

TABLA DE CONTENIDO

1. INTRODUCCIÓN	2
2. OBJETIVO	2
3. ALCANCE	2
4. CONTEXTO DE LA ENTIDAD	3
4.1. Contexto externo	3
4.2. Contexto interno	3
5. POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS	4
6. NORMATIVIDAD	4
7. TÉRMINOS Y DEFINICIONES	6
8. RESPONSABILIDAD Y AUTORIDAD	6
9. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO	8
9.1. Adopción Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP	9
9.2. Definición roles y responsabilidades para el SIGRIP	9
9.3. Niveles de aceptación del riesgo o tolerancia al riesgo	9
10. LINEAMIENTOS GENERALES GESTIÓN PREVENTIVA RIESGOS FISCALES	10
11. LINEAMIENTOS GENERALES PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	10
11.1. Riesgo de seguridad de la información	10
12. MONITOREO Y SEGUIMIENTO DEL RIESGO	11
13. MATERIALIZACIÓN DEL RIESGO	12
13.1. Primera línea de defensa	12
13.2. Segunda línea de defensa	12
13.3. Tercera línea de defensa	13
13.4. Línea estratégica	13
14. DIRECTRICES GENERALES DE LA DEBIDA DILIGENCIA	13
15. REVISIÓN Y DETECCIÓN DE OPERACIONES SOSPECHOSAS DE LA/FT/FP	14
16. COMPROMISO ANTISOBORNO Y ANTIFRAUDE	14
17. VIGENCIA	16

1. INTRODUCCIÓN

La administración del riesgo comprende el conjunto de elementos de control y sus interrelaciones, para que la entidad evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales; contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de autocontrol y autoevaluación institucional.

En este documento encontrarán la política que la Secretaría Distrital de Ambiente -SDA, establece la manera cómo gestionarlos, teniendo en cuenta los diferentes lineamientos correspondientes a los riesgos de gestión, fiscales, seguridad de la información y aquellos asociados al Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, que incluye como amenazas el soborno, el fraude, la inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP en la estructura de procesos de la SDA. La política integra los riesgos de gestión, fiscales, de corrupción, integridad pública, seguridad de la información y LA/FT/FP/ADM.

Esta política se desarrolla en concordancia con el Modelo Integrado de Planeación y Gestión - MIPG, el Modelo Estándar de Control Interno - MECI y los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 del Departamento Administrativo de la Función Pública (DAFP).

2. OBJETIVO

Definir los lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en la entidad, con el fin de fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público; asegurar la integridad, transparencia y eficiencia en la administración del patrimonio y de la gestión pública; y promover una cultura organizacional basada en la ética individual, la legalidad y el cumplimiento. Este objetivo incluye la definición clara de roles y responsabilidades bajo el esquema de líneas de defensa, garantizando la prevención, la gestión de las incertidumbres que puedan afectar el interés general y el logro de los objetivos institucionales.

3. ALCANCE

La Política de Gestión Integral del Riesgo es aplicable a los procesos (estratégicos, misionales, de apoyo y evaluación) del modelo de operación por procesos vigente de la Secretaría Distrital de Ambiente, e incluye:

- La definición de roles y responsabilidades.
- El seguimiento periódico obligatorio.
- Las acciones institucionales ante la materialización del riesgo.
- Incluye a servidores públicos, contratistas y terceros que desarrollen actividades para la Entidad

El tratamiento de los riesgos de seguridad de la información se complementará con los lineamientos específicos para el Modelo de Seguridad y Privacidad de la Información - MSPI.

El tratamiento de los riesgos de LA/FT/FPADM se complementará de manera específica con los lineamientos de los documentos Técnicos de la Secretaría General de la Alcaldía Mayor de Bogotá- y la Ruta Metodológica para la Implementación del SARLAFT en Entidades Distritales, así mismo se tendrán en cuenta los lineamientos de tratamiento establecidos en el SIGRIP.

4. CONTEXTO DE LA ENTIDAD

4.1. Contexto externo

La Secretaría Distrital de Ambiente establece un contexto estratégico externo que permite comprender el entorno en el cual se desarrollan sus procesos y las condiciones que inciden en la gestión de riesgos. Para ello, se tienen en cuenta datos e información objetivos y verificables, acordes con la realidad institucional y sectorial.

