| | |
|---|---|
| Nombre de la política / plan: | PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |
| Dependencia responsable: | Subdirección Administrativa y Financiera<br>Área de apoyo tecnológico de la información |
| Fecha de aprobación de la política / plan: | 28 enero del 2025 |
| No. de acta del Comité Institucional de Gestión y Desempeño del AMB en que fue aprobada: | Acta numero 1 |
| Vigencia de la política / plan: | 2025 |
| Dimensión del MIPG a la que se asocia la política / plan: | Información y Comunicación |

# Plan 2025

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LAINFORMACIÓN.

SUBDIRECCÓN ADMINISTRATIVA Y FIANNCIERA
Apoyo Tecnológico y de Información

# Contenido

# INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

El Área Metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura, que sea competitiva en el nuevo mundo digital. Por ello La gestión de la seguridad de la información debe realizarse sistemáticamente por procesos completamente documentados y conocidos por toda la entidad.

Con base en lo dispuesto en el Documento CONPES 3995 de 2020, el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015), y la Resolución 500 de 2021, que reglamenta los lineamientos y estándares para la estrategia de seguridad digital y adopta el modelo de seguridad y privacidad de la información, se proponen acciones encaminadas a mitigar el impacto en la entidad frente a la materialización de riesgos previsibles. Estas acciones incluyen el diseño e implementación de estrategias para la identificación, análisis, control, evaluación y monitoreo continuo de los riesgos, con un enfoque basado en las buenas prácticas y estándares internacionales como ISO 27001 e ISO 31000:2018, así como en la guía de administración del riesgo establecida en el Modelo Integrado de Planeación y Gestión (MIPG). De esta manera, se priorizan soluciones como la implementación de medidas de seguridad perimetral, la realización periódica de copias de seguridad y el fomento de una cultura organizacional orientada a la seguridad, privacidad y gestión efectiva del riesgo.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Área Metropolitana de Bucaramanga AMB

# OBJETIVOS

## Objetivo General

Establecer un marco estratégico y operativo para la implementación de medidas efectivas que permitan gestionar los riesgos asociados a la seguridad y privacidad de la información, garantizando la protección de los activos informáticos y la continuidad de los servicios que se prestan al público, mitigando los impactos derivados de posibles amenazas, asegurando el cumplimiento de la normatividad vigente, promoviendo una cultura de seguridad en la entidad y fomentando la confianza de los ciudadanos en la gestión de la información, contribuyendo al logro de los objetivos institucionales y al fortalecimiento de la transparencia y la gobernanza digital.

## Objetivos Específicos

Definir y apropiar políticas de seguridad que permitan preservar la confidencialidad, disponibilidad y autenticidad de la información institucional.

Garantizar el cumplimiento de los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas aplicables a la seguridad y privacidad de la información.

Identificar, valorar y gestionar los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad operativa.

Promover y fortalecer el conocimiento interno relacionado con la gestión de riesgos asociados a la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación de los servicios.

# ALCANCE DEL PLAN

Implementar una gestión eficiente de riesgos en las áreas de seguridad y privacidad de la información, seguridad digital y continuidad operativa, asegurando la integración de buenas prácticas en los procesos de la entidad, permitiendo prevenir incidentes que puedan comprometer los objetivos institucionales.

# DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** 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 dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **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.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Ley de Habeas Data**: Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000) Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- **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 en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder**): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

**Alta Dirección:**

Aprueban las directrices para la administración del riesgo en la Entidad. La alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

**Proceso Administración del Sistema Integrado de Gestión:**

Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

**Responsables de los procesos:**

Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año.

**Servidores públicos y contratistas:**

Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

**Quien haga las veces de Control Interno:**

Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

# POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

En el área metropolitana de Bucaramanga, AMB adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo de la seguridad y privacidad de la información, y para ello todos los servidores de la entidad se comprometan a:

1. Gestión de recursos necesarios para implementación de nuevos esquemas para prevenir el riesgo de la seguridad y privacidad de la información en el AMB.

