SECRETARÍA DISTRITAL DE PLANEACIÓN

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

Responsable:

Comité Institucional de Gestión y Desempeño
Secretaría Distrital de Planeación
Actualización presentada y aprobada en sesión del Comité Institucional de Gestión y Desempeño de la SDP realizada el 22 de enero de 2025

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

La Secretaría Distrital de Planeación (SDP) lidera la planeación integral de Bogotá (territorial, económica, social y ambiental) y busca optimizar su gestión a través de las TIC, dentro del marco del Gobierno Digital. Así mismo, en cumplimiento del Decreto 612 de 2018, la SDP integró sus planes institucionales y estratégicos al Plan de Acción, publicándolos en el sitio web definido antes del 31 de enero de cada vigencia.

Mediante la Resolución No. 2153 de 2023, la SDP actualizó su Sistema de Gestión (SG) bajo el Modelo Integrado de Planeación y Gestión (MIPG). Este sistema se estructura en siete dimensiones, diecinueve políticas de gestión y desempeño institucional, y un componente ambiental, cada uno liderado por dependencias específicas dentro de la SDP.

La Resolución No. 2153 de 2023 establece que:

- El Comité Institucional de Gestión y Desempeño es responsable de dirigir la implementación de las políticas de Gobierno Digital y Seguridad Digital, asegurando los recursos necesarios para la transformación digital y la seguridad de la información.

- La Dirección de las Tecnologías de la Información y las Comunicaciones lidera estas políticas, definiendo e implementando el Plan Estratégico de Tecnologías de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Integrando sus procesos y planes bajo un marco normativo y estratégico claro, con roles y responsabilidades bien definidos la SDP refleja el interés estratégico de la alta dirección en la seguridad de la información, respaldando el desarrollo de planes de gestión del riesgo y aprobando instrumentos asociados al Sistema de Gestión de Seguridad de la Información.

2. OBJETIVO

Generar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información siguiendo lo establecido en la Política de Administración del Riesgo DEI-PO-001, en la cual se definió la guía metodológica que permite a los responsables de los procesos de la SDP gestionar los riesgos, que en materia de seguridad y privacidad de la información sea necesario sobre los activos de información que hacen parte del Registro de Activos de Información de la SDP (RAI) – Datos/Información, Hardware, Software, Redes y Comunicaciones y Servicios, clasificados con una criticidad ALTA por sus dueños, según la

valoración dada de acuerdo con los principios fundamentales de la seguridad de la información, confidencialidad, integridad y disponibilidad.

2.1. OBJETIVOS ESPECÍFICOS

- Realizar la actualización y aprobación del Inventario de Activos de Información de la SDP, en concordancia con la guía y formato formalizados en el Sistema de Gestión de la entidad.
- Elaborar mapas de riesgos de seguridad de la información para cada proceso, que incluyan la evaluación de riesgos, la determinación del nivel de riesgo residual y la definición del tratamiento (Aceptar, Evitar, Transferir o Mitigar).
- Formular y hacer seguimiento a los planes de acción en los mapas de riesgos de seguridad de la información.
- Evaluar la eficacia del tratamiento implementado mediante la revisión de segunda línea de defensa.
- Publicar el Registro de Activos de Información e Índice de información clasificada y reservada en el sitio web definido.
- Revisar, actualizar y aprobar los mapas de riesgos de seguridad de la información de los procesos institucionales.

3. ALCANCE

El alcance de la gestión de riesgos de seguridad de la información, incluyendo su tratamiento, abarca todos los activos de información de la SDP identificados con criticidad ALTA en el Registro de Activos de Información de la SDP (RAI) – Datos/Información, Hardware, Software, Redes y Comunicaciones y Servicios. Esta gestión se realiza conforme a las normas vigentes, la Política de Administración del Riesgo DEI-PO-001, la metodología DEI-MA-001, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 6) y el Anexo 4 del Modelo Nacional de Gestión de Riesgos de Seguridad de la Información para Entidades Públicas, siguiendo las pautas de la NTC-ISO/IEC 27001 para su seguimiento, monitoreo, evaluación y mejora continua.

4. DOCUMENTOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

A continuación, se relacionan artefactos del SGSI como parte del Sistema de Gestión-MIPG relacionados con el plan:

Tabla 1. Documentos del Sistema de Gestión de Seguridad de la Información

	Proceso	Código	Título Documento
1	Dirección Estratégica Institucional	DEI-PO-001	Política de Administración del Riesgo
2	Dirección Estratégica Institucional	DEI-MA-001	Instructivo para la Gestión del Riesgo
3	Gobierno de Tecnologías de la Información	GTI-GA-001	Guía para la Gestión de Activos de Información de la SDP
4	Gobierno de Tecnologías de la Información	GTI-FO-003	Formato Registro de Activos de Información (RAI)
5	Gobierno de Tecnologías de la Información	GTI-DI-001	Registro de Activos de Información (RAI)

Fuente: Sistema de Gestión Gestiónate

5. MARCO DE REFERENCIA

La Secretaría Distrital de Planeación asume la gestión de los riesgos de seguridad y privacidad de la información con base en la Política de Administración del Riesgo DEI-PO-001 y recomendaciones de las ISO 31000 y 27005.

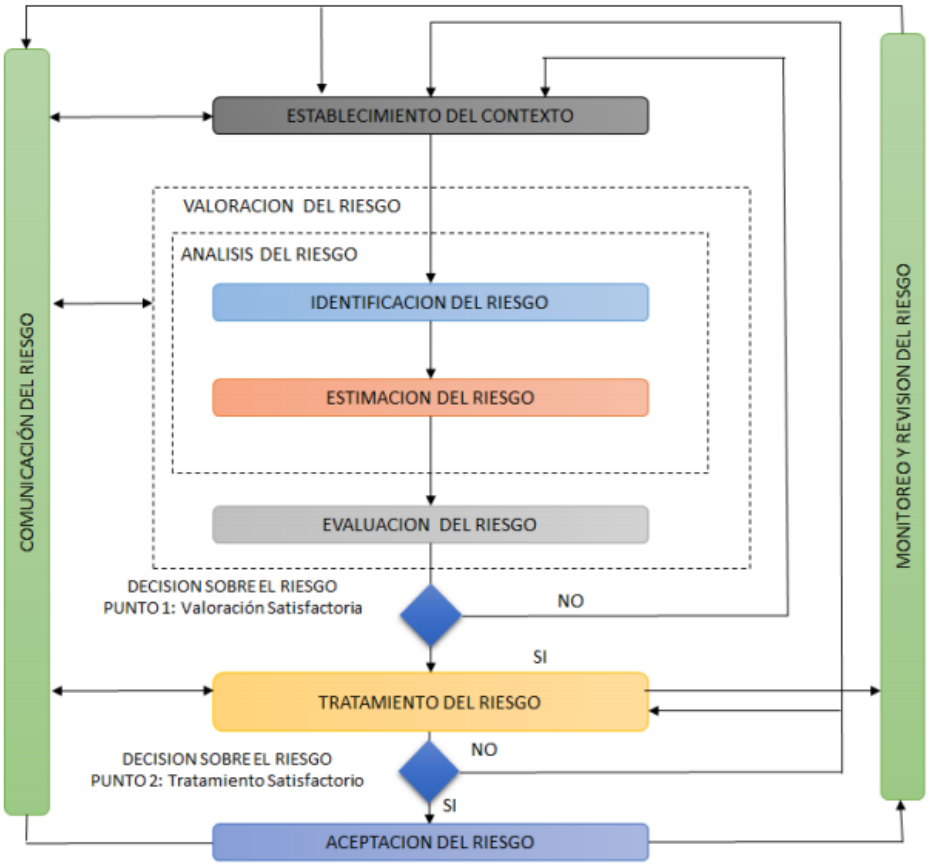
La administración del riesgo en la SDP sigue las siguientes etapas y lineamientos generales, los cuales son desarrollados en profundidad en los documentos que hacen parte del Sistema de Gestión.