Este análisis incluye:

- Factores políticos, normativos y regulatorios que inciden en la gestión ambiental y el desarrollo rural.
- Condiciones sociales, económicas y culturales que afectan la prestación de servicios y la implementación de programas
- Variables ambientales y territoriales que determinan riesgos específicos en la operación de la Entidad
- Relación con actores externos: ciudadanía, organizaciones sociales, entidades públicas y privadas, organismos de control y cooperación internacional.
- Cada proceso deberá comprender el ambiente en el que se desenvuelve, identificando los factores de riesgo externos de manera objetiva y alineada con la realidad institucional, garantizando que la gestión se articule con las políticas distritales y nacionales.

4.2. Contexto interno

El contexto interno se define a partir de la información general de la Entidad, incluyendo su misión, visión y objetivos estratégicos, así como la estructura de procesos que soporta el modelo de operación por procesos y los sistemas de gestión vigentes.

Este análisis comprenderá:

- La misión, visión y objetivos estratégicos de la Secretaría Distrital de Ambiente.
- La estructura organizacional y jerárquica, con identificación de roles y responsabilidades en la gestión del riesgo.
- Los procesos estratégicos, misionales, de apoyo y de evaluación, en articulación con los sistemas de gestión institucionales.
- Los sistemas de información y herramientas tecnológicas utilizadas para el seguimiento y control.

- Los manuales internos, lineamientos y metodologías adoptadas para la administración del riesgo.
- La participación de terceros que apoyan la gestión institucional, incluyendo contratistas y aliados estratégicos.

Este contexto interno permitirá fortalecer el análisis de controles en la etapa de valoración, asegurando que los riesgos se gestionen de manera integral y que las medidas adoptadas sean pertinentes, efectivas y sostenibles.

COPIA CONTROLADA

5. POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS

La Secretaría Distrital de Ambiente, se compromete a identificar y gestionar de manera efectiva los riesgos de gestión, fiscales, de corrupción, integridad pública, seguridad de la información y LA/FT/FP/ADM; en los procesos estratégicos, misionales, de apoyo y de evaluación, a través del establecimiento del contexto, la identificación, análisis, evaluación, monitoreo, revisión y seguimiento de los riesgos e implementación de acciones de control para su mitigación, así como planes de contingencia ante la materialización de los riesgos; lo anterior, con el fin de asegurar la continuidad de las operaciones y contribuir con el logro de los objetivos y metas institucionales.

El cumplimiento de esta política es responsabilidad de toda la entidad, bajo el esquema de líneas de defensa, y evaluación independiente por parte de la Oficina de Control Interno, para lo cual se utilizará la herramienta dispuesta para el desarrollo de la metodología de riesgos.

6. NORMATIVIDAD

Tabla 1. Marco normativo - Administración del riesgo

NORMA	DESCRIPCIÓN
Ley 87 de 1993	Crea el Sistema Institucional de Control Interno y dota a la administración de un marco para el control de las actividades estatales, directamente por las mismas autoridades.
Ley 190 de 1995	Por la cual se dictan normas tendientes a preservar la moralidad en la Administración Pública y se fijan disposiciones con el fin de erradicar la corrupción administrativa.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712 de 2014	Por medio de la cual se crea la "Ley de Transparencia y del derecho de acceso a la Información Pública Nacional" y se dictan otras disposiciones.
Ley 2195 de 2022	Por medio del cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción capítulo 3 y 4 y se dictan otras disposiciones.
Decreto Nacional 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. (título 21)
Decreto Nacional 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del

NORMA	DESCRIPCIÓN
	<p>Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015; ARTÍCULO 2.2.22.3.1.</p> <p>Actualización del Modelo Integrado de Planeación y Gestión. Para el funcionamiento del Sistema de Gestión y su articulación con el Sistema de Control Interno, se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión - MIPG.</p>
Decreto Nacional 648 de 2017	Por la cual se modifica y adiciona el De 1083 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública
Decreto Nacional 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto Nacional 1122 de 2024	Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública
Decreto Distrital 640 de 2025	Por medio del cual se expide el Decreto Único del Sector Gestión Pública
Resolución MINTIC 500 de 2021	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
Resolución MINTIC 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
Resolución 02277 de 2025	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 MINTIC SDA 2534 de 2025	Por medio de la cual se actualiza el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Ambiente creado mediante la Resolución 1017 de 2023 y se dictan otras disposiciones.

NORMA	DESCRIPCIÓN
Circular 22 de Superintendencia Financiera de 2007	Instrucciones de la Superintendencia Financiera de Colombia respecto al reporte de información sobre la administración del riesgo de lavado de activos y de la financiación del terrorismo.
Circular 055 de Superintendencia Financiera de 2016	Modificación de las instrucciones relativas a la administración del riesgo de lavado de activos y de la financiación del terrorismo.
Circular Externa 027 de la Superintendencia Financiera de 2020	Instrucciones relativas a la administración del riesgo de lavado de activos y de financiación del terrorismo.