2. Dar a Conocer a todos los funcionarios del área metropolitana de Bucaramanga y hacer cumplir las normas internas y externas relacionadas con la administración de los riesgos.

3. Fortalecer dentro de la institución la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

4. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

5. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para alcanzar lo anteriormente expuesto, es fundamental que la entidad lleve a cabo las gestiones necesarias para asegurar la disponibilidad de los recursos humanos, presupuestales y tecnológicos requeridosque permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del mismo en la entidad y que tienen como propósito evitar la materialización del riesgo.

# ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

Las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: Actualizar los factores externos e internos del riesgo.

- Identificación: Actualizar la identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Actualizar la calificación y evaluación del riesgo inherente.
- Valoración: Actualizar la identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: evaluación integral de los riesgos.

## CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información de Ministerio Tic.

| ACTIVIDAD | TAREA A DESARROLLAR PARA EL PLAN | RESPONSABLE | FECHA INICIAL PLANIFICADA | FECHA FINAL PLANIFICADA |
|---|---|---|---|---|
| Identificar Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación | Identificar, analizar y evaluar los riesgos Seguridad y privacidad de la información | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MARZO 2025 | ABRIL 2025 |
| Realizar análisis de vulnerabilidades de seguridad a los activos de información a su infraestructura On Premise | Revisar inventario de activos de Información y determinar las vulnerabilidades | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MARZO 2025 | JUNIO 2025 |
| Implementar controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información | Elaborar y/o actualizar políticas según el modelo de Seguridad y Privacidad de la Información, el plan de tratamiento de riesgos | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MARZO 2025 | JULIO 2025 |
| Implementar políticas de seguridad a nivel de red perimetral | Implementar soluciones de seguridad perimetral que permitan mitigar las principales amenazas cibernéticas | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MAYO 2025 | AGOSTO 2025 |

| | | | | |
|---|---|---|---|---|
| Implementar políticas de copias de seguridad en red | Implementar soluciones tipo NAS o en la nube para salvaguardar la información | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MARZO 2025 | NOVIEMBRE 2025 |
| Socialización de controles de seguridad, privacidad de la información y gestión de riesgo | Socializar políticas y documentos | Secretaria General (Resolución N° 000020 del 31 de enero de 2023)<br><br>Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información | MARZO 2025 | DICIEMBRE 2025 |

## DOCUMENTOS DE REFERENCIA

- MPSI Modelo de Seguridad y Privacidad de la Información del Ministerio de TIC
- ISO 27001 Norma internacional emitida por la Organización Internacional de Normalización (ISO) sobre gestión de seguridad de la información.
- LEY 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

## MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital

## REQUISITOS TECNICOS

Norma técnica colombiana NTC ISO/IEC 27001 Sistemas de Gestión de la seguridad de la información.

Documento Maestro del Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones.

Guía de gestión de riesgos, Ministerio de Tecnologías de la Información y las Comunicaciones

# RECURSOS

## Humano

Se requiere la contratación de personal con experiencia acreditada en la implementación en seguridad informática – ISO 27001

## Tecnológico

Implementación de un esquema de seguridad perimetral para mitigar riesgos de ataques cibernéticos a la red de datos del AMB

Implementación de una infraestructura de red que permita salvaguardar la información generada por los funcionarios del AMB almacenada en dispositivos de escritorio, portátiles y servidores de datos

Renovación tecnológica de los equipos informáticos que actualmente presentan obsolescencia en Sistemas Operativos e infraestructura y herramientas ofimáticas.

Consecución de recursos económicos para la implementación de hardware, software y la contratación de recurso humano con experticia en seguridad informática, que permitan mantener una infraestructura con un bajo riesgo de pérdida de información y continuidad del negocio

Elaboró

Ing. Freddy Neil Varela Lemus.
Profesional Universitario
Subdirección Administrativa y Financiera