Nombre de la política / plan:	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Dependencia responsable:	Subdirección Administrativa y Financiera Área de apoyo tecnológico de la información
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 TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Entidad: Área Metropolitana De Bucaramanga-AMB

MARCO DE REFERENCIA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga (AMB) constituye un instrumento fundamental para garantizar la protección, continuidad y resiliencia de los activos de información que soportan los procesos estratégicos, misionales y de apoyo de la entidad. Este documento define las acciones, controles y medidas orientadas a mitigar, reducir, transferir o aceptar los riesgos identificados, en concordancia con el Modelo de Seguridad y Privacidad de la Información –MSPI– y el Sistema de Gestión de Seguridad de la Información (SGSI).

El plan se construye a partir de los resultados del proceso de identificación, análisis y evaluación de riesgos, en el cual fueron reconocidas las amenazas, vulnerabilidades y probabilidades de materialización que podrían afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional. Para ello, se aplicaron criterios de priorización basados en el impacto operativo, legal, reputacional, financiero y tecnológico, asegurando que los riesgos de mayor criticidad cuenten con un tratamiento oportuno y eficaz.

En cumplimiento del Documento CONPES 3995 de 2020, el Decreto 1078 de 2015 (Política de Gobierno Digital), la Resolución 500 de 2021 y su actualización (Anexo 1 de la Resolución 02277 de 2025), así como el Decreto 612 de 2018 para la actualización anual de los planes institucionales, este plan establece lineamientos orientados a fortalecer la capacidad del AMB para anticipar, responder y recuperarse ante eventos que puedan comprometer la seguridad de la información. Asimismo, adopta las buenas prácticas y estándares internacionales como ISO/IEC 27001, ISO 31000:2018, y los

lineamientos de administración del riesgo del Modelo Integrado de Planeación y Gestión (MIPG).

El AMB, como entidad pública comprometida con la modernización y la transformación digital del territorio, reconoce la necesidad de operar bajo una infraestructura tecnológica moderna, segura y resiliente. Por ello, este plan promueve la adopción de medidas orientadas a fortalecer la seguridad perimetral, garantizar la disponibilidad de la información mediante copias de seguridad periódicas, robustecer los controles técnicos y administrativos, y consolidar una cultura institucional de seguridad y privacidad, involucrando a servidores públicos, contratistas y terceros.

De esta manera, el Plan de Tratamiento de Riesgos se convierte en una herramienta operativa y estratégica, orientada a elevar el nivel de madurez del SGSI, fortalecer el control interno y garantizar que la gestión de la seguridad de la información esté alineada con los objetivos institucionales y con las exigencias del entorno digital actual.

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).

1.1. 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.
- Decreto 255 de 2022 – Ajustes normativos para garantizar el adecuado tratamiento y protección de datos personales.
- Constitución Política de Colombia, artículos 15, 20, 23 y 74 – Derechos a la intimidad, habeas data, acceso a la información, derecho de petición y publicidad de la información.

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 asociados:
  - Decreto 1081 de 2015
  - Decreto 2578 de 2012
  - Decreto 4124 de 2004
  - Decreto 1100 de 2014

Estos lineamientos regulan la gestión documental, preservación digital, administración de archivos electrónicos e integridad del expediente digital.

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 – Actualizan la Política de Gobierno Digital y sus componentes.
- Decreto 2106 de 2019 – Simplificación de trámites; exige seguridad, integridad y disponibilidad de expedientes electrónicos.
- Decreto 1083 de 2015 – Disposiciones sobre organización administrativa y Sistema de Control Interno, incluyendo gestión del riesgo.

1.4. Normatividad Específica sobre Seguridad y Privacidad de la Información

- Resolución 500 de 2021 – MinTIC – Establece lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Resolución 746 de 2022 – MinTIC – Ajusta y amplía los lineamientos del MSPI.
- Resolución 02277 de 2025 – MinTIC – Actualiza y moderniza el MSPI para entidades públicas, vigente para su implementación 2025–2026.
- Lineamientos MinTIC 2025 para Gestión de Incidentes de Seguridad Digital.
- Manual de Gobierno Digital – Módulo de Seguridad y Privacidad.