Fuente: Elaboración propia, Secretaría Distrital de Ambiente - SDA

7. TÉRMINOS Y DEFINICIONES

La Secretaría adopta el Glosario contenido en el Anexo 2 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 del Departamento Administrativo de la Función Pública (DAFP), en el cual se consolidan los términos y definiciones aplicables a las diferentes tipologías de riesgo y a los conceptos generales utilizados en la metodología de gestión del riesgo.

Este glosario incorpora y amplía las definiciones necesarias para la adecuada comprensión y aplicación de la presente política, en concordancia con las actualizaciones metodológicas desarrolladas en los diferentes capítulos del documento, particularmente aquellas relacionadas con las categorías o tipologías de riesgo allí establecidas

8. RESPONSABILIDAD Y AUTORIDAD

La responsabilidad y autoridad para la Administración del Riesgo por procesos, en la entidad está definida mediante las líneas de defensa y se acogen según la siguiente tabla:

Tabla 2. Responsabilidad y autoridad- Líneas de defensa

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
------------------	-------------	----------------------------------

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Secretario (a) Distrital de Ambiente Subsecretarios Directores Comité Institucional de Coordinación de Control Interno	<ul style="list-style-type: none"> Aprobar la Política de Gestión Integral del Riesgo como estrategia que apunte al cumplimiento de los planes de la entidad la cual incluye los niveles de responsabilidad y autoridad, con énfasis en la prevención del daño antijurídico. Asignar recursos para su implementación Definir apetito del riesgo Analizar los cambios en el entorno interno y externo que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles
	Comité Institucional de Gestión y Desempeño	<ul style="list-style-type: none"> Hacer monitoreo en el Comité Institucional de Coordinación de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando. Revisar los informes presentados de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos, así como la ejecución de los planes de acción establecidos para estos casos. Designar la función de cumplimiento en el Sistema de Administración del Riesgo LA/FT/FP/ADM.

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Primera Línea de Defensa	Las y los servidores públicos con responsabilidades de dirección y/o jefatura de dependencia, políticas, proyectos y/o procesos.	<ul style="list-style-type: none"> Identificar los riesgos de servicios o actividades tercerizados, cuando aplique. Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo, acciones de mejora, planes de manejo, planes de contingencia y de continuidad de las operaciones. Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados, alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo de su proceso. Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles, implementar mejoras si se requieren y reportar en la herramienta disponible. Reportar trimestralmente el estado de la gestión de los riesgos de los procesos de los cuales es responsable en la herramienta o aplicativo disponible, adjuntando los soportes correspondientes, debidamente identificados, para cada actividad.
		<ul style="list-style-type: none"> Procurar que las actividades de control de los riesgos se encuentren documentadas y actualizadas en los procedimientos. Revisar, hacer análisis y atender los informes de evaluación y auditoría para la actualización de los riesgos del proceso Revisar y aprobar el Mapa de Riesgos Los líderes de los procesos deben garantizar el monitoreo permanente de los riesgos, sus controles y acciones a fin de evitar su materialización. Contribuir con el diseño del Sistema de Administración del Riesgo LA/FT/FP/ADM.
Segunda Línea de Defensa	Oficina Asesora de Planeación y las y los Servidores públicos del nivel directivo o asesor, que realizan actividades de supervisión de temas transversales de conformidad con sus funciones y competencias	<ul style="list-style-type: none"> Orientar metodológicamente la gestión del riesgo en su identificación, análisis, valoración, monitoreo, acciones de mejora, planes de manejo, planes de contingencia y de continuidad de las operaciones Brindar orientación para el diseño adecuado y fortalecimiento de los controles establecidos por la primera línea de defensa Presentar al Comité Institucional de Coordinación de Control Interno - CICCI el Mapa de Riesgos institucional

