Plan de Tratamiento de Riesgos de Seguridad de la Información

Código SG/MIPG	127-PPPGI-12
Vigencia desde	31/01/2025
Versión	01

Proceso Gestión de la Tecnología y la Información

ALCALDÍA MAYOR DE BOGOTÁ D.C.
DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO
BOGOTÁ

Tabla de Contenido

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad de la Información 2025 se enmarca dentro de la estrategia de la entidad para fortalecer la cultura de seguridad, gestionando riesgos asociados a la información crítica y alineando controles con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la normativa vigente.

Este plan establece medidas para mitigar, transferir o aceptar los riesgos, asegurando la integridad, disponibilidad y confidencialidad de la información en el DADEP.

2. Elementos Estratégicos

3. Misión

3.1 Contribuir al mejoramiento de la calidad de vida en Bogotá, por medio de una eficaz defensa del espacio público, de una óptima administración del patrimonio inmobiliario de la ciudad y de la construcción de una nueva cultura del espacio público, que garantice su uso y disfrute colectivo y estimule la participación comunitaria.

4. Visión

En 2030, la entidad será líder en la gestión integral del Espacio Público a nivel distrital, contribuyendo a que la ciudadanía disfrute de espacios públicos seguros e inclusivos. Además, seremos referentes en la gestión del patrimonio inmobiliario distrital, la generación de conocimiento urbanístico, la creación de alianzas estratégicas y el fomento de la participación y cultura ciudadana.

5. Objetivos Estratégicos 2025 – 2030

- ✓ Fomentar la aplicación de los diversos instrumentos de administración del patrimonio inmobiliario distrital y del espacio público, incluyendo proyectos de bienestar de y para la comunidad.
- ✓ Aumentar la oferta cualitativa y cuantitativa de espacio público inclusivo y seguro, con enfoque de género, poblacional, étnico y diferencial.

- ✓ Liderar la gobernanza del espacio público en la ciudad a través de la coordinación interinstitucional e intersectorial de acuerdo con las competencias de las entidades públicas.
- ✓ Fortalecer la capacidad institucional en el marco de un Modelo Integrado de Planeación y Gestión eficiente, que propenda por una gestión pública inteligente, transparente y ágil en la respuesta a los requerimientos de la ciudadanía, promoviendo la participación y el control social.

6. Generalidades del Plan

6.1 Diagnóstico

Este proceso comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Durante el mes de noviembre de 2024, la Oficina de Tecnologías de la Información y las Comunicaciones llevó a cabo la actualización del Plan de Tratamiento de Riesgos de Seguridad de la Información, cuyo registro está disponible para consulta interna en la entidad. Adicionalmente, se tiene programado realizar el diagnóstico del MSPI en marzo de 2025, con el fin de actualizar la identificación de riesgos y definir nuevos controles según sea necesario.

Los resultados del análisis realizado con datos recopilados durante 2024 se pueden observar en las siguientes tablas.

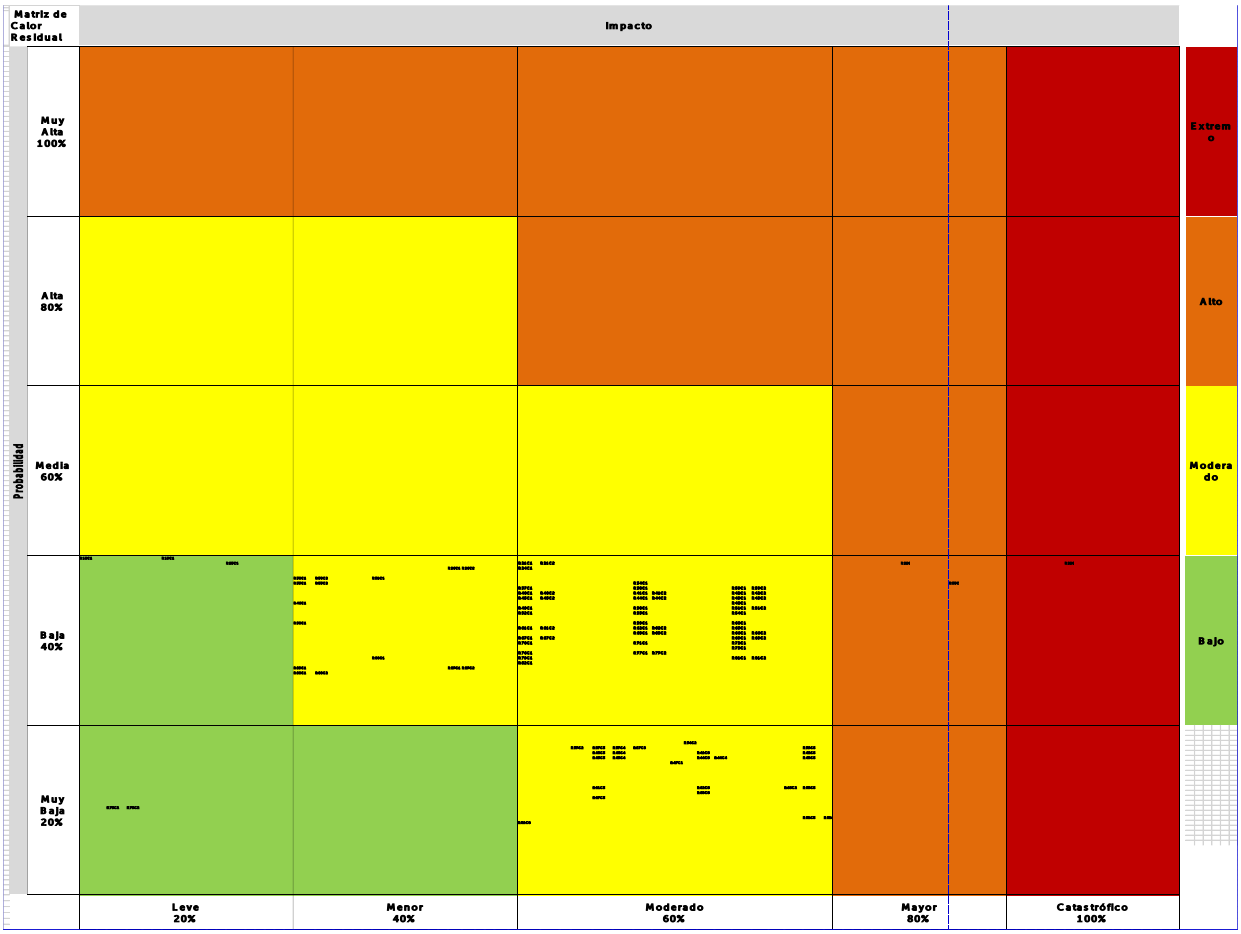
Tabla 1. Análisis de riesgo puro – DADEP – noviembre de 2024