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.
- Decisión Andina 351 de 1993 – Régimen común de derechos de autor.
- Ley 527 de 1999 – Regula mensajes de datos, comercio electrónico y firmas digitales.

2. Relación con el Modelo Integrado de Planeación y Gestión – MIPG

La Seguridad y Privacidad de la Información se articula con varias dimensiones del MIPG, entre ellas:

2.1. Gestión del Conocimiento y la Información

Promueve la protección de la información como activo estratégico, garantizando integridad, disponibilidad, confidencialidad y uso ético.

2.2. Gestión del Riesgo

Identificación, análisis, valoración y tratamiento de los riesgos asociados a activos de información y seguridad digital.

2.3. Control Interno

Define responsabilidades, controles, verificaciones, auditorías y mecanismos para evaluar el cumplimiento del MSPI y el SGSD.

2.4. Gestión del Desempeño y Resultados

Vincula la seguridad de la información con la calidad del servicio, eficiencia institucional y cumplimiento de metas.

2.5. Arquitectura Institucional y Talento Humano

Define roles, competencias y responsabilidades para garantizar prácticas seguras y cultura de protección de datos.

3. Marcos, Estándares y Buenas Prácticas Internacionales

3.1. Estándares ISO

- ISO/IEC 27001:2022 – Requisitos del SGSI.
- ISO/IEC 27002:2022 – Controles de seguridad.
- ISO/IEC 27005 – Gestión del riesgo en seguridad de la información.
- ISO/IEC 22301 – Continuidad de 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 – Requisitos para identificación, protección, detección, respuesta y recuperación.

3.3. COBIT

Marco para gobierno y control de TI, complementario a la seguridad y planeación estratégica.

4. Lineamientos Técnicos del MinTIC para el MSPI

- Modelo de Seguridad y Privacidad de la Información (MSPI 2025).
- Manual de Gobierno Digital – Módulo de Seguridad y Privacidad.
- Lineamientos de Gestión de Incidentes de Seguridad Digital (2025).
- Estrategia de Seguridad Digital – MinTIC.
- Guía de gestión de riesgos, Ministerio de Tecnologías de la Información y las Comunicaciones.

1. OBJETIVO

Establecer las medidas, controles y actividades necesarias para gestionar y tratar los riesgos de seguridad y privacidad de la información identificados en el Área Metropolitana de Bucaramanga, reduciéndolos a niveles aceptables y garantizando la protección de los activos institucionales. Así mismo, asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información, fortalecer la continuidad y resiliencia de los servicios misionales, y asegurar el cumplimiento de la normatividad vigente y del Modelo de Seguridad y Privacidad de la Información.

2. OBJETIVOS ESPECÍFICOS

- Implementar los controles necesarios para mitigar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información administrada por el AMB.
- Definir responsables, recursos y plazos para asegurar la ejecución efectiva de cada medida de tratamiento establecida por el AMB
- Priorizar los riesgos identificados conforme a su nivel de criticidad e impacto sobre los procesos misionales, estratégicos y de apoyo del AMB.
- Establecer mecanismos de seguimiento y evaluación que permitan medir la eficacia de los controles implementados.
- Garantizar el cumplimiento de la normatividad interna y externa aplicable a la seguridad y privacidad de la información en el AMB.
- Fortalecer la cultura institucional del AMB en materia de gestión del riesgo, seguridad digital y mejora continua.
- Integrar las medidas de tratamiento de riesgos con los procesos de continuidad del negocio y gestión de incidentes del AMB.

3. GLOSARIO

Acceso a la Información Pública: Derecho fundamental que faculta a todas las personas a conocer y acceder a la información pública en posesión o bajo control de los sujetos obligados. (Ley 1712 de 2014, art. 4).

Activo: Cualquier información o elemento relacionado con su tratamiento (sistemas, soportes, infraestructura física, edificios, personas, procesos, etc.) que tiene valor para la entidad. (ISO/IEC 27000).