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
		<ul style="list-style-type: none"> Consolidar el mapa de riesgos para su socialización y publicación en la página web. Realizar seguimiento trimestralmente a los riesgos identificados y los controles establecidos por la primera línea de defensa y registrar el resultado a la gestión de los riesgos en el sistema de información o herramienta disponible. Proponer al Comité Institucional de Coordinación de Control Interno, las mejoras a la Política de Gestión Integral del Riesgo de la Secretaría Distrital de Ambiente y los demás instrumentos asociados.
Segunda Línea de Defensa	Oficina de Tecnologías de la Información y la Comunicación	<ul style="list-style-type: none"> Articular con la Oficina Asesora de Planeación la actualización de la política Gestión Integral del Riesgo, incluyendo los lineamientos para la identificación, valoración, tratamiento, monitoreo y revisión de los riesgos de seguridad de la información. Definir lineamientos y asesorar a la primera línea de defensa para la identificación, actualización y revisión de los activos de información asociados a su proceso. Asesorar y acompañar a los procesos en la identificación de riesgos de seguridad de la información en articulación con la Oficina Asesora de Planeación. Realizar la revisión anual de los resultados de la eficacia de la implementación de controles relacionados con seguridad de la información, con el fin de identificar mejoras y establecer planes de trabajo que las subsanen.
Tercera Línea de Defensa	Oficina de Control Interno	<ul style="list-style-type: none"> Llevar a cabo la evaluación independiente a los riesgos registrados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional Coordinador de Control Interno. Para esto tendrá en cuenta los resultados de los seguimientos aplicados por parte de la Segunda Línea de Defensa, a fin de contar con información de base para sus evaluaciones y generar recomendaciones a estas instancias. Generar recomendaciones y/o alertas con alcance preventivo a la línea estratégica, a fin de incorporar acciones inmediatas a los temas críticos identificados.

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
		<ul style="list-style-type: none"> Asesorar y acompañar a toda la Alta Dirección en la incorporación de estrategias y metodologías para la gestión de riesgo, acorde con las actualizaciones en materia de riesgos corrupción, fiscales, de lavado de activos y otros que se definan en normas nacionales.

Fuente: Elaboración propia- SDA

9. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

La metodología establecida en el presente documento se encuentra basada en la Guía para la Gestión Integral del Riesgo en Entidades Públicas - Versión 7 del Departamento Administrativo de la Función Pública (DAFP)

Para Seguridad de la información, se tendrán en cuenta los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas Versión 5 publicado el 21 de abril de 2025 por parte del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC como parte del Modelo de Seguridad y Privacidad de la Información - MSPI.

Teniendo en cuenta que una correcta actuación de los colaboradores de la entidad frente a la administración de riesgos puede aportar al cumplimiento de los objetivos estratégicos institucionales y a la misión de la entidad y que a su vez eviten la materialización del riesgo y ayuden a mitigar las consecuencias ante posibles materializaciones-

La información de la construcción, evaluación y valoración de los riesgos para cada uno de los procesos se registrará en el formato denominado Mapa de Riesgos y se realiza su seguimiento a través de la aplicación de la herramienta tecnológica dispuesta.

9.1. Adopción Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP

A través de la presente política se adopta el SIGRIP orientado a la “prevención, gestión y administración de riesgos de lavado de activos, financiación del terrorismo y proliferación de armas y riesgos de corrupción, incluidos los reportes de operaciones sospechosas a la UIAF, consultas en las listas restrictivas y otras medidas específicas (...)”, en cumplimiento de la Ley 2195 de 2022 (artículo 31).

Este sistema busca prevenir, detectar y corregir los eventos que amenazan el ejercicio íntegro del servicio público (riesgos asociados a Corrupción) o la integridad de la entidad frente a posibles riesgos de lavado de activos, financiación del terrorismo y proliferación de armas, de manera integral.

9.2. Definición roles y responsabilidades para el SIGRIP

En complemento y en articulación con la presente política se definen los siguientes roles y responsabilidades para el adecuado funcionamiento del SIGRIP, en función del esquema de líneas y los roles existentes en el Programa de Transparencia y Ética Pública PTEP diseñado por la entidad:

Tabla 3. Definición roles y responsabilidades para el SIGRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional 1 de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 6.3.7.3	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas v7. 2025

9.3. Niveles de aceptación del riesgo o tolerancia al riesgo

La estrategia para combatir el riesgo (tratamiento), se realizará acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el Comité Institucional de Coordinación de Control Interno de la Secretaría Distrital de Ambiente, los niveles aceptables de desviación, relativa a la consecución de los objetivos asociados a la estrategia, se aplicará de la siguiente manera:

- Riesgos de Gestión, Fiscal y seguridad de la información, se ACEPTA el riesgo en zona de riesgo residual BAJA, no se hace necesario generar acciones complementarias diferentes a los controles ya establecidos, el proceso debe monitorearlo con la periodicidad establecida. Si hay mayor exposición al riesgo, se revalora la probabilidad y el impacto. Si se materializa se proponen acciones de contingencia
- Riesgos del Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP, Ningún riesgo SIGRIP, podrá ser aceptado ni compartido o transferido. Se adoptarán medidas para reducir la probabilidad, el impacto o ambos factores del riesgo. Las medidas de tratamiento contemplan controles, acciones complementarias y medidas de contingencia e investigación ante la materialización del riesgo

10. LINEAMIENTOS GENERALES GESTIÓN PREVENTIVA RIESGOS FISCALES

Con el propósito de identificar y gestionar los riesgos que puedan provocar un daño patrimonial, el cual, en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado, en primer lugar, se identifican los siguientes gestores fiscales (comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores

de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones inciden en la gestión fiscal).

