PERSONERÍA
DE BOGOTÁ, D. C.

PLAN DE TRATAMIENTO DE RIESGOS DEL SGSI
2024
03 – PL – 09

Dirección de Tecnologías de la Información y las Comunicaciones - DTIC

Versión – 04
25 – 01 – 2024

CONTROL DE CAMBIOS		
VERSIÒN	**FECHA**	**DESCRIPCIÒN DE LA MODIFICACIÓN**
1	29/01/2021	Versión inicial del documento
2	20/01/2022	Versión actualizada del documento
3	12/12/2022	Actualización de la valoración de los riesgos por proceso y cronograma.
4	25/01/2024	Actualización general del documento 2024

Elaboró:	Revisó:	Aprobó:
Edgar Martín Cubides Rojas Director de Tecnologías de la Información y las Comunicaciones – DTIC	**Alexandra Ramírez Suárez** Directora Oficina de Planeación	Comité Institucional de Gestión y Desempeño

TABLA DE CONTENIDO

1. INTRODUCCION

El plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la Entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer las situaciones que pueden comprometer el cumplimiento de los objetivos trazados del entorno TIC.

La Personería de Bogotá, D.C., como Entidad de carácter público y de servicio al ciudadano está permanentemente intercambiando todo tipo de información con entidades públicas y privadas, así como con la ciudadanía en general. La información que se recibe de entidades y personas es el insumo principal para el desarrollo de sus funciones y con base en ella se toman decisiones y se ejecutan acciones que pueden derivar en la generación de comunicados, resoluciones, oficios etc. Esta información puede ser de carácter público para conocimiento de la ciudadanía en general o puede tratarse de investigaciones de alta confidencialidad dentro del desarrollo de sus procesos misionales. Por lo anterior, es de suma importancia identificar claramente el tipo de información que se está procesando para determinar los riesgos a los que está expuesta con el fin de protegerla debidamente.

Para la toma de decisiones y prestar servicios a las personas y funcionarios(as) de la Entidad, es necesario que la información sea real, oportuna y de acceso a quienes lo requieren, para ello la información debe contar con altos estándares de calidad, en materia de políticas y gestión de seguridad de la información.

Internacionalmente la norma ISO 31000 ayuda a establecer 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 posibles afectaciones a la Entidad.

De igual manera el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, establece metas, resultados y entregables correspondientes a cada una de las fases de implementación del SGSI en sus fases de Planificación e Implementación, las cuales deben ser tenidas en cuenta.

Basado en la norma ISO31000 y el Modelo de Seguridad y Privacidad de la Información – MSPI, de la Política de Gobierno Digital de MINTIC, la Personería

de Bogotá, D. C. establece el plan de trabajo para el año 2024 mediante el cual se adelantarán las actividades correspondientes para identificar, valorar y gestionar los riesgos de seguridad de la información en la entidad.

2. DEFINICIONES

Activo: Cualquier elemento que tenga valor para la organización.

Reducir/Mitigar: El riesgo se trata mediante la transferencia o la implementación de acciones que mitiguen su nivel. No necesariamente es un control adicional.

Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.

Causa: Elemento específico que origina el evento.

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).

Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.

Criterios de riesgos: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.

Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.

Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la Entidad (materializar el riesgo).

3. OBJETIVO

Identificar, clasificar y valorar los riesgos de seguridad de la información para cada uno de los procesos de la Entidad y establecer las acciones para la mitigar la probabilidad de materialización de los riesgos, alienados a la guía para la administración del riesgo del DAFP, la política de gobierno digital y la norma ISO 27001 vigente.