Activo Crítico de Información: Activo cuya afectación puede comprometer la continuidad operativa, la prestación del servicio, la seguridad institucional o el cumplimiento de funciones esenciales de la entidad.

Activos de Información y Recursos: Elementos de hardware, software, infraestructura, comunicaciones, bases de datos, procesos, procedimientos y personal involucrado en el manejo de la información misional, operativa y administrativa. (CONPES 3854 de 2016).

Administración del Riesgo: Conjunto de actividades coordinadas para identificar, analizar, valorar y gestionar los riesgos que puedan afectar el logro de los objetivos institucionales, siguiendo los lineamientos del MIPG y de la Guía de Administración del Riesgo del DAFP.

Amenaza: Causa potencial de un incidente no deseado que puede generar daño a un sistema, activo o proceso. (ISO/IEC 27000).

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

Archivo: Conjunto de documentos producidos o recibidos por una entidad en el ejercicio de sus funciones, conservados como testimonio e información. (Ley 594 de 2000, art. 3).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluar el cumplimiento de criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del titular para realizar el tratamiento de sus datos personales. (Ley 1581 de 2012, art. 3).

Bases de Datos Personales: Conjunto organizado de datos personales sometidos a tratamiento. (Ley 1581 de 2012, art. 3).

Ciberespacio: Ambiente físico y virtual compuesto por sistemas computacionales, software, redes de telecomunicaciones, datos e información utilizados para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciberseguridad: Protección de los activos de información frente a amenazas provenientes del ciberespacio mediante la implementación de controles y medidas de seguridad.

Control: Medida, política, procedimiento o práctica adoptada para modificar, reducir o mantener el riesgo dentro del nivel aceptable. También denominado salvaguarda o contramedida. (ISO/IEC 27000).

Control de Seguridad: Acciones, prácticas o herramientas diseñadas para mitigar riesgos de seguridad y privacidad. Pueden ser organizacionales, físicos o tecnológicos.

Datos Abiertos: Datos primarios o sin procesar, en formatos estándar e interoperables, puestos a disposición de cualquier ciudadano de manera libre y sin restricciones. (Ley 1712 de 2014, art. 6).

Datos Personales: Cualquier información asociada o que pueda asociarse a una persona natural identificada o identificable. (Ley 1581 de 2012, art. 3).

Datos Personales Mixtos: Información que contiene simultáneamente datos públicos junto con datos privados o sensibles.

Datos Personales Privados: Datos de naturaleza íntima o reservada que solo son relevantes para el titular. (Ley 1581 de 2012).

Datos Personales Públicos: Datos que no son privados, semiprivados ni sensibles, tales como estado civil, profesión u oficio o calidad de servidor público. (Decreto 1377 de 2013, art. 3).

Datos Personales Sensibles: Datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación. Incluye datos sobre origen étnico, orientación política, creencias religiosas, salud, vida sexual, datos biométricos, entre otros. (Decreto 1377 de 2013, art. 3).

Derecho a la Intimidad: Derecho fundamental que garantiza una esfera privada libre de injerencias del Estado o particulares, permitiendo el desarrollo personal y social. (Corte Constitucional).

Dominio de Seguridad: Conjunto de componentes del MSPI agrupados en categorías como gobierno de la seguridad, protección de activos, gestión del riesgo, gestión de incidentes, continuidad, cumplimiento y seguridad física.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que realiza tratamiento de datos personales por cuenta del responsable. (Ley 1581 de 2012).

Gestión de Incidentes de Seguridad de la Información: Procesos para detectar, reportar, analizar, responder, tratar y aprender de los incidentes de seguridad. (ISO/IEC 27000).

Gobierno de Seguridad de la Información: Estructura organizacional, políticas, roles y responsabilidades que permiten dirigir y controlar la seguridad y privacidad de la información en la entidad.