De igual forma, para establecer los procesos donde principalmente se genera una gestión fiscal crítica que exija la identificación, valoración y monitoreo de esta tipología de riesgos.

11. LINEAMIENTOS GENERALES PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Con el propósito de incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y para asegurar los activos de información identificados por la entidad, en cumplimiento del Modelo de Seguridad y Privacidad de la Información desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones (MINTIC), a continuación se establecen los lineamientos para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información.

11.1. Riesgo de seguridad de la información

Se debe tener en cuenta que la política de seguridad digital se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI, con el Modelo Integrado de Planeación y Gestión (MIPG) y con la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas. Este modelo pertenece al habilitador transversal de seguridad y privacidad de la Política, mediante el soporte transversal de los otros habilitadores de la política de gobierno digital, que en la Secretaría Distrital de Ambiente se tiene definido en el Plan Estratégico de Tecnologías de la información-PETI.

El riesgo de seguridad de la información es la 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. Para gestionar cada riesgo de seguridad de la información, hay que acudir también a otras normas, como el ISO 31000:2018 o el ISO/IEC 27005:2022, estas ofrecen un marco de referencia para la identificación, manejo y mitigación de los riesgos.1 ISO/IEC 27001:2022

Para la identificación de los riesgos de seguridad de la información es necesario identificar los activos de información del proceso, teniendo en cuenta los siguientes pasos:

1. Listar los activos (primarios) por proceso: En cada proceso, deberán listarse los activos primarios, indicando algún consecutivo, nombre y descripción breve de cada uno. Para cada activo primario identificado se deberán relacionar los Activos soporte en los cuales está contenido o de los cuales depende cada Activo primario.
2. Identificar el dueño (propietario) de los activos: Los procesos deberán identificar los responsables de cada uno de los activos tanto primarios como de soporte, si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
3. Clasificar los activos de información: Los Activos primarios se deben clasificar en términos de grado de importancia de acuerdo con las necesidades de seguridad de la información, con base en la confidencialidad, integridad, disponibilidad y los requisitos de las partes interesadas, una vez se hayan valorado los Activos primarios, los Activos soporte tomarán el mismo valor, sin embargo, el Activo soporte tomará el mayor valor de los Activos primarios que contiene o con los que tiene relación.

4. Clasificar la información: Realizar la clasificación de la información (Activo primario) conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2022 y demás normatividad aplicable, lo anterior para darle un valor e importancia a cada Activo primario.
5. Determinar la criticidad del activo (Valoración del Activo): Cuando se haya evaluado la criticidad de los activos soporte, se deberán priorizar los activos de mayor valor e importancia en el análisis y gestión de riesgos, teniendo presente esta criticidad.
6. Determinar si existe Infraestructura Crítica Cibernética -ICC: identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC.

Tras realizar la identificación y evaluación de los activos de información, se efectúa la detección de las amenazas y las vulnerabilidades. Con esto definimos los criterios de aceptación de los riesgos de seguridad de la información y se realiza el cálculo de cada uno, considerando el impacto y la probabilidad de ocurrencia. Para finalizar se asignan los propietarios de los riesgos y el plan de tratamiento.

12. MONITOREO Y SEGUIMIENTO DEL RIESGO

Los cortes para el monitoreo y seguimiento del riesgo se realizarán de manera trimestral:

A través de las líneas de defensa se realizarán los monitoreos y seguimientos, los cuales se desarrollarán de la siguiente manera:

- Línea estratégica: en el marco del Comité de Coordinación de Control Interno realizará monitoreo por lo menos 1 vez al año al cumplimiento de la Política de Gestión Integral del Riesgo.
- Primera línea de defensa: Realiza monitoreo trimestral a los controles y acciones tendientes a controlar y gestionar los riesgos, realizando el registro en la herramienta establecida los diez (10) días siguientes a la fecha de corte establecida en cada trimestre.
- Segunda línea de defensa: Realizará seguimiento trimestral a través de los reportes por proceso, asegurando que los controles y acciones implementados por la primera línea de defensa están diseñados apropiadamente y funcionen como se pretende. La segunda línea de defensa realizará el registro en la herramienta establecida los diez (10) días siguientes a la primera línea.
- Tercera línea de defensa: Realizará seguimiento y evaluación semestral, el cual se realizará a través de los reportes de la segunda línea de defensa y solicitudes independientes a la primera línea de defensa, en caso de requerirse, registrándose en la herramienta establecida.

