic	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información

3. Concientización y Cultura (Enero – Diciembre 2026)

Proyecto	Actividades	Meses 2026	Responsable
Actividad 1: Plan anual de sensibilización	Diseño, aprobación y divulgación del plan.	Ene	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información / Profesional de Comunicación y Cultura
Actividad 2: Jornadas de sensibilización	Charlas, talleres, capacitaciones internas.	Feb – Nov	Secretaría General / Talento Humano/ Gestión del Talento Humano/ Profesional de Comunicación y Cultura
Actividad 3: Transferencia de conocimiento	Cursos externos, certificaciones, formación especializada.	Abr – Nov	Secretaría General / Talento Humano/ Gestión del Talento Humano/ Profesional de Comunicación y Cultura
Actividad 4: Medición del nivel de sensibilización	Aplicar encuestas, analizar resultados, plan de mejora.	Sep – Dic	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información / Profesional de Comunicación y Cultura
Actividad 5: Campañas permanentes	Boletines, afiches, mensajes de correo, piezas gráficas.	Ene – Dic	Subdirección Administrativa y Financiera

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

			Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información / Profesional de Comunicación y Cultura
--	--	--	--

4. Implementación de Controles (Enero – Diciembre 2026)

Control	Actividades	Meses 2026	Responsable
Control 1: Política de respaldos	Elaboración, aprobación y pruebas de respaldo.	Ene – Abr	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
Control 2: Gestión de Cambios	Diseño del procedimiento e implementación.	Feb – Jun	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información
Control 3: Clasificación de la información	Crear matriz y lineamientos de manejo.	Mar – Ago	Subdirección Administrativa y Financiera Equipo de Gobierno en Línea / Transformación Digital/ Apoyo Tecnológico y de Información / Dependencias
Control 4: Desarrollo Seguro	Definir lineamientos y aplicarlos.	Abr – Sep	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital / Proveedores
Control 5: WAF	Adquisición, configuración y despliegue.	May – Oct	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital
Control 6: Acceso lógico	Ajustes a perfiles, roles, autenticación, revisiones.	Ene – Dic	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital / Gestión del Talento Humano
Control 7: Hardening	Endurecimiento de servidores, endpoints y apps.	Feb – Nov	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital

5. Gestión de Incidentes (Enero – Diciembre 2026)

Proyecto	Actividades	Meses 2026	Responsable
Actividad 1: Procedimiento de Incidentes	Elaboración, revisión y publicación.	Ene – Mar	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital
Actividad 2: Capacitación	Formación en identificación y reporte.	Abr – Ago	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información

	PROCESO DE DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO: DIE-FO-014
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	VERSIÓN: 02

			Transformación Digital / Talento Humano
Actividad 3: Registro oficial de incidentes	Crear el repositorio y habilitar uso institucional.	Mar – Abr	Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital
Actividad 4: Simulacros de incidentes	Ejecución y reporte de lecciones aprendidas.	Sep – Nov	Subdirección Administrativa y Financiera / Equipo de Gobierno en Línea / Apoyo Tecnológico y de Información Transformación Digital / Todas las dependencias

11. ANÁLISIS PRESUPUESTAL

Con base en los proyectos definidos en el cronograma de actividades y en el presupuesto proyectado por la Entidad, se realizará la asignación de los recursos conforme a la disponibilidad presupuestal para la vigencia 2026. Este estimado corresponde a los requerimientos asociados a los proyectos establecidos, los cuales serán presentados a la Alta Dirección para su análisis, consideración y evaluación de viabilidad.

12. APROBACIÓN

El presente plan fue puesto a consideración y conocimiento de la Alta Dirección y del Comité de Gestión y Desempeño Institucional, y ha sido aprobado conforme a lo aquí establecido.