Indicadores de Seguridad: Medidas cuantitativas o cualitativas que permiten evaluar la efectividad de los controles, la madurez del SGSI y el comportamiento de los riesgos.
Información Pública Clasificada: Información cuyo acceso puede ser restringido debido a que pertenece al ámbito privado o semiprivado de una persona. (Ley 1712 de 2014, art. 6).

Información Pública Reservada: Información exceptuada de acceso público por el daño que podría causar a intereses públicos, cumpliendo requisitos legales. (Ley 1712 de 2014, art. 6).

Ley de Habeas Data: Hace referencia a la Ley 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Hace referencia a la Ley 1712 de 2014.

Matriz de Riesgos de Seguridad y Privacidad: Herramienta que consolida los activos, amenazas, vulnerabilidades, valoraciones y tratamientos asociados, alineada con el MSPI.
Mecanismos de Protección de Datos Personales: Acciones como accesos controlados, cifrado, seudonimización o anonimización para proteger los datos personales.

Mejora Continua: Proceso permanente para optimizar el desempeño institucional mediante acciones correctivas, preventivas y de innovación.

Modelado de Amenazas: Proceso de identificación estructurada de amenazas potenciales considerando el entorno digital, servicios, usuarios y tecnologías.

Nivel de Riesgo: Resultado del proceso de análisis y valoración del riesgo que combina probabilidad e impacto, clasificado por niveles (bajo, medio, alto, extremo).

Partes Interesadas (Stakeholders): Personas u organizaciones que pueden afectar o verse afectadas por una decisión o actividad.

Plan de Continuidad del Negocio: Conjunto de estrategias y acciones que permiten asegurar la continuidad de las funciones misionales ante eventos que puedan interrumpirlas. (ISO/IEC 27000).

Plan de Tratamiento de Riesgos: Documento que define las acciones y controles necesarios para gestionar los riesgos de seguridad de la información que superan el nivel aceptable. (ISO/IEC 27000).

Planeación Institucional: Proceso que orienta la definición de objetivos, metas, acciones y recursos de la entidad, integrando la gestión del riesgo y los controles.

Política de Seguridad y Privacidad de la Información: Documento de alto nivel que establece lineamientos, objetivos, roles y estructuras para gestionar la seguridad en la entidad.

Privacidad de la Información: Capacidad de proteger los datos personales y garantizar los derechos del titular durante su tratamiento.

Registro Nacional de Bases de Datos (RNBD): Directorio público administrado por la SIC que contiene las bases de datos sometidas a tratamiento en el país. (Ley 1581 de 2012, art. 25).

Responsabilidad Demostrada (Accountability): Obligación del responsable o encargado de demostrar ante la autoridad de control el cumplimiento de la normativa de protección de datos personales.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que decide sobre el tratamiento de los datos personales. (Ley 1581 de 2012).

Riesgo: Posibilidad de que una amenaza aproveche una vulnerabilidad para causar daño a un activo de información, combinando probabilidad y consecuencias. (ISO/IEC 27000).

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, independientemente del medio en que se encuentre. (ISO/IEC 27000).

Seguridad Digital: Protección de información que reside o se gestiona mediante medios digitales.

Seguridad Física: Conjunto de medidas para proteger instalaciones, equipos y personal contra accesos no autorizados, daños o interferencias que puedan afectar los activos de información.

Seguridad Técnica o Tecnológica: Herramientas, configuraciones y prácticas para proteger sistemas de información, redes, bases de datos y dispositivos frente a ataques o incidentes.

SGSI – Sistema de Gestión de Seguridad de la Información: Marco estructurado basado en ISO 27001 para gestionar seguridad de la información mediante políticas, procedimientos, controles y mejora continua.

Terceros con Acceso a la Información: Personas naturales o jurídicas ajenas a la entidad que, por contrato o relación funcional, tienen acceso a información institucional y deben cumplir las políticas de seguridad.

Titular de la Información: Persona natural cuyos datos personales son objeto de tratamiento. (Ley 1581 de 2012).

Tratamiento de Datos Personales: Cualquier operación realizada sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012).