Nota: La aplicación de esta Política entra en vigor a partir del 1° de julio de 2026, previa aprobación del Comité Institucional de Coordinación de Control Interno.

13. MATERIALIZACIÓN DEL RIESGO

En el evento de materializarse un riesgo, es necesario realizar ajustes a los controles o

acciones, tales como se mencionan a continuación:

13.1. Primera línea de defensa

1. Cuando se identifique la materialización de un riesgo de gestión, fiscal o de seguridad de la información, informar oportunamente a la segunda y tercera línea de defensa mediante comunicación oficial interna (memorando), indicando el hecho presentado y sus posibles afectaciones.
2. Activar de manera inmediata el plan de contingencia definido para atender la situación presentada y mitigar sus efectos sobre la operación institucional.
3. Realizar el análisis de causas que originaron la materialización del riesgo, así como la evaluación del impacto generado sobre los objetivos, procesos, recursos o servicios de la entidad.
4. Revisar y actualizar, de ser necesario, la identificación del riesgo, sus controles, causas, consecuencias y acciones de tratamiento, conforme a los resultados del análisis efectuado.
5. Remitir a la segunda y tercera línea de defensa, mediante comunicación oficial interna (memorando), la actualización del riesgo y del mapa de riesgos, debidamente revisada y aprobada por el líder del proceso.
6. Definir e implementar acciones preventivas, correctivas y de mejora orientadas a evitar la recurrencia de la materialización del riesgo y fortalecer la efectividad de los controles establecidos.
7. Cuando se trate de riesgos asociados a la integridad pública, informar de manera inmediata a la Alta Dirección sobre los hechos identificados y, de considerarse procedente, efectuar la denuncia ante los entes de control competentes y poner la situación en conocimiento de la Oficina de Control Disciplinario Interno.
8. En los casos relacionados con riesgos de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), informar de manera inmediata a la Alta Dirección, realizar el reporte de operaciones inusuales y/o sospechosas conforme a los procedimientos internos y efectuar el reporte correspondiente ante la UIAF, así como poner los hechos en conocimiento de la Oficina de Control Disciplinario Interno.

13.2. Segunda línea de defensa

Materialización de riesgos detectada por segunda línea de defensa:

1. Cuando la segunda línea de defensa identifique la materialización de riesgos de gestión, fiscales o de seguridad de la información, deberá comunicar oportunamente el hecho a la Oficina de Control Interno y al líder del proceso correspondiente, para lo de su competencia y con el fin de que se adelanten las acciones de revisión, análisis y tratamiento requeridas.
2. Realizar seguimiento a las acciones implementadas por la primera línea de defensa, verificando la definición de acciones correctivas, preventivas y de mejora, así como la actualización del mapa de riesgos y de los controles asociados.
3. Acompañar metodológicamente a la primera línea de defensa en la revisión y ajuste de los riesgos, sus causas, controles y acciones de tratamiento, conforme a los lineamientos institucionales de administración del riesgo.
4. Cuando se identifiquen riesgos asociados a la integridad pública, incluyendo aquellos relacionados con Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), la segunda línea de defensa deberá comunicar de manera inmediata el hecho a la Oficina de Control Interno,

a la Oficina de Control Disciplinario Interno y al líder del proceso correspondiente, para lo de su competencia y para la implementación de las acciones de revisión, análisis y tratamiento requeridas.

5. En los casos relacionados con riesgos LA/FT/FPADM, se deberá verificar que se efectúe el reporte de operaciones inusuales y/o sospechosas conforme a los procedimientos internos establecidos y el correspondiente reporte ante la UIAF, así como la actualización del mapa de riesgos y la adopción de las acciones de mejora correspondientes.

