2025

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Versión: 02

Subdirección de Informática y Sistemas

SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO
BOGOTÁ

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2025

Versión	Elaboró	Revisó	Aprobó	Fecha
01	**María Alejandra Suárez** Contratista Subdirección de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	29/01/2024
02	**María Alejandra Suárez** Contratista Subdirección de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	

Versión	Control de Cambios del Plan
01	Versión para la vigencia 2024, aprobado en acta CIGD No.: 001 del 29/01/2024
02	Se incorpora ítem con el marco normativo En el numeral 5 se ajusta la Columna "presupuesto" por "tipo de recurso Se incorpora introducción Actualización de las actividades para la vigencia 2025 **Versión para la vigencia 2025, aprobado en acta CIGD No.:**

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO

BOGOTÁ

Tabla de Contenido

Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025 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.

1. Marco Normativo

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 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

Normatividad	Entidad	Descripción
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

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. 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.

3.1. Objetivos Específicos

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

- Diseñar e implementar un conjunto de controles específicos para mitigar los riesgos identificados, asegurando la protección de los activos de información.

- 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. 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.

Esta aproximación garantiza un enfoque integral y sistematizado hacia la seguridad de la información, alineando las necesidades y riesgos específicos de cada proceso institucional con las estrategias globales de gestión de riesgos de la entidad.

5.2. Identificación de Riesgos

En el proceso de identificación de riesgos, se evaluarán las amenazas y vulnerabilidades que puedan afectar los activos de información, analizando sus posibles consecuencias y estimando tanto la probabilidad como el impacto en la seguridad de la información. Este

análisis se centrará en los tres pilares fundamentales de la seguridad de la información: integridad, confidencialidad y disponibilidad.

El proceso incluye el análisis de cómo cada amenaza detectada podría interrumpir o comprometer uno o más aspectos de esta tríada. Para ello, se considerarán factores como la naturaleza de la amenaza (interna o externa), la sensibilidad de los activos afectados y el contexto operativo de la entidad.

La solicitud para priorizar los análisis se formaliza mediante un memorando interno, en el que se insta a las áreas responsables a dar prioridad a los activos de información que, según el formato GT-P5-F1, hayan sido clasificados con una criticidad "ALTA" en la casilla correspondiente. Las áreas que no identifiquen activos con criticidad alta podrán, de manera voluntaria, solicitar el apoyo de la Subdirección de Informática y Sistemas para realizar un análisis de riesgos de seguridad en activos que consideren relevantes.

Para cada riesgo identificado, se calcularán tanto la probabilidad de ocurrencia como la magnitud del impacto potencial. Este enfoque asegura que se aborden no solo los riesgos con alta probabilidad, sino también aquellos que, aunque menos frecuentes, podrían tener un impacto significativo en la entidad.

Adicionalmente, este proceso será dinámico y continuo, adaptándose a los cambios en el entorno operativo, así como a las nuevas amenazas y vulnerabilidades emergentes en el panorama de la seguridad de la información. La identificación efectiva y precisa de riesgos es un paso fundamental para desarrollar estrategias de mitigación adecuadas y garantizar una gestión integral, proactiva y efectiva de los riesgos de seguridad de la información

5.3. Evaluación y análisis del riesgo

En el proceso de gestión de riesgos, se definen criterios específicos para dos etapas clave: el análisis y la evaluación del riesgo. Estos criterios son fundamentales para garantizar un enfoque sistemático y coherente en la gestión de riesgos de seguridad de la información.

- Análisis del Riesgo: Los criterios establecidos para el análisis del riesgo deben incluir la identificación de las fuentes de riesgo, la naturaleza de las amenazas y vulnerabilidades, y la manera en que estas podrían afectar a los activos de información.