Tratamiento del Riesgo de Seguridad de la Información: Acciones destinadas a mitigar, reducir, transferir o aceptar los riesgos identificados mediante controles definidos en el Plan de Tratamiento.

Trazabilidad: Capacidad de asociar de manera inequívoca todas las acciones realizadas sobre la información o los sistemas a un individuo o entidad. (ISO/IEC 27000).

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

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga – AMB abarca la gestión integral de los riesgos asociados a la seguridad de la información, seguridad digital y continuidad operativa, promoviendo la aplicación de buenas prácticas y estándares que permitan prevenir incidentes que afecten el logro de los objetivos institucionales.

Este plan aplica a:

- Todos los procesos estratégicos, misionales y de apoyo del AMB.
- Todos los activos de información definidos en el inventario institucional (físicos, digitales, infraestructura tecnológica, servicios, personas y terceros).
- Los riesgos identificados en la valoración del SGSI, incluyendo amenazas y vulnerabilidades que impacten la confidencialidad, integridad, disponibilidad y privacidad de la información.
- Todo el personal del AMB, incluidos funcionarios, contratistas y terceros que tengan acceso a activos de información.
- Los sistemas de información, aplicaciones, equipos tecnológicos, redes, servicios en la nube y demás medios utilizados para el procesamiento, almacenamiento o transmisión de datos.

Quedan excluidos aquellos riesgos que, por decisión de la alta dirección, sean aceptados formalmente bajo criterios documentados.

5. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

La gestión y tratamiento de los riesgos de seguridad y privacidad de la información requiere la participación, articulada y responsable de todos los niveles de la organización. A continuación, se definen los roles y responsabilidades de los actores involucrados en el proceso:

Alta Dirección

- Aprobar las políticas, lineamientos, estrategias y directrices relacionadas con la administración del riesgo de seguridad y privacidad de la información.
- Garantizar la asignación de recursos técnicos, financieros y humanos requeridos para la implementación del Plan de Tratamiento de Riesgos.
- Fomentar una cultura institucional orientada a la seguridad, la protección de datos y la gestión responsable de los activos de información.
- Supervisar el cumplimiento del marco normativo aplicable y garantizar la integración del tratamiento de riesgos con la planificación institucional, el SGSD y el MIPG.

Proceso de Administración del Sistema Integrado de Gestión (SIG)

- Diseñar, actualizar y difundir la metodología institucional de gestión de riesgos, de acuerdo con los lineamientos del MSPI y del MIPG.
- Liderar, coordinar y asesorar a las dependencias en la identificación, análisis, valoración y tratamiento de los riesgos de seguridad y privacidad de la información.
- Capacitar a los equipos de trabajo en la aplicación metodológica y en el uso de herramientas para la gestión de riesgos.
- Consolidar la matriz institucional de riesgos y hacer seguimiento a la implementación de los controles definidos.

Responsables de Procesos

- Identificar, analizar, valorar y evaluar los riesgos asociados a la seguridad y privacidad de la información dentro de su proceso, al menos una vez por vigencia o cuando exista un cambio relevante.
- Proponer e implementar medidas y controles de tratamiento alineados con el Plan de Seguridad y Privacidad de la Información.
- Verificar la eficacia de los controles implementados y reportar oportunamente cualquier cambio en los riesgos de su proceso.
- Documentar los riesgos y mantener actualizada la información en la matriz institucional.

Servidores Públicos y Contratistas

- Cumplir y aplicar los controles, medidas y buenas prácticas establecidos para la mitigación de riesgos de seguridad y privacidad de la información.
- Informar oportunamente la existencia de nuevos riesgos, debilidades, incidentes o situaciones que puedan afectar la seguridad digital de la entidad.
- Participar en actividades de sensibilización, capacitación y fortalecimiento de capacidades en seguridad y gestión del riesgo.
- Manejar la información institucional según los principios de confidencialidad, integridad, disponibilidad y privacidad.