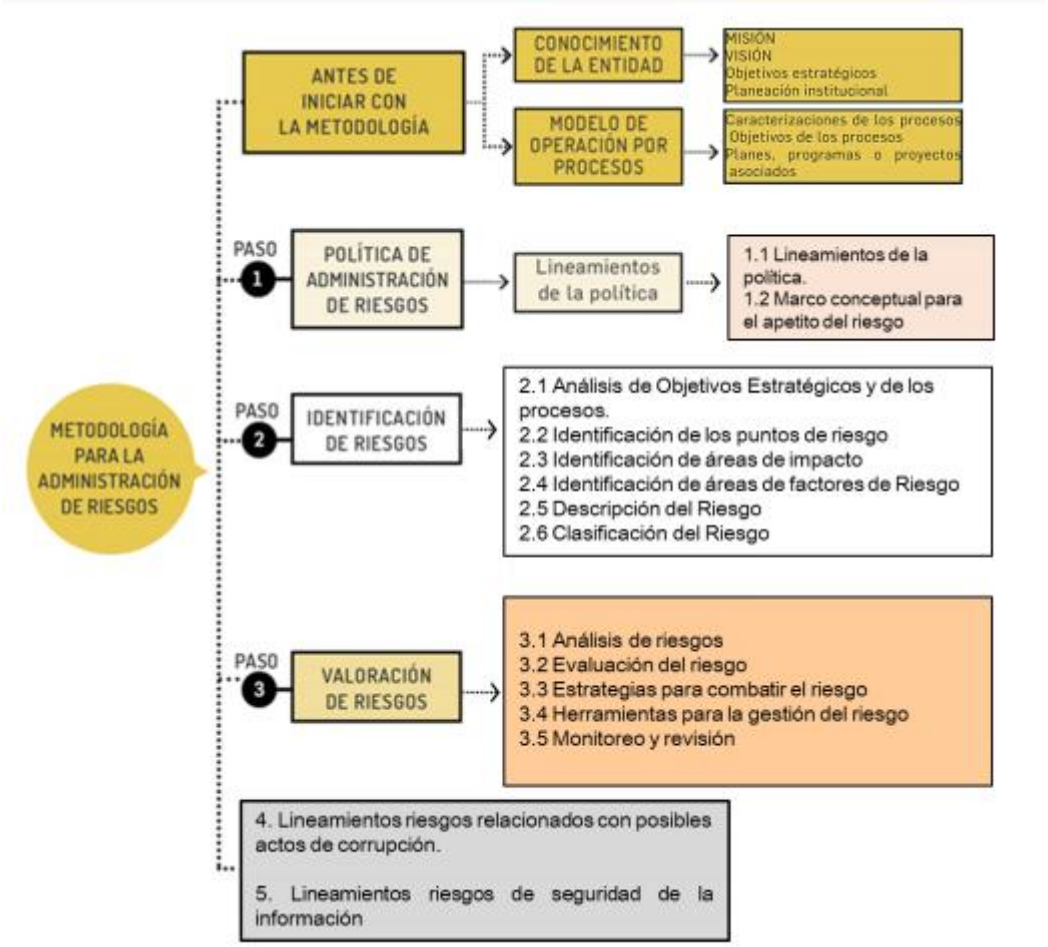
4. ALCANCE

Este documento, proporciona el plan de trabajo para desarrollar la administración y gestión de los riesgos de seguridad de la información a nivel de los procesos en la Entidad, desde la identificación de los riesgos de seguridad de la información hasta la definición del plan de tratamiento, responsables y fechas de implementación.

5. MARCO DE REFERENCIA

La Personería de Bogotá, utiliza como marco de referencia la guía para la administración de los riesgos v 6 del DAFP, con el objetivo de mantener una cultura de la gestión del riesgo que permita fortalecer las medidas de prevención, monitoreo y seguimiento al control para mitigar la posible materialización de los riesgos.

En la Gráfica 1 se presenta el modelo de gestión de riesgos de seguridad de la información para su adecuada administración:



Gráfica 1

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la Entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo:

1. Política de administración de riesgos
2. Identificación del riesgo
3. Valoración del riesgo

Finalmente, se desarrolla la definición e implantación de estrategias de comunicación transversales a toda la Entidad para que su efectividad pueda ser evidenciada.

6. RESPONSABLES

El responsable de implementar, mantener, aplicar y mejorar las actividades necesarias para el cumplimiento de los requisitos del Sistema de Gestión de la Seguridad de la Información (SGSI) es el director de Tecnologías de la Información las Comunicaciones de acuerdo con lo establecido en la Resolución 250 en su artículo 22 del 2023.

Así mismo, el sistema establece los roles y responsabilidades de las partes interesadas que intervienen en la gestión, identificación, valorización y control de los riesgos.

Los responsables de identificar los riesgos, establecer acciones y/o controles para mitigar los riesgos identificados son:

1. Equipo de SGSI
2. Analista de los riesgos de seguridad de la información
3. Referentes del SGSI

Igualmente son los encargados de actualizar los mapas de riesgos y generar los informes de gestión y ejecución, de acuerdo con los lineamientos establecidos en la Entidad.

