PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN / SEGURIDAD DIGITAL DE LA SECRETARÍA GENERAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C.

Bogotá, D.C. 30 de enero de 2026

Cra 8 No. 10-65
Código Postal 111711
Tel: +57 (601) 381 3000
www.secretariageneral.gov.co
Info: Línea 195

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

Contenido

Ilustraciones

Tablas

1. Introducción

Entendiendo que la seguridad de la información se ha convertido en un pilar fundamental para garantizar la continuidad de las organizaciones frente a las amenazas del ciberespacio, y considerando las múltiples vulnerabilidades, ciberataques y fugas de información que demuestran que ningún sistema es completamente inmune, definir un plan de tratamiento de riesgos de seguridad de la información no solo es una buena práctica, sino una necesidad estratégica para toda entidad gubernamental.

En este sentido, la Secretaría General de la Alcaldía Mayor de Bogotá presenta a la ciudadanía, usuarios y grupos de interés el Plan de Tratamiento de Riesgos de Seguridad de la Información/Seguridad Digital correspondiente a la vigencia 2026. Este plan forma parte de la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), también conocido como el Sistema de Gestión de Seguridad de la Información (SGSI).

El plan permitirá identificar, priorizar y mitigar las amenazas que podrían comprometer los activos críticos de la entidad. Este proceso, estructurado y orientado a la acción, no solo minimiza los impactos potenciales, sino que también optimiza los recursos al enfocar los esfuerzos en los riesgos más relevantes.

La implementación de un plan de tratamiento bien definido no solo protege la información y los sistemas de la entidad, sino que también refuerza la confianza de los clientes internos y externos, promueve el cumplimiento normativo y salvaguarda la reputación organizacional.

En este contexto, el tratamiento adecuado de los riesgos de seguridad de la información y seguridad digital se convierte en un componente esencial para garantizar la sostenibilidad y el éxito en el entorno actual.

2. Objetivos

2.1 Objetivo General

Fortalecer la gobernanza de seguridad de la información la información / seguridad digital en la Secretaría General de la Alcaldía Mayor de Bogotá, atendiendo las actividades definidas en el plan de tratamiento, con el fin de evitar la materialización de riesgos de seguridad asociados a la pérdida de confidencialidad, integridad y disponibilidad.

2.2 Objetivos específicos

- Apropiar el conocimiento de la gestión de riesgos de seguridad de la información / seguridad digital al interior de la entidad.

- Dar cumplimiento a la normatividad vigente y a las normas técnicas de seguridad de la información.

- Fortalecer los procesos de definición en el tratamiento de riesgos asociados al interior de la entidad.

3. Alcance

El Plan de Tratamiento de Riesgos de seguridad de la información / seguridad digital de la Secretaría General de la Alcaldía Mayor de Bogotá para la vigencia 2026 abarca todas las dependencias de la Entidad. Este plan contempla todos los riesgos que se encuentran en nivel residual moderado, alto y extremo, conforme con lo descrito en la metodología de riesgos de la entidad.

4. Política de Administración de Riesgos

La Política de Administración del Riesgo es la declaración del compromiso del equipo directivo de la Secretaría General de la Alcaldía Mayor de Bogotá D.C para gestionar de manera integral los riesgos que puedan afectar el cumplimiento de la misión, los objetivos estratégicos y la prestación del servicio público. Esta política orienta las acciones necesarias para anticipar, prevenir y mitigar riesgos, promoviendo la transparencia, la integridad y la mejora continua en todos los procesos y proyectos de inversión de la entidad."

Esta política aplica a todos los sistemas de gestión, procesos institucionales y proyectos de inversión de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., en el marco de la planeación estratégica y operativa. Incluye la gestión de riesgos que puedan afectar la integridad, la transparencia y la correcta administración pública, tales como riesgos de contratación, seguridad digital, defensa jurídica, ambientales, seguridad y salud en el trabajo, gestión, fiscales, corrupción, lavado de activos y financiación del terrorismo, integridad pública y riesgos asociados a proyectos de inversión.