Oficina o Ente de Control Interno (o quien haga sus veces)

- Evaluar el diseño, implementación y efectividad de la política, los procedimientos y los controles de la gestión de riesgos de seguridad y privacidad de la información.
- Realizar seguimiento independiente y formular recomendaciones de mejora al proceso de administración del riesgo.
- Emitir informes que permitan a la Alta Dirección tomar decisiones informadas sobre la mejora del SGSD, del MSPI y del Plan de Tratamiento de Riesgos.
- Verificar el cumplimiento normativo y el nivel de madurez del proceso de gestión de riesgos.

6. POLÍTICA DE ADMINISTRACION DE RIESGOS

El Área Metropolitana de Bucaramanga AMB, a través de su Modelo Integrado de Gestión, se compromete a fortalecer una cultura institucional orientada a la gestión integral del riesgo, que permita prevenir, mitigar y controlar los posibles eventos que puedan afectar el logro de los objetivos institucionales. Esta política busca consolidar medidas efectivas de prevención, monitoreo y seguimiento, aplicables a todas las actividades que desarrolla la entidad para diseñar, adoptar, ejecutar y promover políticas, planes, programas e iniciativas asociadas a la gestión pública y al uso estratégico de la información.
La presente política abarca los riesgos relacionados con la estrategia, la gestión institucional, la integridad pública, la seguridad y privacidad de la información, la seguridad digital, la continuidad de la operación, la protección ambiental y la seguridad y salud en el trabajo, garantizando que los recursos institucionales se utilicen de manera eficiente y que se brinde atención adecuada a los grupos de interés.

6.1. Objetivo de la Política

Establecer los parámetros y lineamientos necesarios para la adecuada gestión de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios en el AMB, procurando prevenir su materialización y minimizar sus impactos. Esta política se fundamenta en la *Guía para la Administración del Riesgo y el Diseño de Controles del DAFP*, promoviendo la toma de decisiones oportunas y la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, garantizando la continuidad operativa y el cumplimiento de las obligaciones institucionales.

6.2. Tratamiento del Riesgo

El tratamiento de los riesgos constituye la respuesta definida por la primera línea de defensa: los líderes o responsables de proceso, junto con sus equipos de trabajo. Su propósito es reducir la probabilidad o impacto de los riesgos identificados, mediante la implementación de acciones y controles definidos en el Plan de Tratamiento de Riesgos.

6.3. Alternativas de tratamiento del riesgo

1. Aceptar el riesgo

Consiste en no adoptar medidas adicionales que modifiquen la probabilidad o el impacto del riesgo.

- Aplica únicamente para riesgos clasificados como bajos o aquellos que no pueden ser intervenidos con controles razonables.
- No se aceptan riesgos asociados a integridad pública o corrupción.
- Requiere seguimiento continuo.

2. Reducir el riesgo

Implica implementar controles orientados a disminuir la probabilidad de ocurrencia, el impacto o ambos.

- Involucra medidas operativas, técnicas, administrativas o físicas.
- Debe garantizarse la segregación de funciones y la eficacia del control.

3. Evitar el riesgo

Consiste en eliminar las actividades o condiciones que generan el riesgo.

- Aplica cuando el nivel de riesgo es inaceptable y no puede mitigarse utilizando controles.
- Implica suspender, rediseñar o reemplazar la actividad generadora del riesgo.

4. Transferir o compartir el riesgo

Se reduce la probabilidad o impacto del riesgo mediante la transferencia o compartición de parte del riesgo.

- Se puede realizar a través de seguros, contratos o tercerización.
- Los riesgos de corrupción pueden compartirse, pero no puede transferirse su responsabilidad.

