



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

2025



SECRETARÍA DE
SEGURIDAD, CONVIVENCIA
Y JUSTICIA



TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS.....	4
2.1. Objetivo General	4
2.2. Objetivos Específicos.....	4
3. ALCANCE	4
4. GLOSARIO.....	5
5. MARCO NORMATIVO.....	5
6. JUSTIFICACIÓN.....	5
7. RESULTADOS ACTUALES.....	6
7.1. Levantamiento Activos de Información.	6
7.2. Riesgos de Seguridad de la Información.	7
8. ACTIVIDADES A DESARROLLAR.....	8

1. INTRODUCCIÓN

En cumplimiento de la Política de Administración de Riesgos PO-FI-02 de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, se actualiza el presente plan con el objetivo de establecer acciones que permitan identificar, analizar, controlar y mitigar los riesgos de seguridad de la información, protegiendo así los activos de información de la Entidad y garantizando el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales.

En este contexto, la gestión de riesgos de seguridad de la información es una actividad continua mediante el cual se identifican, evalúan y minimizan los riesgos, lo que implica identificar los peligros y amenazas potenciales, y tomar las medidas preventivas y correctivas necesarias para eliminar o reducir las probabilidades de su materialización.

Por lo tanto, se define el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025, alineado con las necesidades de la Entidad y el cumplimiento de la normativa aplicable. Este plan da continuidad a las acciones de mejora continua, a partir de la identificación de los riesgos inherentes relacionados con la integridad, confidencialidad y disponibilidad de la información.

2. OBJETIVOS

2.1. Objetivo General

Ejecutar las actividades descritas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, conforme a lo establecido en la Política de Administración de Riesgos de la Entidad, con el fin de adoptar medidas y acciones efectivas para reducir y mitigar los riesgos relacionados con la seguridad de la información.

2.2. Objetivos Específicos

- a. Implementar las acciones definidas en el plan para la gestión de riesgos de seguridad de la información en la Entidad, cumpliendo con la normativa vigente y promoviendo su apropiación a todos los niveles.
- b. Actualizar y revisar los activos de información conforme a las Tablas de Retención Documental, las necesidades de la Entidad y la normativa aplicable a cada proceso.
- c. Realizar el seguimiento a los controles establecidos para la mitigación de los riesgos de seguridad de la información, asegurando su efectividad y cumplimiento continuo.

3. ALCANCE

El presente Plan de Tratamiento de Riesgos establece los criterios y buenas prácticas en Seguridad y Privacidad de la Información, con el objetivo de prevenir y mitigar los incidentes de seguridad que puedan afectar el logro de los objetivos institucionales de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

Este documento se basa en lo definido en la Política de Administración de Riesgos PO-FI-02, a través de la cual se delinearán las actividades necesarias para la identificación y/o actualización de activos de información, evaluación de riesgos inherentes, valoración de riesgos, y la identificación y evaluación de controles.

4. GLOSARIO.

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta a la definición de términos establecidos en el Ítem 6 “Glosario” del MA-GT-01 “Manual de Seguridad y Privacidad de la información” aprobado para la Entidad.

5. MARCO NORMATIVO.

El Plan de Tratamiento de Riesgo de Seguridad y Privacidad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta al Ítem 4 “Normatividad Asociada” establecido en el MA-GT-01 “Manual de Seguridad y Privacidad de la información” aprobado para la Entidad.

6. JUSTIFICACIÓN.

La Política de Gobierno Digital, definida por el Gobierno Nacional, promueve la transformación digital en el sector público, reconociendo que la Administración Pública y diversos actores de la sociedad, como los ciudadanos, las empresas privadas y otros entes externos, son fundamentales para el desarrollo integral del Gobierno Digital en Colombia. Las necesidades y desafíos de las entidades determinan el uso y aprovechamiento de las TIC, contribuyendo a la generación de valor público y al bienestar de la sociedad.

La transformación digital implica la incorporación de tecnologías en las operaciones de las entidades, lo que genera nuevas fuentes de información y, a su vez, riesgos de seguridad de la información. Estos riesgos deben ser identificados, analizados y gestionados de manera efectiva para garantizar la protección adecuada.

En cumplimiento con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Política de Administración del Riesgo de la Entidad, es necesario actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025. Este plan define las acciones necesarias para gestionar los riesgos de seguridad de la información, garantizando la protección de los principios de integridad, confidencialidad y disponibilidad.

7. RESULTADOS ACTUALES.

De acuerdo con las actividades realizadas para la actualización de los activos de información y la evaluación de los riesgos de seguridad de la información, conforme a lo establecido en la Política de Administración de Riesgos de la Entidad para la vigencia 2024, se obtuvieron los siguientes resultados:

7.1. Levantamiento Activos de Información.

Para la vigencia 2024, se llevaron a cabo mesas de trabajo con la participación de la Dirección de Recursos Físicos y Gestión Documental, la Dirección de Tecnologías y Sistemas de la Información, y representantes de todas las áreas que conforman los 21 procesos de la Entidad (Estratégicos, Misionales, de Evaluación y de Apoyo). Durante estas sesiones, se proporcionaron instrucciones sobre el formato F-GD-1081 - Registro de Activos de Información e Índice de Información Clasificada y Reservada, con el fin de actualizar los activos de acuerdo con la normativa vigente y la guía interna de levantamiento de activos de la organización.