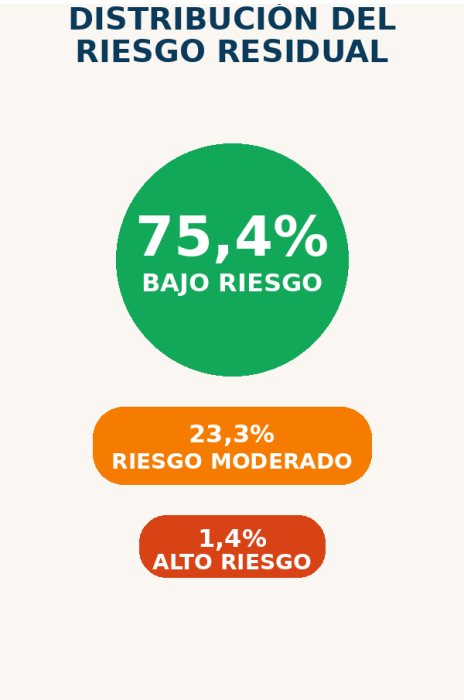
La Política de Administración del Riesgo se fundamenta en el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno y la normativa vigente en materia de gestión del riesgo. Su aplicación abarca todos los procesos institucionales, proyectos de inversión, servicios y trámites, así como las interacciones con terceros y grupos de valor. La entidad complementará esta política con lineamientos, procedimientos y herramientas específicas que aseguren una respuesta adecuada frente a riesgos que puedan comprometer la transparencia, la legalidad y el interés público.

La gestión del riesgo se desarrollará conforme a la metodología institucional definida en la Guía de administración y gestión de riesgos "4202000-GS-079".

Respecto a seguridad digital, a continuación, se detalla el consolidado actual del mapa de riesgos de seguridad de la información de la Secretaría General de la Alcaldía Mayor de Bogotá.

Tabla 1 Riesgos de seguridad de la información / seguridad digital

Fuente: Elaboración propia



Riesgos en nivel bajo - 389 riesgos (75,4 %) - Acepta

- No requieren acciones adicionales de tratamiento.
- Deben mantenerse bajo monitoreo periódico y control operacional.

Riesgos en nivel moderado - 120 riesgos (23,3 %) – Reducir el riesgo

Son el foco principal del Plan de Tratamiento 2025–2026.

Requieren:

- Acciones de mitigación adicionales o fortalecimiento de controles existentes.
- Priorización por impacto, dependencia y criticidad del activo.

- Seguimiento al indicador de cumplimiento definido

Riesgos en nivel alto - 7 riesgos (1,4 %) – Reducir el riesgo

- Requieren tratamiento obligatorio e inmediato.

- Se deben reportar al Comité Institucional de Gestión y Desempeño

Tabla 2 Riesgos en nivel residual alto

Proceso	Grupo de activo	Tipo de activo	Descripción del riesgo
Paz, víctimas y reconciliación	Correos electrónicos	Información / comunicación	Pérdida de confidencialidad e integridad de la información
Fortalecimiento de la gestión pública	Información electrónica / digital	Información	Pérdida de confidencialidad e integridad de la información
Fortalecimiento de la gestión pública	Información electrónica / digital	Información	Pérdida de disponibilidad de la información

Proceso	Grupo de activo	Tipo de activo	Descripción del riesgo
Gestión de servicios administrativos y tecnológicos	Información electrónica	Información	Pérdida de confidencialidad e integridad de la información
Gestión de contratación	Recurso humano	Personas	Pérdida de confidencialidad e integridad de la información
Gestión de contratación	Sistema de información – Sistema Contractual	Sistema de información	Pérdida de confidencialidad e integridad de la información
Gestión del talento humano	Recurso humano	Personas	Pérdida de confidencialidad e integridad de la información

Las acciones contempladas en el plan de tratamiento de riesgos son las siguientes:

Aceptar el riesgo: Riesgos en nivel bajo. No se debe realizar ninguna acción o actividad por parte de los responsables de los riesgos (primera línea de defensa). Sin embargo, es importante que se realice el respectivo seguimiento y monitoreo.