6.4. Enfoque General de la Gestión de Riesgos

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios permite al AMB identificar, analizar, valorar y tratar amenazas y vulnerabilidades que puedan afectar los activos de información y el cumplimiento de los objetivos institucionales. Este proceso:

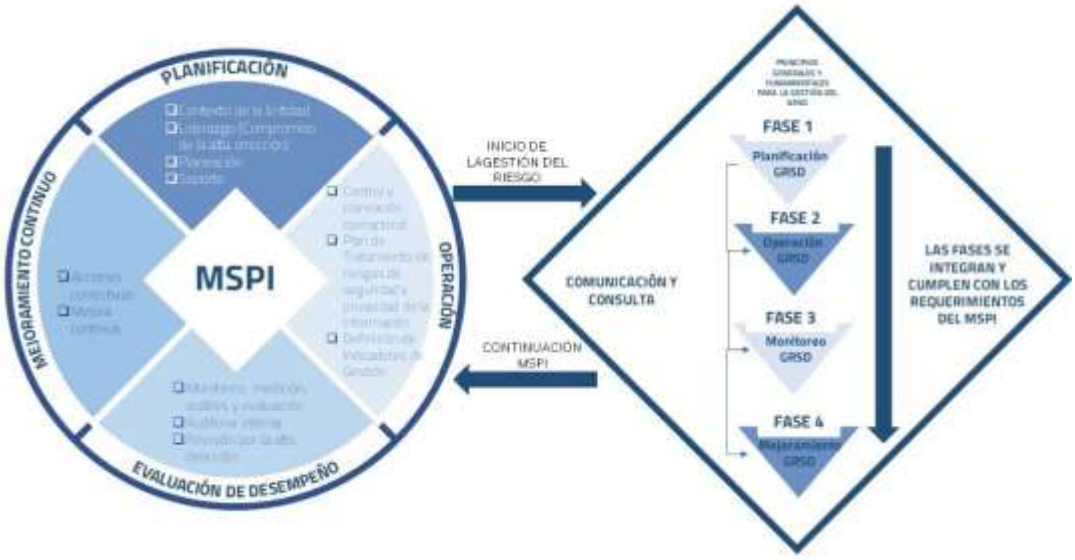
- Alinea la gestión de riesgos con los objetivos estratégicos, políticas y planes institucionales.
- Permite establecer prioridades, asignar recursos y tomar decisiones basadas en riesgo.
- Fortalece la resiliencia institucional y la capacidad de respuesta ante incidentes.
- Facilita mantener un nivel de riesgo aceptable para la entidad y la Alta Dirección.

7. METODOLOGIA

La metodología establecida para el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga (AMB) para la vigencia 2026 se fundamenta en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Gestión del Riesgo de Seguridad Digital (GRSD) y el ciclo de mejoramiento continuo PHVA (Planear – Hacer – Verificar – Actuar).

Su propósito es garantizar la definición, implementación, seguimiento y mejora de las acciones orientadas a mitigar riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional.

Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones[1]

8. DESARROLLO METODOLOGICO

La metodología adoptada por el Área Metropolitana de Bucaramanga (AMB) para el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información durante la vigencia 2026 se fundamenta en un enfoque integral que garantiza la protección de la confidencialidad, integridad y disponibilidad de la información institucional. Este enfoque articula los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), la Norma ISO 27001, el Modelo Integrado de Planeación y Gestión (MIPG) y la normativa aplicable en materia de gestión de riesgos.

[1] Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Ministerio de tecnologías de la información y las comunicaciones https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-401774_recurso_1.pdf

La metodología se estructura en cinco fases principales, representadas en la infografía institucional que guía el proceso de gestión del riesgo en el AMB que a continuación se describen:

1. Identificación de Riesgos
En esta fase se realiza el reconocimiento de los activos de información, procesos, recursos tecnológicos y ambientes operativos que pueden verse afectados por amenazas internas o externas.

Incluye la identificación de vulnerabilidades, escenarios de riesgo y posibles consecuencias que comprometan el logro de los objetivos institucionales. Este paso permite comprender el contexto organizacional y definir el alcance de la gestión del riesgo.

2. Análisis y Evaluación de Riesgos
Una vez identificados los riesgos, se procede a su valoración considerando la probabilidad de ocurrencia y el impacto potencial en los activos de información. Este análisis permite clasificarlos según su nivel de criticidad y priorizar aquellos que requieren intervención inmediata.

Los resultados son consolidados en la Matriz de Riesgos de Seguridad y Privacidad del AMB o que haga sus veces.