13.3. Tercera línea de defensa

Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa):

1. Cuando se identifique la materialización de riesgos de gestión, fiscales o de seguridad de la información, la tercera línea de defensa deberá informar oportunamente al líder del proceso sobre el hecho detectado y orientarlo frente a la revisión, análisis y definición de las acciones requeridas para atender la situación presentada.
2. Verificar que la primera y segunda línea de defensa adelanten las acciones correctivas, preventivas y de mejora correspondientes, así como la actualización del mapa de riesgos y de los controles asociados.
3. Presentar al Comité Institucional de Coordinación de Control Interno los hechos identificados, las acciones implementadas y las actualizaciones efectuadas al mapa de riesgos, para el análisis y toma de decisiones correspondientes.
4. Cuando se trate de riesgos asociados a la integridad pública, informar de manera inmediata al representante legal y a la Oficina de Control Disciplinario Interno sobre los hechos detectados y convocar al Comité Institucional de Coordinación de Control Interno para el análisis de la situación y la definición de las acciones institucionales a seguir.
5. Dependiendo del alcance y de la normativa aplicable al hecho identificado, promover la remisión de la información y/o la denuncia ante los entes de control competentes.
6. Facilitar y verificar el desarrollo de las acciones requeridas por parte del líder del proceso para la revisión y ajuste del mapa de riesgos, sus controles y acciones de tratamiento, realizando seguimiento a la implementación de las medidas definidas.
7. Cuando se identifiquen riesgos relacionados con Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FPADM), comunicar de manera inmediata los hechos a la Oficina de Control Disciplinario Interno, a la Alta Dirección y al líder del proceso correspondiente, para lo de su competencia y la adopción de las acciones requeridas.
8. En los casos relacionados con riesgos LA/FT/FPADM, verificar que se efectúe el reporte de operaciones inusuales y/o sospechosas conforme a los procedimientos internos establecidos y el correspondiente reporte ante la UIAF, así como la actualización del mapa de riesgos y la implementación de las acciones de mejora correspondientes.

13.4. Línea estratégica

1. Analizar los hechos y las causas asociadas a la materialización de los riesgos informados por las líneas de defensa, con el fin de evaluar su impacto institucional y determinar las decisiones y acciones a seguir.
2. Definir y orientar las acciones institucionales requeridas para la atención de los hechos identificados, incluyendo el inicio de las actuaciones administrativas, disciplinarias o de mejora que correspondan.

3. Realizar seguimiento a las decisiones adoptadas y a la implementación de las acciones definidas para el tratamiento de la materialización de los riesgos y el fortalecimiento de los controles institucionales.
4. Cuando la situación lo amerite y de conformidad con la normatividad vigente, promover o efectuar la remisión de la información y/o la denuncia ante los entes de control competentes.

14. DIRECTRICES GENERALES DE LA DEBIDA DILIGENCIA

La debida diligencia es la identificación de la persona natural o jurídica que celebra el contrato, identificación del beneficiario final, objetivo del contrato estatal e identificación de fuentes de fondos, perfil de riesgo y actividad comercial.

En el marco del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, se debe desarrollar el principio de debida diligencia en todas las interacciones con contrapartes, en las que exista una exposición a riesgos para la integridad pública, es decir, en aquellas interacciones en que se haya identificado un riesgo de soborno, fraude, inadecuada gestión de conflicto de intereses; Corrupción, Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva.

Este principio debe aplicarse en concordancia con el principio de razonabilidad utilizando mecanismos adecuados para los fines que persigue y necesarios para alcanzarlos, y el principio de proporcionalidad utilizando mecanismos se aplique desde un enfoque basado en riesgos.

15. REVISIÓN Y DETECCIÓN DE OPERACIONES SOSPECHOSAS DE LA/FT/FP

La revisión y detección de operaciones sospechosas tiene como finalidad identificar las actividades, hechos y operaciones, que por sus características no son razonables respecto de una actividad económica o sector y que las hace sospechosas. Con el propósito de generar un ambiente de detección, la entidad debe definir mecanismos específicos para dar cumplimiento a las medidas aquí sugeridas con las siguientes acciones:

Comprobar
 Supervisar
 Observar críticamente
 Registrar los procesos derivados de una nueva actividad, acción o sistema

En un primer nivel, ello permite identificar las operaciones inusuales que fueron generadas en el proceso de monitoreo respecto del control detectivo y que sugieren ser evaluadas.

Es decir, se debe detectar las operaciones inusuales con base en el registro de usuarios o clientes, Personas Públicamente Expuestas (PEP's) proveedores y la existencia de cambios atípicos en las operaciones como los montos y el número de transacciones relacionadas con los productos, bienes o servicios ofrecidos por la entidad distrital.

Detectadas las operaciones inusuales, se analizan y se determinan los criterios objetivos que le otorgan características sospechosas de LA/FT/FP catalogados como importantes y significativas por su grado de complejidad, debido a que se salen de los patrones habituales sin fundamento a fin de remitirle a la UIAF de manera oportuna

16. COMPROMISO ANTISOBORNO Y ANTIFRAUDE

La secretaría Distrital de Ambiente, buscando una gestión transparente y eficaz se compromete a adoptar prácticas de buen gobierno que permitan prevenir y detectar potenciales situaciones de soborno, fraude y conductas irregulares en el accionar de la institución.

