2026

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

SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO

Subdirección de Informática y Sistemas

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE DESARROLLO ECONÓMICO

BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCIÓN. 3

2. DEFINICIONES Y SIGLAS 3

3. NORMATIVIDAD 4

4. GENERALIDADES DEL PLAN O PROYECTO O PROGRAMA 5

4.1 Objetivo(s) 5

4.2 Alcance 5

5. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6

5.1. Análisis de Información 6

5.2. Identificación de Riesgos 6

5.3. Evaluación y análisis del riesgo 7

5.4. Control del riesgo 8

6. METODOLOGÍA DE SEGUIMIENTO 8

6.1 Monitoreo y revisión de riesgos 8

7. CRONOGRAMA DE ACTIVIDADES 9

8. ANEXOS 9

1. INTRODUCCIÓN.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 de la Secretaría Distrital de Desarrollo Económico (SDDE) establece una hoja de ruta para identificar, evaluar y mitigar los riesgos asociados a los activos de información críticos de la entidad. Este plan responde a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y cumple con las normativas nacionales e internacionales vigentes en materia de seguridad digital. Además, se encuentra alineado con el Modelo Integrado de Planeación y Gestión (MIPG), específicamente con la dimensión de Gestión y Desempeño Institucional, integrando sus políticas para fortalecer la capacidad de respuesta institucional frente a los desafíos del entorno digital.

El desarrollo de este plan contribuye a fortalecer las condiciones y capacidades institucionales de la SDDE, promoviendo un enfoque integral de gestión del riesgo que alinea la seguridad de la información con los procesos organizacionales y sus activos críticos. Este enfoque refuerza la integridad, confidencialidad y disponibilidad de la información institucional mediante la implementación de controles y medidas de tratamiento efectivas. Asimismo, a través de un proceso continuo de análisis, supervisión y monitoreo, se busca garantizar la resiliencia de la entidad frente a amenazas actuales y emergentes, fomentando una cultura institucional orientada a la seguridad.

2. DEFINICIONES Y SIGLAS

- **Aceptación del riesgo:** Decisión informada de tomar un riesgo particular.
- **Análisis de riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- **Control:** Medida que modifica el riesgo.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **Propietario del riesgo:** Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Riesgo de Seguridad de la Información:** Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo.
- **Tríada de la información:** Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una o más amenazas.

3. NORMATIVIDAD

Normatividad	Entidad	Descripción
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 2277 de 2025	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia
Resolución 500 de 2021	Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	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.
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Normatividad	Entidad	Descripción
	de Colombia Departamento Nacional de Planeación	

4. GENERALIDADES DEL PLAN O PROYECTO O PROGRAMA

4.1 Objetivo(s)

Objetivo General

Establecer y desarrollar un plan de acción integral para la gestión de riesgos de seguridad de la información y digital, con el objetivo primordial de preservar la integridad, confidencialidad y disponibilidad de los activos de información institucional.

Objetivos Específicos

- Realizar un análisis de riesgos que evalúe el impacto potencial en la integridad, confidencialidad y disponibilidad de la información institucional.

- Documentar y gestionar las decisiones de tratamiento, mitigación o aceptación de los riesgos de seguridad y privacidad de la información, con base en el análisis del riesgo residual y la capacidad institucional.

- Implementar estrategias proactivas para reducir la probabilidad de incidentes, acompañados de formación y concienciación para los funcionarios y contratistas sobre prácticas de seguridad de la información.

4.2 Alcance

Este plan se enfocará en la identificación, evaluación y mitigación de riesgos asociados a los activos de información de la SDDE. Además, se incorporarán prácticas continuas de monitoreo y revisión para adaptarse a las cambiantes amenazas de seguridad y garantizar una protección efectiva de la información.

5. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El proceso de gestión de riesgos de seguridad de la información que se llevará a cabo en la entidad se estructura en un ciclo continuo y dinámico, alineado con las metodologías y directrices establecidas por el DAFP y el MinTIC. Este ciclo, detallado a continuación, se fundamenta en la ejecución de las actividades propuestas para asegurar una gestión efectiva y actualizada de los riesgos asociados a la seguridad de la información

5.1. Análisis de Información

El primer paso en el proceso de identificación de riesgos será la identificación, clasificación y actualización periódica de los activos de información en cada una de las áreas. Esta tarea, esencial para una gestión efectiva de la seguridad de la información, involucrará una revisión detallada y precisa de todos los activos de información, asegurando que su clasificación refleje adecuadamente su importancia y sensibilidad.

El líder de cada área desempeñará un papel clave en este proceso, será su responsabilidad no solo identificar y clasificar los activos de información, sino también realizar una priorización cuidadosa de aquellos activos que tengan una calificación de riesgo en nivel alto. Esta priorización debe basarse en criterios establecidos y objetivos, utilizando el formato designado para tal fin. Además de los activos de alto riesgo, el líder del área también deberá considerar incluir en la evaluación aquellos activos que, aunque no estén clasificados inicialmente como de alto riesgo, puedan ser relevantes para la generación y gestión de riesgos debido a su naturaleza, uso o importancia estratégica.

La priorización de los activos de información se realizará considerando aquellos que, de acuerdo con su valoración de riesgos, superen el nivel de tolerancia definido por la entidad, y que requieran la implementación de acciones de tratamiento específicas durante la vigencia.

5.2. Identificación de Riesgos

En la etapa de identificación de riesgos se evaluarán las amenazas y vulnerabilidades que puedan afectar los activos de información de la entidad, analizando sus posibles consecuencias y estimando tanto la probabilidad de ocurrencia como el impacto sobre la seguridad de la información. Este análisis se enfocará en los tres principios fundamentales: confidencialidad, integridad y disponibilidad.

El proceso contempla determinar de qué manera cada amenaza, ya sea interna o externa, podría interrumpir o comprometer uno o más componentes de esta tríada. Para ello, se considerarán aspectos como la sensibilidad de los activos involucrados y el contexto operativo en el que se gestionan.

La priorización de los análisis se formalizará mediante memorando interno, en el cual se solicitará a las áreas responsables dar prioridad a los activos de información que, conforme al formato GT-P5-F1, hayan sido clasificados con criticidad "ALTA". Las áreas que no identifiquen activos con dicha criticidad podrán, de manera voluntaria, solicitar el acompañamiento de la Subdirección de Informática y Sistemas para analizar riesgos asociados a activos que consideren relevantes.
Para cada riesgo identificado se estimarán la probabilidad de ocurrencia y la magnitud del impacto potencial, con el fin de abordar no solo los riesgos más probables, sino también aquellos que, aunque menos frecuentes, podrían generar consecuencias significativas para la entidad.
Este ejercicio se desarrollará de manera dinámica y continua, de forma que se ajuste oportunamente a cambios en el entorno operativo y a la evolución del panorama de amenazas y vulnerabilidades. Una identificación rigurosa de riesgos constituye un insumo esencial para definir medidas de tratamiento y fortalecer una gestión integral, proactiva y efectiva de los riesgos de seguridad de la información.

5.3. Evaluación y análisis del riesgo

En el marco de la gestión de riesgos se establecen criterios específicos para dos etapas fundamentales: el análisis y la evaluación del riesgo. Estos criterios permiten asegurar un enfoque sistemático, consistente y alineado con las buenas prácticas en la gestión de riesgos de seguridad de la información.

Análisis del riesgo:

En esta etapa se identifican las fuentes de riesgo, así como la naturaleza de las amenazas y vulnerabilidades que podrían afectar los activos de información. El análisis busca comprender cómo dichos factores pueden incidir sobre la confidencialidad, integridad y disponibilidad de la información, considerando el contexto operativo de la entidad.