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Rara vez (1)					
Improbable (2)					
Posible (3)				R3- Hurto de la información	
Probable (4)	R6- Equipo de			R5- Integridad	R1- Información

	cómputo R8- Accesibilidad			R7- Interrupción	R2- Fuga de Información R4- Disponibilidad R9- Ciberseguridad R10-Sistema de Incendio
Casi Seguro (5)					

Una vez valorados los riesgos identificados al a fecha de corte, se procedió a establecer los controles correspondientes para determinar los riesgos residuales.

Tabla 2. Análisis de riesgo residual – DADEP – noviembre 2024



6.2 Formulación

En la formulación del plan de tratamiento de riesgos de seguridad de la información participaron el jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, el gerente de proyectos y el personal técnico de apoyo para el MSPI.

6.3 Objetivo general

Presentar el Plan de Tratamiento para los riesgos de seguridad de la información, identificados en los procesos del DADEP.

6.4 Objetivos específicos

- Identificar los riesgos asociados a los procesos y los activos de información que hacen parte del alcance del MSPI.
- Evaluar y analizar el nivel de riesgo.
- Establecer el plan de tratamiento de riesgos.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos.

6.5 Alcance del Plan

Aplica a todos los niveles del Ministerio/Fondo de las TIC, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

6.6 Recursos

ECONÓMICO: los recursos financieros para la implementación del presente plan se determinaron en el presupuesto anual asignado para el profesional que desarrollará las actividades.
HUMANO: la Oficina de Sistemas, los líderes de proceso, Oficina de Control Interno y un profesional de apoyo con experiencia en seguridad informática.
FÍSICO: infraestructura tecnológica y controles de acceso físico.

6.7 Metodología de seguimiento y publicación

El seguimiento y monitoreo a la ejecución de las actividades, se realizará trimestralmente en cabeza del apoyo técnico para MSPI, a través de reuniones de validación de los riesgos en donde se determinará:

1. Estado de los riesgos (latente, cerrado, materializado)
2. Seguimiento a las actividades preventivas (realización y efectividad)
3. Identificación de nuevos riesgos
4. Revaloración de los riesgos latentes
5. Revisión y ajustes a actividades preventivas
6. Validación del presupuesto asignado

7. Actividades del Plan 2025

Riesgo	Descripción del Control	Meta	Producto
Identificar y documentar los riesgos críticos en los sistemas de información.	Identificación y análisis de riesgos en sistemas críticos.	Riesgos documentados y priorizados	Matriz de riesgos actualizada.
Evaluar y mitigar los riesgos de ciberseguridad en los servicios de nube pública/privada utilizados.	Realizar una evaluación de riesgos de seguridad en los servicios de nube pública y privada.	Identificar y priorizar los riesgos de ciberseguridad en los entornos de nube y definir acciones de mitigación.	Informe de evaluación de riesgos de seguridad digital en servicios de nube con recomendaciones de mitigación.
Evaluar riesgos de ciberseguridad en infraestructuras.	Realizar evaluación de riesgos de seguridad digital.	Identificar riesgos y medidas para mitigarlos.	Informe de evaluación de riesgos.
Identificar y tratar riesgos en los proyectos de TI para fortalecer la seguridad de los sistemas.	Identificación y tratamiento de riesgos en proyectos de TI.	Riesgos evaluados y tratados.	Documento de riesgos evaluados y tratados.
Evaluar riesgos de ciberseguridad en servicios en la nube.	Realizar evaluación de seguridad de servicios en la nube.	Identificar riesgos en servicios en la nube y mitigarlos.	Informe de riesgos en servicios en la nube.
Evaluar riesgos de seguridad en activos de información.	Realizar evaluación de riesgos en activos de información.	Identificar riesgos y medidas de mitigación.	Informe de evaluación de riesgos de activos.
Validar y mitigar riesgos críticos.	• Evaluación de riesgos de TI • Análisis de Vulnerabilidades	Riesgos evaluados y mitigados.	• Matriz de riesgos • Reporte de vulnerabilidades.