Figura 1. Metodología Administración de Riesgos en la SDP

Fuente: Elaboración propia con los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas *elaborada por el DAFP*.

Es oportuno mencionar que, en el Modelo de Gestión de Riesgos de Seguridad de la Información, se definió que, para la adecuada administración, la valoración y/o tratamiento del riesgo, es necesario realizar seis actividades; el establecimiento del contexto, la valoración del riesgo, el tratamiento del riesgo, la aceptación del riesgo, la comunicación del riesgo y monitoreo y revisión del riesgo. En la siguiente figura se observa la iteración entre las actividades definidas:

Figura 2. Proceso Gestión de Riesgos de Seguridad Digital

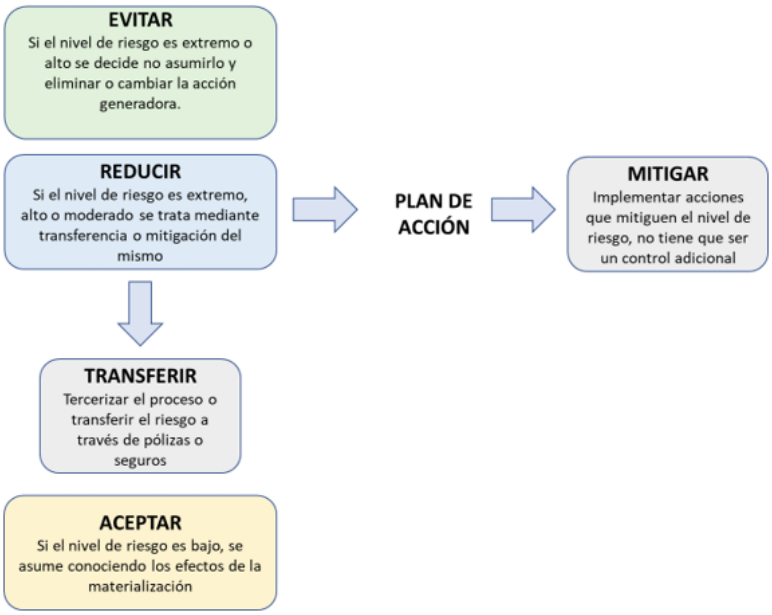


Fuente: *ISO/IEC 27005*

El Plan de Tratamiento de Riesgos de la SDP, tiene como base el ejercicio documentado de identificación del contexto organizacional, aplicado a cada uno de los procesos estratégicos, misionales, apoyo y de evaluación de la entidad contenido en el documento Política de Administración del Riesgo DEI-PO-001, formulada por la Dirección de Planeación Institucional de la SDP, la cual incluye la metodología a seguir para la identificación, valoración, análisis, evaluación del riesgo, definición y valoración de controles, niveles de aceptación del riesgo y su tratamiento.

Para el tratamiento de los riesgos, en la Política de Administración del Riesgo se establecieron tres opciones de tratamiento del riesgo residual; Evitar, Reducir y Transferir, como puede verse a continuación:

Figura 3. Tratamiento del Riesgo Residual



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas elaborada por el DAFP.

Tabla 2. Descripción Tratamiento del Riesgo Residual

Aceptar	Consiste en retener el riesgo sin acción posterior, los riesgos se analizan y se viabiliza su aceptación si la frecuencia es baja y el impacto es leve o menor y no se pone en riesgo la estabilidad y operatividad.
Evitar	Evitar la actividad o la acción que da origen al riesgo particular, esta alternativa de tratamiento ocurre cuando su probabilidad es alta y representa un alto peligro. Es de analizar si los costos para implementar los controles exceden los beneficios se puede viabilizar la decisión de evitar entonces el riesgo.
Reducir	Minimizar el impacto del riesgo, o reducir las posibilidades de que ocurra, es también una acción válida dentro de un proceso de Gestión de Riesgos, dado que mitigar significa que se puede limitar el impacto de un riesgo, de modo que, aunque este ocurra, el impacto sea mínimo y fácil de subsanar
Transferir	Transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular, la transferencia se puede realizar mediante un seguro, al transferir el

	riesgo a un tercero le damos responsabilidad para su administración, pero no significa que se elimine el riesgo.
Eliminar	Se puede eliminar la fuente del riesgo.