Conforme a lo anteriormente mencionado el líder de cada proceso, es quien realiza la aprobación de los riesgos de seguridad de la información.

7. METODOLOGÍA

La metodología de gestión de riesgos, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que: el concepto de riesgo, así como el contexto, se planean mediante la programación de acciones y controles que permiten reducir la afectación a la Entidad en caso de materialización. Adicional, busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer las situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el entorno de las TIC.

En la Personería de Bogotá, D.C, mediante la gestión de la seguridad de la información se busca establecer y mantener programas, controles, acciones y políticas para conservar la confidencialidad, integridad y disponibilidad de la información sobre los requerimientos que registran los (as) ciudadanos(as) ante la

Personería de Bogotá D.C., toda vez que la misión de la Entidad es promover la efectividad integral de los derechos de las personas, trabajar al servicio de la Ciudad, intervenir y actuar como garante del respeto del ordenamiento jurídico por parte de las autoridades públicas del Distrito Capital, y vigila la conducta de los (as) servidores(as) públicos(as).
La Personería de Bogotá D.C., implementa el Sistema de Gestión de Seguridad de la Información - SGSI y establece su alcance para todos los procesos, clasificados en procesos estratégicos, procesos misionales, procesos de apoyo y procesos de evaluación, seguimiento y control.

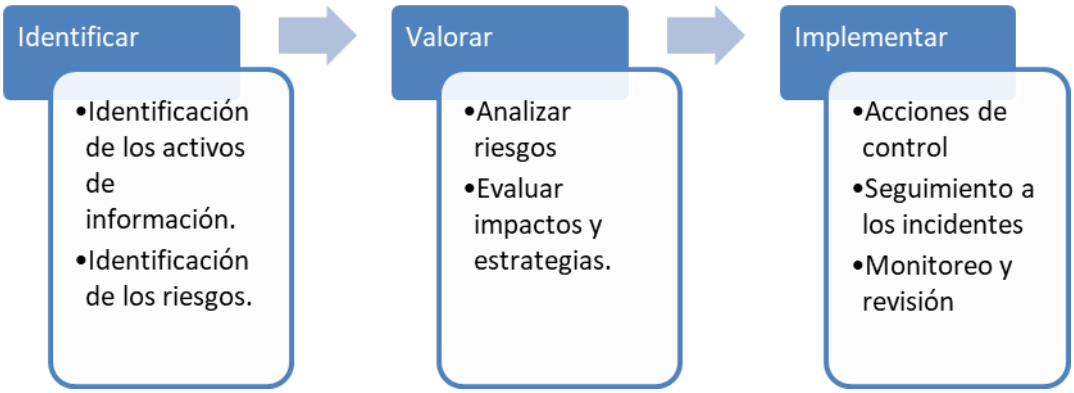
7.1. DESCRIPCIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

A continuación, se relaciona el plan de actividades que se deben desarrollar:

	ACCIÓN	ACTIVIDAD	RESPONSABLE
Gestión de Riesgos 2024	**Actualización de lineamientos**	Actualizar políticas y metodología de gestión de Riesgos	Analista de los riesgos de seguridad de la información
	Sensibilización	Socialización guías y herramientas gestión de riesgos del SGSI y continuidad de la operación	Analista de los riesgos de seguridad de la información
	Identificación de riesgos	Análisis de objetivos estratégicos y de los procesos	Referentes del SGSI
	Valoración de riesgos	Identificación de los puntos de riesgo.	Referentes del SGSI
		Identificación de áreas de impacto	Analista de los riesgos de seguridad de la información
		Identificación de áreas de factores de riesgo	Referentes del SGSI y Equipo de SGSI
		Descripción del riesgo	Analista de los riesgos de seguridad de la información
		Clasificación del riesgo	Referentes del SGSI y Analista de los riesgos de seguridad de la información
		Análisis de riesgos	Analista de los riesgos de seguridad de la información
	Aceptación de Riesgos identificados	Evaluación del riesgo	Analista de los riesgos de seguridad de la información

		Estrategias para combatir el riesgo	Analista de los riesgos de seguridad de la información
		Herramientas para la gestión del riesgo	Analista de los riesgos de seguridad de la información
		Monitoreo y revisión	Equipo de SGSI
		Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de SGSI
	Publicación	Publicación matriz de Riesgos de los procesos	Equipo de SGSI
	Seguimiento y fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación evidencias	Equipo de SGSI
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Analista de los riesgos de seguridad de la información
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Analista de los riesgos de seguridad de la información
	Monitoreo y Revisión	Actualizar políticas y metodología de gestión de riesgos de acuerdo a los cambios solicitados	Analista de los riesgos de seguridad de la información
		Generación, presentación y reporte de indicadores	Analista de los riesgos de seguridad de la información

7.2. PROCESO



7.3. MATERIALIZACIÓN DE UN RIESGO

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de reporte de incidentes de seguridad y privacidad de la información.

