

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

2022

Secretaría Distrital de Seguridad,
Convivencia y Justicia



SECRETARÍA DE
SEGURIDAD, CONVIVENCIA
Y JUSTICIA





	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 2 de 12

TABLA DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS.....	4
2.1. Objetivo General	4
2.2. Objetivos Específicos	4
3. ALCANCE	5
4. CONCEPTOS TECNICOS.....	5
5. MARCO NORMATIVO.....	6
6. JUSTIFICACIÓN.....	8
7. ACTIVIDADES A DESARROLLAR	9
8. CONTROL DE CAMBIOS.....	12

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 3 de 12


1. INTRODUCCIÓN

La materialización de los riesgos de seguridad de la información afecta el cumplimiento adecuado, efectivo y óptimo de los objetivos institucionales y en este sentido, los activos de información deben alinearse a la Política de Administración del Riesgo de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, cumpliendo las actividades de identificar, analizar, controlar y mitigar los riesgos de seguridad de la información que podrían afectar de manera negativa el logro de los objetivos institucionales.

Bajo esa perspectiva, la gestión de riesgos de seguridad de información se presenta como una herramienta para el desarrollo, implementación y mejora continua de la Entidad frente a la prestación de servicio y manejo de la información, tanto física como digital.

Es así como, internacionalmente la norma ISO (Organización Internacional de Normalización) 31000:2018 establece un Sistema de Gestión de Riesgos de cualquier tipo, incluyendo riesgos asociados a la información, esto permite reducir las falencias propias de la información a través de un tratamiento continuo y apropiado de los controles que mitiguen las afectaciones negativas a la organización.

En virtud de lo expuesto, se define el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2022, de acuerdo con las necesidades de la Entidad y al cumplimiento normativo aplicable, dando continuidad a los procesos de mejora continua a partir de la identificación de riesgos inherentes asociados con la integridad, confidencialidad y disponibilidad de la información.

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 4 de 12


2. OBJETIVOS

2.1. Objetivo General

Desarrollar e implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información acorde con los lineamientos definidos en la Política de Administración de Riesgos de la Entidad, con el propósito de adoptar medidas y acciones encaminadas a reducir y/o eliminar riesgos de Seguridad de Información mediante la definición, valoración y aplicación de controles.

2.2. Objetivos Específicos

- a. Revisar y actualizar los activos de información de acuerdo con las Tablas de Retención Documental y la normatividad vigente aplicable a cada uno de los procesos de la Entidad.
- b. Gestionar los riesgos de Seguridad y Privacidad de la información de acuerdo a lo definido en la Política de Administración del Riesgo de la Entidad.
- c. Fortalecer y apropiar el conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información.
- d. Definir un cronograma de actividades que permita la administración y gestión de los riesgos de la Entidad a nivel de Seguridad de la Información.

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 5 de 12


3. ALCANCE

El Plan de Tratamiento de Riesgos aquí propuesto, establece los criterios de gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos de la Secretaría Distrital de Seguridad, Convivencia y Justicia, buenas prácticas que contribuyen a prevenir y/o mitigar los incidentes que afectan el logro de los objetivos.

El presente documento aplica lo definido en la Política de Administración de Riesgos PO-DS-1 versión 7, para desarrollar las actividades de Identificación y/o actualización de activos de la información, de riesgos Inherentes, Valoración de riesgos, Identificación y evaluación de controles, así como la efectividad de la aplicación de los mismos.

4. CONCEPTOS TECNICOS


- a. **ACTIVO:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- b. **AMENAZAS:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.
- c. **ANÁLISIS DEL RIESGO:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).
- d. **CAUSA:** Factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- e. **CONSECUENCIA:** Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- f. **CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.
- g. **CONTROL:** Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- h. **DISPONIBILIDAD:** Propiedad de ser accesible y utilizable a demanda por la entidad.