Fuente: ISO 31000 de 2018

En la SDP se establecen las siguientes opciones de tratamiento e instrumentos de conformidad con el nivel de riesgo residual identificado, los líderes de proceso definirán las medidas de tratamiento que aplicarán de acuerdo con la evaluación de los riesgos:

Tabla 3. Opciones de Tratamiento por Nivel de Riesgo

NIVELES DE RIESGO RESIDUAL	OPCIONES DE TRATAMIENTO	INSTRUMENTOS
BAJO	Asumir el riesgo	Controles
	Reducir el riesgo	Controles
MODERADO	Reducir el riesgo	Controles
ALTO	Reducir el riesgo	Controles y Plan de Acción. Contar con un indicador clave de riesgo.
	Transferir el riesgo	Pólizas, contratos u otros documentos que den constancia de la transferencia del riesgo. Contar con un indicador clave de riesgo.
	Evitar el riesgo	Eliminación o suspensión de la actividad o proceso en el sistema de gestión.
EXTREMO	Reducir el riesgo	Controles y Plan de acción. Contar con un indicador clave de riesgo.
	Transferir el riesgo	Pólizas, contratos u otros documentos que den constancia de la transferencia del riesgo. Contar con un indicador clave de riesgo.
	Evitar el riesgo	Eliminación o suspensión de la actividad o proceso en el sistema de gestión.

Fuente: *Elaboración propia*

Bajo el contexto anterior, se estableció un cronograma de actividades para adelantar en la vigencia 2025.

6. PLAN DE TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD E LA INFORMACIÓN PARA LA VIGENCIA 2025

A continuación, se presenta el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2025. Este plan abarca: 1) la identificación de activos de información (Datos/información, Hardware, Software, Redes y Comunicaciones y Servicios); 2) la identificación, clasificación y seguimiento de riesgos de seguridad digital; y 3) la publicación del Registro de Activos de Información y la Información Clasificada y Reservada.

Tabla 4. Cronograma de Actividades Tratamiento de Riesgos de Seguridad Digital

1. Gestión de Activos de Información					
Actividad		**Resultado Esperado**	**Responsable**	**Mes inicio**	**Mes fin**
1.1	Revisión y/o actualización de Instrumentos	Instrumentos actualizados: • GTI-GA-001 - Guía para la Gestión de Activos de Información de la SDP. • GTI-FO-003 - Formato Registro de Activos de Información (RAI).	Profesional que ejerce el rol de Oficial de Seguridad de la Información. Enlace del Sistema de Gestión - SG Proceso Gobierno de TI. Líder de la Dirección Administrativa encargado de la Seguridad Física. Líder de Gestión del Talento Humano.	Febrero 2025	Mayo 2025
1.2	Revisión y actualización de Activos de Información	Inventario de Activos de Información de la SDP actualizado: GTI-DI-001 - Registro de Activos de información (RAI).	Profesional que ejerce el rol de Oficial de Seguridad de la Información. Todos los Directivos - Líder y responsable por proceso. Los enlaces del Sistema de Gestión - SG de cada dependencia.	Junio 2025	Septiembre 2025

1.3	Aprobación de Activos de Información	Inventario de Activos de Información de la SDP aprobado: GTI-DI-001 - Registro de activos de información (RAI).	Comité Institucional de Gestión y Desempeño de la SDP.	Septiembre 2025	Noviembre 2025