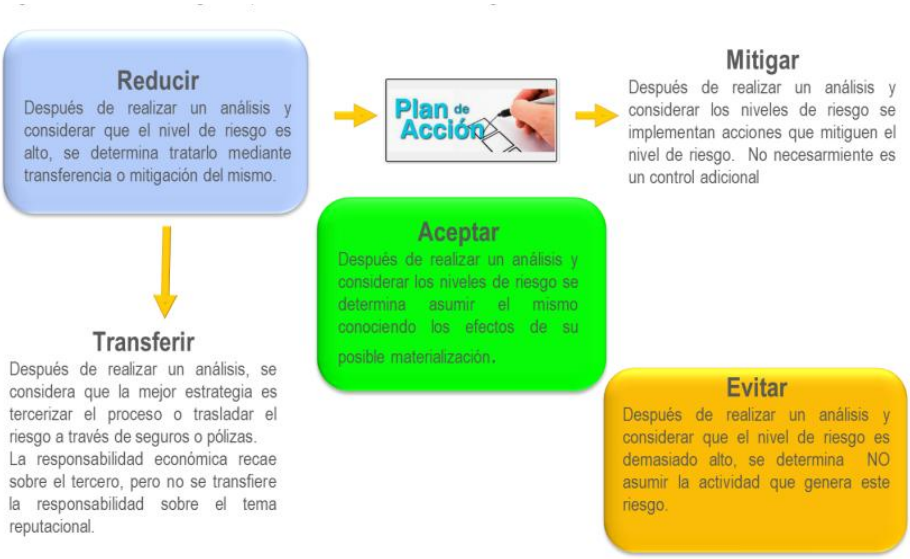
Reducir el riesgo (Mitigar): Riesgos en nivel moderado, alto o extremo. Se adoptan medidas adicionales a los controles implementados para cada uno de los activos de información, con el fin de reducir la probabilidad e impacto del riesgo.

Reducir el riesgo (Transferir): Riesgos en nivel moderado, alto o extremo. Se realiza la tercerización del riesgo / transferencia del riesgo a un tercero. (ej. Seguros), con el fin de reducir la probabilidad e impacto del riesgo.

Evitar el riesgo: NO se asumen las actividades que generan el riesgo.

Ilustración 1 Acciones de plan de tratamiento de riesgos

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6.



5. Plan de tratamiento de Riesgos de Seguridad de la Información / Seguridad digital

El plan de tratamiento de riesgos de seguridad de la información / seguridad digital es revisado y aprobado por cada uno de jefes de las dependencias de la Secretaría General de la Alcaldía Mayor de Bogotá y aprobado posteriormente por el Comité Institucional de Gestión y Desempeño.

Las actividades definidas en los planes de tratamiento se consolidan en las siguientes líneas estratégicas;

1. **Fortalecimiento de la cultura de seguridad**

- Charlas y capacitaciones recurrentes a funcionarios y contratistas.
- Inducción en seguridad para personal nuevo.
- Enfoque en confidencialidad, uso adecuado de la información y correos.

2. **Gestión de accesos a la información**
   - Definición y aplicación de controles de acceso lógico.
   - Principio de mínimo privilegio en información electrónica y sistemas.
3. **Protección de sistemas críticos**
   - Refuerzo de controles de acceso a sistemas contractuales y administrativos.
   - Coordinación directa con TIC.
4. **Control del factor humano**
   - Acciones específicas sobre recurso humano como activo crítico.
   - Sensibilización orientada a errores no intencionales.
5. **Gobernanza y responsabilidad**
   - Liderazgo explícito de jefes de proceso y Oficial de Seguridad.