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 6 de 12


- i. **GESTIÓN DEL RIESGO:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- j. **IMPACTO:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
- k. **INTEGRIDAD:** Propiedad de exactitud y completitud.
- l. **LÍNEA ESTRATÉGICA:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.
- m. **MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo.
- n. **POLÍTICA DE ADMINISTRACIÓN DEL RIESGO:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.
- o. **PROBABILIDAD:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.
- p. **RIESGOS DE SEGURIDAD DIGITAL:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.
- q. **RIESGO INHERENTE:** Riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- r. **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- s. **TRATAMIENTO AL RIESGO:** Respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.
- t. **VULNERABILIDAD:** Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

5. MARCO NORMATIVO

El Plan de Tratamientos de Seguridad y Privacidad de la Información, considera entre otros el siguiente marco normativo:

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 7 de 12

- a. Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- b. 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”*.
- c. 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”*.
- d. Decreto 1008 de 14 de junio de 2018, *“Por el cual se establecen los lineamientos generales de la política de Gobierno Digital”*.
- e. Resolución 500 de marzo 10 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”*.
- f. Resolución 0025 de 29 de enero del 2021, *“Por medio de la cual se adopta la Política de Seguridad y Privacidad de la Información” en la Secretaría Distrital de Seguridad, Convivencia y Justicia.*
- g. NTC-ISO/IEC 27001:2013, *Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI)*
- h. NTC-ISO/IEC 27002:2015, *“Proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, la implementación y la gestión de controles, teniendo en cuenta el(los) entorno(s)”*.
- i. NTC-ISO/IEC 31000:2018, *“es un estándar de origen internacional que ha sido desarrollado por ISO, y que proporciona los principios y directrices para la Gestión de Riesgos”*.
- j. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información del 06 de noviembre del 2016 del Ministerio de Tecnologías de las Información y las Comunicaciones – MinTIC.
- k. Guía N° 7 de Gestión de Riesgos del 01 de abril del 2016 del Ministerio de Tecnologías de las Información y las Comunicaciones – MinTIC.

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 8 de 12

6. JUSTIFICACIÓN


El Gobierno Nacional plantea la Política de Gobierno Digital¹, con la cual se genera un nuevo enfoque, en donde no sólo la Administración Pública sino también los diferentes actores de la sociedad tales como el ciudadano, la empresa privada, entes externos, etc., son elementos fundamentales para un desarrollo integral del Gobierno Digital en Colombia y en donde las necesidades y problemáticas de las entidades, determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público y aporte a la sociedad.

La transformación digital del estado colombiano es una fuente de generación y uso de información, originando riesgos que deben ser identificados, analizados y gestionados de manera efectiva. El Gobierno Nacional plantea el “Modelo Integrado de Planeación y Gestión “– MIPG², el cual da directrices de como las entidades deben manejar la administración y gestión de riesgos.

De acuerdo a lo requerido por el Artículo 1 del Decreto 612 del 2018 expedido por el Gobierno Nacional, la Política de Administración del Riesgo de la Entidad y las directrices dadas por el Ministerio de Tecnologías de las Comunicaciones – MinTIC, se hace necesario actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2022, en el que se definen las acciones para gestionar los riesgos de seguridad de la información salvaguardando los principios de integridad, confidencialidad y disponibilidad.

¹ Ministerio de Tecnología y Comunicaciones – MINTIC. Política de Gobierno Digital. Bogotá. 2018. En: <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/75180:La-nueva-politica-de-Gobierno-Digital-promueve-la-proactividad-y-la-innovacion-ciudadana#:~:text=El%20Ministerio%20de%20Tecnolog%C3%ADas%20de,para%20consolidar%20un%20Estado%20y>

² Función Pública. Modelo integrado de Planeación y Gestión. Bogotá, 2019. <https://www.funcionpublica.gov.co/web/mipg>


	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 9 de 12

7. ACTIVIDADES A DESARROLLAR


El Plan definido da cumplimiento a las actividades asociadas a la gestión del Sistema de Gestión de Seguridad de la Información y la Política de Administración de Riesgos” – PO-DS-1.