El equipo de seguridad analiza el riesgo y valida en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que el incidente esté relacionado con un riesgo que no estaba identificado en la matriz general de riesgos, este deberá ser incluido para que se inicie su correspondiente identificación, valoración y elaboración de plan de acción para la mitigación de la probabilidad de que vuelva a ocurrir.

8. NORMATIVIDAD APLICABLE

TIPO DE NORMA	NÚMERO	AÑO	EMISOR	ARTÍCULOS (APLICACIÓN)
Ley	1266	2008	Congreso de la República	Toda la norma
Ley	1581	2012	Congreso de la República	Toda la norma
Decreto	1263	2022	Ministerio de Tecnologías de la Información y las Comunicaciones	Artículos 2.2.23.1.4, 2.2.23.1.5
Decreto	767	2022	Ministerio de Tecnologías de la Información y las Comunicaciones	Artículos 2.2.9.1.1.1,2.2.9.1.1.2,2.2.9.1.1.3, 2.2.9.1.2.1,2.2.9.1.3.2,2.2.9.1.3.3, 2.2.9.1.3.4,2.2.9.1.3.5,2.2.9.1.4.1
Decreto	1008	2018	Ministerio de Tecnologías de la Información y las Comunicaciones	Toda la norma
Norma técnica ISO/IEC	27001	2013	ISO	Toda la norma
Norma técnica ISO/IEC	27032	2012	ISO	Toda la norma

9. CRONOGRAMA

	ACCIÓN	ACTIVIDAD	RESPONSABLE	FECHA
Gestión de Riesgos 2024	**Actualización de lineamientos**	Actualizar políticas y metodología de gestión de Riesgos	Analista de los riesgos de seguridad de la información	Enero y Febrero
	Sensibilización	Socialización guías y herramientas gestión de riesgos del SGSI y continuidad de la operación	Analista de los riesgos de seguridad de la información	Febrero y Marzo
	Identificación de riesgos	Análisis de objetivos estratégicos y de los procesos	Referentes del SGSI	Febrero Marzo
	Valoración de riesgos	Identificación de los puntos de riesgo.	Referentes del SGSI	Marzo y Abril
		Identificación de áreas de impacto	Analista de los riesgos de seguridad de la información	Marzo y Abril
		Identificación de áreas de factores de riesgo	Referentes del SGSI y Equipo de SGSI	Marzo y Abril
		Descripción del riesgo	Analista de los riesgos de seguridad de la información	Marzo y Abril
		Clasificación del riesgo	Referentes del SGSI y Analista de los riesgos de seguridad de la información	Marzo y Abril
		Análisis de riesgos	Analista de los riesgos de seguridad de la información	Marzo y Abril
		Evaluación del riesgo	Analista de los riesgos de seguridad de la información	Marzo y Abril
	Aceptación de Riesgos identificados	Estrategias para combatir el riesgo	Analista de los riesgos de seguridad de la información	Marzo y Abril
		Herramientas para la gestión del riesgo	Analista de los riesgos de seguridad de la información	Marzo y Abril
		Monitoreo y revisión	Equipo de SGSI	Marzo y Abril
		Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de SGSI	Mayo

	Publicación	Publicación matriz de Riesgos de los procesos	Equipo de SGSI	Mayo
	Seguimiento y fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación evidencias	Equipo de SGSI	Junio a Diciembre
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Analista de los riesgos de seguridad de la información	Junio a Diciembre Octubre
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Analista de los riesgos de seguridad de la información	Noviembre
	Monitoreo y Revisión	Actualizar políticas y metodología de gestión de riesgos de acuerdo a los cambios solicitados	Analista de los riesgos de seguridad de la información	Diciembre
		Generación, presentación y reporte de indicadores	Analista de los riesgos de seguridad de la información	Mayo a Diciembre