8. Riesgos asociados al Plan

Tabla 3. Identificación de los riesgos del plan y el respectivo plan de respuesta

Área de Riesgo	Riesgo	Valoración final del riesgo final del riesgo (impacto * probabilidad	Estrategia	Actividades
Otros	Identificar y documentar los riesgos críticos en los sistemas de información.	Riesgos documentados y priorizados	Transferir	Identificación y análisis de riesgos en sistemas críticos.
Otros	Evaluar y mitigar los riesgos de ciberseguridad en los servicios de nube pública/privada utilizados.	Identificar y priorizar los riesgos de ciberseguridad en los entornos de nube y definir acciones de mitigación.	Transferir	Realizar una evaluación de riesgos de seguridad en los servicios de nube pública y privada.
Otros	Evaluar riesgos de ciberseguridad en infraestructuras.	Identificar riesgos y medidas para mitigarlos.	Transferir	Realizar evaluación de riesgos de seguridad digital.
Otros	Identificar y tratar riesgos en los proyectos de TI para fortalecer la seguridad de los sistemas.	Riesgos evaluados y tratados.	Transferir	Identificación y tratamiento de riesgos en proyectos de TI.
Otros	Evaluar riesgos de ciberseguridad en servicios en la nube.	Identificar riesgos en servicios en la nube y mitigarlos.	Transferir	Realizar evaluación de seguridad de servicios en la nube.
Otros	Evaluar riesgos de seguridad en activos de información.	Identificar riesgos y medidas de mitigación.	Transferir	Realizar evaluación de riesgos en activos de información.
Otros	Validar y mitigar riesgos críticos.	Riesgos evaluados y mitigados.	Transferir	• Evaluación de riesgos de TI • Análisis de vulnerabilidades

9. Indicadores de seguimiento

Tabla 4. Indicadores del plan

Nombre	Indicador	Meta	Frecuencia
Índice de desempeño del cronograma (SPI)	Riesgos documentados y priorizados	Riesgos documentados y priorizados	Anual
Reprocesos	Identificar y priorizar los riesgos de ciberseguridad en los entornos de nube y definir acciones de mitigación.	Identificar y priorizar los riesgos de ciberseguridad en los entornos de nube y definir acciones de mitigación.	Anual

Evaluación de ciberseguridad.	Identificar riesgos y medidas para mitigarlos.	Identificar riesgos y medidas para mitigarlos.	Anual
Evaluación de ciberseguridad.	Riesgos evaluados y tratados.	Riesgos evaluados y tratados.	Anual
Evaluación de ciberseguridad.	Identificar riesgos en servicios en la nube y mitigarlos.	Identificar riesgos en servicios en la nube y mitigarlos.	Anual
Evaluación de ciberseguridad.	Identificar riesgos y medidas de mitigación.	Identificar riesgos y medidas de mitigación.	Anual
Evaluación de ciberseguridad.	Riesgos evaluados y mitigados.	Riesgos evaluados y mitigados.	Anual

10. Normatividad

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993 - Modifica y adiciona la Ley 23 de 1982 en materia de derechos de autor, relevante para el área de desarrollo del DADEP.
- Ley 1581 de 2012 - Protección de Datos Personales.
- Ley 1273 de 2009 - Delitos Informáticos y protección de datos.
- Ley 1712 de 2014 - Ley de Transparencia y Acceso a la Información Pública.
- Ley 2052 de 2020 - Código General Disciplinario.
- Decreto 338 de 2022 - Lineamientos generales para la seguridad digital y la gestión de infraestructuras críticas cibernéticas.
- Decreto 1499 de 2017 - Sistema de Gestión de Seguridad de la Información.
- Decreto 1008 de 2018 - Política de Gobierno Digital.
- Decreto 2106 de 2019 - Simplificación de trámites administrativos en seguridad digital.
- Resolución 512 de 2019 - Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de Servicios.
- CONPES 3701 de 2011 - Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

Actualizó: Sandra Marcela Venegas Páez - contratista
Revisó: Hugo Roberto Hernández Díaz – jefe OTIC
Aprobó: Hugo Roberto Hernández Díaz – jefe OTIC

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
1.0	22/04/2024	Creación del plan de tratamiento de Riesgos de Seguridad de la información
2.0	11/04/2025	Actualización para el 2025
	28/1/2025	Actualización para aprobación en Comité de Gestión