El detalle de las actividades a realizar, tiempo de ejecución de estas, responsable y participantes, para adelantar la implementación de este plan se definen a continuación.


N°	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA FIN
1	Actualizar de lineamientos de riesgos Seguridad y Privacidad de la información	Actualizar la Política de Administración del Riesgo en lo referente a seguridad de la información	Dirección de Tecnologías y Sistemas de la Información Oficina Asesora de Planeación	1/02/2022	15/02/2022
2	Revisar y actualizar los activos de información acorde con las Tablas de Retención Documental	Revisar y actualizar los activos de información existentes	Dirección de Tecnologías y Sistemas de la Información Dirección de Recursos Físicos y Gestión Documental Lideres de los procesos	1/02/2022	15/03/2022
		Presentar los activos de información a la Mesa Técnica de Seguridad Digital para aprobación	Dirección de Tecnologías y Sistemas de la Información Mesa Técnica Seguridad Digital	16/03/2022	23/03/2022
		Publicar los activos de información existentes	Dirección de Recursos Físicos y Gestión Documental Dirección de Tecnologías y Sistemas de la Información	24/03/2022	31/03/2022

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 10 de 12

N°	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA FIN
3	Identificar, analizar, valorar y evaluar los Riesgos de Seguridad y Privacidad de la información	Socializar Política de Administración del Riesgo en lo referente a seguridad de la información	Dirección de Tecnologías y Sistemas de la Información	1/04/2022	16/06/2022
		Identificar, analizar y evaluar los riesgos de Seguridad y Privacidad de la información	Dirección de Tecnologías y Sistemas de la Información Líderes de los procesos	1/04/2022	16/06/2022
4	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamientos.	Dirección de Tecnologías y Sistemas de la Información Líderes de los procesos Oficina Asesora de Planeación	16/06/2022	23/06/2022
5	Publicación	Publicación de matriz de riesgos	Dirección de Tecnologías y Sistemas de la Información Oficina Asesora de Planeación	24/06/2022	30/06/2022
6	Seguimiento fase de tratamiento	Seguimiento estados planes de tratamiento de riesgos identificados y verificación de evidencias	Dirección de Tecnologías y Sistemas de la Información	1/07/2022	31/12/2022
7	Monitoreo y revisión	Generación, presentación y reporte de indicadores	Dirección de Tecnologías y Sistemas de la Información	1/07/2022	31/12/2022
8	Evaluación de riesgos residuales	Evaluar los riesgos residuales	Dirección de Tecnologías y Sistemas de la Información	1/09/2022	31/12/2022

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. Secretaría Distrital de Seguridad, Convivencia y Justicia</p>	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 11 de 12

N°	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA FIN
9	Mejoramiento	Identificar oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Dirección de Tecnologías y Sistemas de la Información	15/09/2022	31/12/2022
10	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2023	Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Dirección de Tecnologías y Sistemas de la Información	1/10/2022	15/01/2023

	Proceso:	Gestión de Tecnología de Información	Código:	PL-GT-3
			Versión:	6
	Documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha Aprobación:	24/01/2020
			Fecha de Vigencia: 31/01/2022	Página 12 de 12

8. CONTROL DE CAMBIOS

Fecha	Versión	Descripción
23/07/2018	1	Creación del Documento
13/03/2020	2	Se ajustan logos de la Alcaldía y de la Certificación ISO 9001-2015 Calidad
31/08/2020	3	Se ajusta y actualiza el documento
21/10/2020	4	Por solicitud de la Dirección de Tecnologías y Sistemas de la Información, se ajusta nuevamente y actualiza el documento.
08/07/2021	5	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2021, aprobado en la sesión del 08 de julio del 2021 de la Mesa Técnica de Seguridad Digital.
26/01/2022	6	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022.

La información de elaboración, revisión y aprobación de este documento podrá ser consultada en el sistema "Portal MIPG" <https://portalmipg.scj.gov.co/>