Evaluación del riesgo:

Una vez realizado el análisis, se procede a evaluar cada riesgo identificado, determinando su probabilidad de ocurrencia y el nivel de impacto o consecuencia en caso de materializarse. Para ello, se aplicarán criterios claros y consistentes que permitan una estimación adecuada del nivel de riesgo inherente. Esta evaluación podrá apoyarse en escalas cualitativas o cuantitativas y considerar aspectos como la severidad del daño potencial, la sensibilidad de los activos afectados y la capacidad de respuesta de la entidad.

Para el desarrollo del ciclo de identificación, análisis y valoración de los riesgos, se empleará la matriz de gestión de riesgos PE-P5-F1, la cual servirá como instrumento de apoyo para la toma de decisiones y la definición de acciones de tratamiento.

5.4. Control del riesgo

Como respuesta a los riesgos identificados en el marco de la gestión de la seguridad de la información, la Entidad implementará controles específicos orientados a mitigar, reducir o tratar dichos riesgos. Para la selección y aplicación de estos controles se tomarán como referencia los estándares establecidos en el Anexo de la NTC-ISO/IEC 27002:2022, sin perjuicio de que la Entidad adopte controles adicionales o alternativos que considere pertinentes, de acuerdo con su contexto, capacidades y necesidades particulares.

Los controles serán seleccionados y ajustados de manera proporcional al nivel de riesgo identificado, con el propósito de disminuir la probabilidad de materialización de incidentes de seguridad de la información y mitigar sus posibles impactos. Estos controles podrán ser de carácter organizativo, técnico o físico, e incluirán políticas, procedimientos y mecanismos operativos necesarios para garantizar una protección efectiva de la información y la sostenibilidad de las medidas implementadas.

6. METODOLOGÍA DE SEGUIMIENTO

6.1 Monitoreo y revisión de riesgos

Con el fin de asegurar la efectividad y pertinencia continua de las estrategias de tratamiento de riesgos, la Subdirección de Informática y Sistemas realizará revisiones periódicas al avance del Plan de Tratamiento de Riesgos de Seguridad de la Información, con una periodicidad cuatrimestral.

Durante estas revisiones se validará el desempeño de los controles implementados, se identificarán nuevas vulnerabilidades o variaciones en el panorama de riesgos y, cuando sea necesario, se efectuarán ajustes al plan para fortalecer su eficacia. Como resultado de este proceso, se elaborará un informe que será remitido a los responsables de cada riesgo, incorporando las evidencias derivadas de los seguimientos realizados y de los reportes de incidentes gestionados.

Las evidencias asociadas al monitoreo y revisión del plan se administrarán a través de un repositorio digital centralizado, bajo la responsabilidad de la Subdirección de Informática y Sistemas, garantizando

su trazabilidad, disponibilidad y conservación, en cumplimiento de las políticas institucionales de gestión documental.

7. CRONOGRAMA DE ACTIVIDADES

El cronograma se encuentra como Anexo PE-P7-F2 Anexo Planes Institucionales y hace parte integral del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

8. ANEXOS

Anexo 1 - PE_P7_F2_V2_ANEXO CRONOGRAMA PLAN TRATAMIENTO RIESGOS-2026

Versión	ELABORÓ	REVISÓ	APROBÓ	FECHA
01	María Alejandra Suárez Contratista Subdirección de Informática y Sistemas	Daniel Cárdenas Equipo MIPG- Oficina Asesora de Planeación Lady Laiton Linares Jefe Oficina Asesora de Planeación Adriana Montoya Ríos Subdirectora de Informática y Sistemas	Comité Institucional de Gestión y Desempeño	29/01/2026

CONTROL DE CAMBIOS			
CAMBIOS EN EL DOCUMENTO	**RESPONSABLE**	**FECHA**	**VERSIÓN**
Formulación y aprobación del Documento en CIGD	Adriana Montoya Ríos Subdirectora de Informática y Sistemas	29/01/2026	01

ALCALDÍA MAYOR
DE BOGOTÁ D.C.

SECRETARÍA DE
DESARROLLO
ECONÓMICO

BOGOTÁ