3. Definición de Estrategias de Tratamiento
Con base en los niveles de riesgo obtenidos, se establecen las acciones de tratamiento que incluyen controles preventivos, correctivos y detectivos.

La estrategia de tratamiento se orienta a mitigar, transferir, aceptar o eliminar el riesgo, dependiendo de su naturaleza y del criterio técnico adoptado por la alta dirección. Cada tratamiento cuenta con responsables, plazos y recursos asociados.

4. Implementación de Controles
En esta fase se ejecutan las acciones definidas en los planes de tratamiento. Incluye la adopción de controles administrativos, tecnológicos, físicos y procedimentales necesarios para reducir la exposición al riesgo.

Entre los controles implementados se encuentran: seguridad perimetral, actualización tecnológica, clasificación de la información, control de accesos, procedimientos de respaldo y fortalecimiento del entorno tecnológico institucional.

5. Seguimiento y Mejoramiento Continuo
La gestión del riesgo requiere un monitoreo constante para validar la eficacia de los controles implementados.

El AMB evalúa de manera periódica la evolución de los riesgos, los incidentes registrados y el nivel de cumplimiento de los planes de tratamiento.

Los resultados alimentan procesos de mejora continua y garantizan la actualización del SGSI conforme a cambios tecnológicos, normativos o institucionales.

8.1. Resultado esperado de la metodología
La aplicación disciplinada de estas cinco fases fortalece la postura de seguridad del Área Metropolitana de Bucaramanga (AMB), garantizando que los riesgos asociados al manejo de la información sean gestionados de manera proactiva, sistemática y alineada con los principios de buen gobierno y eficiencia administrativa.

El Plan de Tratamiento de Riesgos para 2026 permite asegurar que las decisiones adoptadas protejan los activos institucionales, minimicen la exposición a amenazas y contribuyan a la continuidad del negocio, salvaguardando la información pública bajo criterios de transparencia y seguridad.

9. CRONOGRAMA DE TRABAJO

Eje	Actividad	Producto esperado	Cronograma (2026)	Recursos asociados
Gestión de riesgos	**Actividad 1: Identificar, valorar y clasificar los riesgos**	Matriz de riesgos completa	**Enero – Abril 2026**	**Recurso humano:** Profesional experto en seguridad informática ISO 27001 para liderar análisis de riesgos. **Tecnológico (Infraestructura de red y equipos):** Equipos actualizados que permitan realizar identificación y registro confiable. **Recursos económicos** para contratación y herramientas de análisis.
Gestión de riesgos	**Actividad 2: Definir y ejecutar planes de tratamiento**	Planes de tratamiento definidos e implementados	**Abril – Diciembre 2026**	**Recurso humano:** Equipo con experticia para definir controles del SGSI. **Tecnológico – Seguridad perimetral:** Implementación de firewall, WAF, IPS/IDS y filtrado. **Tecnológico – Infraestructura de red:** Red segura para despliegue de controles. **Tecnológico – Renovación de equipos:** Equipos actualizados compatibles con medidas de seguridad. **Recursos económicos** para adquisición de hardware/software.
Gestión de riesgos	**Actividad 3: Actualizar inventario de activos**	Inventario consolidado de activos de información	**Marzo – Mayo 2026**	**Recurso humano:** Responsable del SGSI para la gestión de activos. **Tecnológico – Infraestructura de red:** Equipos y servidores que permitan identificar activos en operación. **Recursos económicos** para herramientas de inventario.
Gestión de riesgos	**Actividad 4: Monitoreo y revisión de riesgos**	Informes trimestrales (abril, julio, octubre, diciembre)	**Abril, Julio, Octubre, Diciembre 2026**	**Recurso humano:** Personal especializado que analice eventos, indicadores e incidentes. **Tecnológico – Seguridad perimetral:** Herramientas de monitoreo continuo contra amenazas. **Tecnológico – Infraestructura de red:** Soporte para trazabilidad y registros de auditoría. **Recursos económicos** para sostenimiento del SGSI

10. 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.