En el proceso de actualización, se consideraron los cambios realizados en la reestructuración del mapa de procesos, que incluyó la eliminación y/o creación de nuevos procesos dentro de la Entidad. Estos ajustes impactaron directamente en los activos de información, especialmente en la documentación que respalda las operaciones, lo que requirió modificaciones en su contenido y codificación.

La matriz de activos resultante fue publicada en el portal de Datos Abiertos Bogotá, en el sitio web de la Entidad, y se informó a los líderes de área a través de memorando interno, así:

Enlace de consulta de los documentos:

Memorando interno: 3-2024-43558

Sitio Web de Datos Abiertos Bogotá:

<https://datosabiertos.bogota.gov.co/dataset/https-scj-gov-co-es-transparencia-datos-abiertosregistros-activos-informacion>.

Sitio Web de la Secretaría Distrital de Seguridad, Convivencia y Justicia:

<https://scj.gov.co/es/transparencia/datos-abiertos/registros-activos-informacion>

7.2. Riesgos de Seguridad de la Información.

Durante la vigencia 2024, se realizó el seguimiento al estado de los controles de tratamiento de riesgos de seguridad de la información, lo cual implicó la recopilación y validación cuatrimestral de evidencias relacionadas con la ejecución de dichos controles. Asimismo, se generaron los informes correspondientes, en cumplimiento con lo establecido en la Política de Administración de Riesgos de la Entidad.

Para abordar las oportunidades de mejora, se llevaron a cabo mesas de trabajo con las diversas áreas de la Entidad, con el objetivo de ajustar los controles y las evidencias, basados en las recomendaciones de la Oficina de Control Interno, tras la entrega del informe de tratamiento de riesgos de seguridad de la información por parte de la Dirección de Tecnologías y Sistemas de la Información (DTSI). Estas mesas de trabajo fueron clave en la revisión exhaustiva de las recomendaciones y la aplicación de los ajustes necesarios a los controles.

La matriz de riesgos de seguridad de la información identificados para la vigencia 2024, se encuentra publicada en la página Web de la Secretaría Distrital de Seguridad Convivencia y Justicia en el siguiente enlace:

<https://scj.gov.co/es/transparencia/planeacion-presupuesto-ingresos/plan-accion>

8. ACTIVIDADES A DESARROLLAR.

El Plan establecido está diseñado para cumplir con las actividades relacionadas con la gestión de Seguridad de la Información y la Política de Administración de Riesgos de la Entidad.

A continuación, se detallan las actividades a realizar, el tiempo de ejecución de estas, los responsables y los participantes para la implementación de este plan:

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN	META	INDICADOR	TIPO INDICADOR
1	Actualización Activos de Información.	Realizar mesas de trabajo para la actualización de activos de información de acuerdo con los requerimientos y/o normatividad vigente.	Dirección de recursos físicos y gestión documental / Dirección de Tecnologías y Sistemas de la Información	01/02/2025	31/12/2025	Activos de Información actualizados.	Activos de información actualizados	Eficacia
2	Socialización y Divulgación sobre gestión de riesgos de seguridad de la información.	Socializar y divulgar lo relacionado con la gestión de riesgos de seguridad de la información.	Dirección de Tecnologías y Sistemas de la Información	01/02/2025	31/12/2025	Actividades de divulgación y socialización realizadas.	(Número de actividades socialización y divulgación realizadas / número de actividades socialización y divulgación planeadas) *100	Eficacia
3	Seguimiento a la ejecución de los controles	Realizar seguimiento cuatrimestral a los controles establecidos	Dirección de Tecnologías y	01/02/2025	31/12/2025	Seguimiento al cumplimiento de	(Número de seguimientos al cumplimiento de los	

	establecidos para los riesgos de seguridad de la información.	en la matriz de riesgos de seguridad de la información, revisando y consolidando la información remitida por las dependencias de la Entidad sobre la gestión de riesgos, y elaborar el informe de resultados sobre la efectividad de los controles implementados.	Sistemas de la Información			los controles ejecutados.	controles / Número de seguimientos al cumplimiento de los controles ejecutados) *100	
4	Revisión y ajuste de controles	Revisión y consolidación y Ajuste controles según recomendaciones de la Oficina de Control Interno de la Entidad.	Dirección de Tecnologías y Sistemas de la Información	01/02/2025	31/12/2025	Ajuste de Controles de acuerdo con las recomendaciones establecidas en los informes de gestión.	(Número de controles ajustados / Número de recomendaciones establecidas) * 100	Eficacia
5	Actualización del Plan 2026.	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026.	Dirección de Tecnologías y Sistemas de la Información	01/10/2025	31/12/2025	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información actualizado	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información actualizado.	Eficacia

Elaboró: Diego Mauricio Usme González – Contratista SDSCJ.

Revisó: Diana Camila Méndez Restrepo – Contratista SDSCJ.

Armando Alfonso Leyton Gonzalez – Contratista SDSCJ.

Jorge Eliecer Velásquez Perilla – Contratista SDSCJ.

Rafael Humberto López Saavedra – Contratista SDSCJ.

Zuleima Astrith Mancera Silva – Contratista SDSCJ.

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - <https://portalmipg.scj.gov.co>