- Evaluación del Riesgo: Una vez analizado el riesgo, se procede a su evaluación. Este paso establece la probabilidad de ocurrencia de cada riesgo identificado, así como el nivel de consecuencia o impacto que tendría en caso de materializarse. Los criterios para esta evaluación deben ser claros y consistentes, permitiendo una estimación precisa de la zona de riesgos inherentes. Esto puede incluir el uso de escalas cuantitativas o cualitativas para medir tanto la probabilidad como el impacto, y la consideración de factores como la severidad del daño potencial, la sensibilidad de los activos afectados y la capacidad de la entidad para responder al riesgo.

Para llevar a cabo el ciclo de identificación, análisis y valoración de riesgos, se utilizará la matriz de gestión de riesgos PE-P5-F1.

5.4. Control del riesgo

En respuesta a los riesgos identificados en la gestión de la seguridad de la información, la Entidad implementará controles específicos destinados a mitigar o tratar dichos riesgos.

Para la selección y aplicación de estos controles, se tomará como referencia los estándares establecidos en el Anexo de la NTC-ISO-IEC 27002:2022. Estos controles serán cuidadosamente seleccionados y adaptados a las necesidades y contextos específicos de la Entidad, con el objetivo principal de reducir la probabilidad de materialización de los riesgos asociados a incidentes de seguridad. Esto incluirá, pero no se limitará a, controles organizativos, técnicos y físicos, así como políticas y procedimientos relevantes para asegurar la protección eficaz de la información.

5.5. Monitoreo y revisión de riesgos

Para garantizar la efectividad y pertinencia continua de las estrategias de tratamiento de riesgos, la Subdirección de Informática y Sistemas realizará revisiones periódicas del avance del plan de tratamiento de riesgos de seguridad de la información, con una periodicidad cuatrimestral.

Durante estas revisiones, se evaluará el desempeño de los controles implementados, se identificarán posibles nuevas vulnerabilidades o cambios en el panorama de riesgos y, en caso necesario, se ajustará el plan para optimizar su eficacia. Como parte de este proceso, se generará un informe detallado que será remitido a los responsables de cada riesgo, incorporando las evidencias obtenidas de los seguimientos y reportes de incidentes.

Estas evidencias se gestionarán mediante un repositorio digital centralizado, administrado por la Subdirección de Informática y Sistemas, el cual garantizará su trazabilidad, disponibilidad y conservación, cumpliendo con las políticas de gestión documental establecidas por la Entidad

6. Cronograma de Actividades

No.	ACTIVIDAD	TIPO DE RECURSO	RESPONSABLE	ENTREGABLE	FECHA INICIO	FECHA FIN
1	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta	Recurso humano	Líderes de área	Formato con riesgos identificados	15/02/2025	31/03/2025
2	Establecer controles y planes de tratamiento sobre los riesgos	Recurso humano	Líderes de área	Formato con riesgos identificados, controles y planes de mejora asociados.	15/02/2025	31/03/2025
3	Estructura las carpetas para almacenamiento de las evidencias reportadas por las áreas	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Estructura en Drive	15/02/2025	31/03/2025
4	Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los líderes de las áreas, con sus respectivas evidencias.	Recurso humano	Líderes de área	Memorando radicado en GesDoc	02/05/2025 02/09/2025	10/05/2025 15/09/2025
5	Configurar la herramienta de ciberseguridad y llevar a cabo las acciones necesarias para el monitoreo continuo de alertas que indiquen anomalías en la red, con el fin de identificar, analizar y mitigar posibles amenazas de manera oportuna	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Herramienta con políticas definidas y funcionales	15/01/2025	28/03/2025

6	Definir e implementar lineamientos específicos para abordar la protección y gestión de la propiedad intelectual en el proceso de contratación, con el fin de garantizar que los derechos de propiedad intelectual de la SDDE sean considerados y protegidos.	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Memorando Oficina Jurídica.	15/01/2025	28/03/2025
7	Documentar instructivo relacionado con el borrado seguro de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Documento publicado en intranet	02/06/2025	29/08/2025
8	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Reportes de las herramientas	01/04/2025	15/12/2025

Fuente: Elaboración propia