Tabla 3 Cruce de actividades de plan de tratamiento / ISO 27001:2022

Línea estratégica	Actividades principales	Controles ISO 27001:2022 asociados
Cultura de seguridad	Charlas, capacitaciones, inducción	A.6.3 Concienciación y formación en seguridadA.5.1 Políticas de seguridad
Gestión de accesos	Controles de acceso a información	A.5.15 Control de accesosA.5.18 Gestión de identidades
Protección de sistemas	Accesos a sistemas contractuales	A.5.17 Información de autenticaciónA.8.9 Gestión de configuraciones

Línea estratégica	Actividades principales	Controles ISO 27001:2022 asociados
Factor humano	Sensibilización al recurso humano	A.6.1 Selección y verificaciónA.6.2 Términos y condiciones laborales
Gobernanza	Responsables y seguimiento	A.5.2 Roles y responsabilidadesA.5.3 Segregación de funciones

6. Marco Normativo

A continuación, se detalla el marco normativo sobre el cual se basó el desarrollo del presente plan se nombra a continuación:

- **Constitución Política de Colombia de 1991**: Artículo 15,20
- **Ley 1273 de 2009**: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1581 de 2012**. Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014**. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 886 de 2014**. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015**. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1008 del 2018**. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 338 de 2022**: Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.

- **Decreto 472 de 2024:** Por el cual se adopta el Modelo de Gobernanza de Seguridad Digital para el Distrito, se modifica el artículo 5 del Decreto Distrital 025 de 2021 y se dictan otras disposiciones.
- **Resolución 777 de 2019.** Por la cual se adopta la Política de Privacidad y Tratamiento de Datos Personales y el "Manual de Políticas y Procedimientos para el Tratamiento de Datos Personales" de la Secretaría General de la Alcaldía Mayor de Bogotá, D. C., y se deroga la Resolución 070 de 2017.
- **Resolución 500 de 2021:** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- **Resolución No. 485 de 2024**: Por la cual se actualiza la reglamentación del Comité Institucional de Gestión y Desempeño en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C. y se sustituyen unos Capítulos del Título II de la Resolución 728 de 2023 “Por la cual se unifica y actualiza la reglamentación de las instancias internas de coordinación en la Secretaría General de la Alcaldía Mayor de Bogotá, D.C."
- **Resolución 2277 de 2025**. Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

- **Resolución 373 de 2025** Por la cual se adopta la Política de Seguridad de la Información y Seguridad Digital y la Estrategia de Seguridad Digital de la Secretaría General de la Alcaldía Mayor de Bogotá, D.C

- **CONPES 3701 de 2011**: Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016**: Política Nacional de Seguridad digital.
- **Conpes 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial
- **Conpes 3995 de 2020:** política Nacional de Seguridad y Confianza Digital

7. Aprobaciones y Control de Cambios

- **Política de Gobierno Digital** - Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC.
- **Manual Operativo del Modelo Integrado de Planeación y Gestión.**
- Norma Técnica Colombiana ISO 27001:2022.

8. Aprobaciones y Control de Cambios

8.1 Aprobaciones

El presente documento fue creado, revisado, modificado y aprobado por:

	NOMBRE	CARGO	FECHA
ELABORÓ	Lourdes María Acuña Acuña	Contratista	Enero/2026
REVISÓ	Erika Tatiana Quintero Quintero	Contratista	Enero/2026
	Arleth Patricia Saurith Contreras	Jefe Oficina de Tecnologías de la Información y las Comunicaciones – OTIC	Enero/2026
APROBÓ	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	Enero/2026

8.2 Control de Cambios

ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	FECHA DEL CAMBIO	VERSIÓN
N/A	Creación del documento	09/01/2025	1.0
Vigencia y actividades del plan	Actualización por vigencia 2026	Enero/2026	2.0