2. Identificación, Clasificación y Seguimiento de los Riesgos de Seguridad Digital					
Actividad		**Resultado Esperado**	**Responsable**	**Mes inicio**	**Mes fin**
2.1	Revisión, actualización y aprobación de Mapas de Riesgos de Seguridad de la Información de los procesos institucionales de acuerdo con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas vigente	Mapa de Riesgos de Seguridad de la Información 2024 para todos los procesos revisado primera y segunda línea de defensa y/o actualizado.	Dirección de Planeación Institucional. Líderes de los procesos. Profesional que ejerce el rol de Oficial de Seguridad de la Información	Enero de 2025	Enero 2025
2.2	Identificación Riesgos de Seguridad Digital 2025	Riesgos de Seguridad Digital identificados y/o sobre los activos de información clasificados en el Registro de Activos de Información con criticidad Alta.	Profesional que ejerce el rol de Oficial de Seguridad de la Información. Líderes de procesos.	Enero 2025	Febrero 2025
2.3	Evaluación y clasificación del Riesgo Inherente de Seguridad Digital	* Riesgos de Seguridad Digital Clasificados y valorados según la metodología definida por la entidad en el DEI-MA-001. * Instructivo para la Gestión del Riesgo, Guía para	Profesional que ejerce el rol de Oficial de Seguridad de la Información. Líderes de todos los procesos.	Marzo 2025	Abril 2025

2. Identificación, Clasificación y Seguimiento de los Riesgos de Seguridad Digital					
Actividad		**Resultado Esperado**	**Responsable**	**Mes inicio**	**Mes fin**
		la Administración del Riesgo y el Diseño de Controles en Entidades Pública, Versión 6, Anexo 4 – Lineamientos para la Gestión del Riesgo de Seguridad Digital en las Entidades Públicas. * Mapa de Riesgos con riesgo inherente calculado (antes de los controles).			
2.3.1	Evaluación y clasificación del Riesgo Residual de Seguridad Digital	*Identificar y valorar por cada uno de los riesgos, los controles de seguridad de la información que hacen parte del Anexo A de la norma NTC-ISO/IEC 27001. *Mapa de Riesgos con riesgos residuales calculado después de los controles).	Profesional que ejerce el rol de Oficial de Seguridad de la Información. Líderes de los procesos.	Marzo 2025	Abril 2025
2.3.2	Aprobación interna de Riesgos de Seguridad Digital y Plan de Tratamiento de Riesgos (Definición de acciones en el marco de los	- Riesgos de Seguridad Digital y Plan de Tratamiento de Riesgos aprobados por los líderes de cada uno de los procesos.	Líderes de los procesos.	Marzo 2025	Abril 2025

2. Identificación, Clasificación y Seguimiento de los Riesgos de Seguridad Digital					
Actividad		**Resultado Esperado**	**Responsable**	**Mes inicio**	**Mes fin**
	Planes de Mejoramiento de la SDP)				
2.4	Monitoreo Segunda Línea de Defensa para los riesgos de todos los procesos	Informes cuatrimestrales segunda línea de defensa para todos los procesos. (Tres revisiones al año, una por cada cuatrimestre)	Profesional que ejerce el rol de Oficial de Seguridad de la Información.	Mayo de 2025	Diciembre de 2025

3. Publicación de los instrumentos de gestión					
Actividad		**Resultado Esperado**	**Responsable**	**Mes inicio**	**Mes fin**
3.1	Consolidación, generación y publicación de los instrumentos	Registro de Activos de Información e Índice de Información Clasificada y Reservada	Profesional que ejerce el rol de Oficial de Seguridad de la Información Todos los Directivos - Líder y responsable por proceso Los enlaces del Sistema de Gestión - SG de cada dependencia	Noviembre de 2025	Noviembre de 2025

Fuente: *Elaboración propia*

7. TERMINOLOGÍA

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.

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 institución (materializar el riesgo).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control o Medida: Medida que permite reducir o mitigar un riesgo. Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Integridad: Propiedad de exactitud y completitud.

Impacto: Son las consecuencias que genera un riesgo una vez se materialice.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad

inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: *Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.*

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.