Del mismo modo, cada una de las actividades, planes y programas emprendidos se realizarán en el marco de los valores y la integridad aplicados en el código de integridad de la entidad, cumpliendo además los lineamientos y leyes antisoborno, anticorrupción y antifraude.

a. Desarrollo de la política

La política antisoborno y antifraude son parte integral del plan anticorrupción y de atención al ciudadano de la entidad, y se encuentra articulada con el código de integridad, documentos que generan estrategias y actividades encaminadas a la lucha contra la corrupción y la transparencia en las actuaciones de los colaboradores de la entidad.

Frente a la lucha contra la corrupción y cero tolerancias de actos de soborno y fraude la entidad se compromete a:

Gestionar los riesgos de corrupción y sobornos asociados a actividades relacionadas con la misionalidad y que tenga vinculación con terceros.

- Contar con controles internos que permitan la mitigación o la detección de actividades que ponen en riesgo las buenas conductas y el buen accionar de la entidad.
- Promover una cultura de integridad basada en la prevención, mitigación y tratamiento de posibles riesgos de corrupción y soborno.
- Evitar cualquier conducta que pueda afectar el desarrollo transparente de su misionalidad. Proteger a los servidores públicos, contratistas y/o grupos de interés, ante cualquier represalia, como consecuencia de denuncias por prácticas que constituyan soborno
- Garantizar la confidencialidad de los datos de quien reporte hechos de corrupción.
- Proteger la identidad de los informantes y de las personas que participan en la denuncia.

b. Conductas indebidas

Se incluyen, sin limitarse a ellas, las siguientes conductas como constitutivas de soborno, cuando estas conductas se presenten asociadas a una contraprestación indebida:

- Modificación de una base de datos.
- Entrega de información confidencial.
- Modificar actos administrativos en beneficio de un particular.

- Facilitar la adjudicación de un contrato a un particular.
- Desembolsos fuera del programa.
- Priorizar vías sin el cumplimiento del modelo de priorización
- Direccionar las condiciones de contratación.
- Pérdida injustificada de expedientes o pérdida de documentos dentro de un expediente.
- Recibir documentos a la mano y cambiarlos dentro un expediente.

Por otro lado, esta política debe ir plenamente articulada con el lineamiento impartido por la entidad en lo que refiere a conflicto de intereses, siendo que las actuaciones fraudulentas o corruptas son una característica principal del conflicto de intereses y se articula con esta política.

A continuación, se expone la metodología a aplicar en esta política:

1. Identificar puntos críticos: Actividades en donde se concentre la gestión administrativa, contractual y presupuestal en las que visiblemente se pueda dar una contraprestación del servicio y pueda terminar gestándose un soborno.
2. De acuerdo con la guía de lineamientos antisoborno para el Distrito Capital de la Veeduría Distrital, los procesos o dependencias que se muestran como puntos críticos son:

- Contratación: “La gestión contractual es, indudablemente, el punto más crítico de soborno en las entidades públicas”.

“En procesos de contratación en donde se destinan altos rubros de presupuesto, existe el riesgo que individuos interesados en obtener la adjudicación de estos contratos ofrezcan sobornos o dadas en las entidades públicas, con el fin de ser quienes reciban el contrato.

Incluso, el soborno puede presentarse para manipular el proceso desde su etapa previa, de manera que un único oferente reciba la adjudicación a través de propuestas o licitaciones “hechas a la medida” de ese oferente”.

- Talento humano: “la provisión de cargos provisionales y de libre nombramiento y remoción, así como contratos de prestación de servicios de manera irregular por favoritismos o retribuciones lleva a una prestación ineficiente del servicio público y por ende a una disminución en la competitividad”.
- Control Interno: “El control interno de gestión supone entonces la eficiencia, eficacia y transparencia en el ejercicio de las funciones de las entidades que conforman el Estado colombiano (DAFP, 2017a. p. 4), lo cual involucra procesos administrativos de la entidad como la contratación, compras, adquisiciones y préstamos.

Los funcionarios encargados de esta labor se ven también expuestos a riesgos de soborno, en tanto pueden ser objeto de ofrecimientos guiados a obviar labores de control propias de su función.

Es así como el soborno puede generar deficiencias en el control de los procesos administrativos, lo cual resultaría también en una pérdida de eficiencia en la prestación de servicios por parte de la entidad pública”.

Este ejercicio de identificación debe articularse con el mapa de riesgos de corrupción formulado por la entidad, en el caso de la SFA es importante verificar los procesos misionales, especialmente en la etapa de contratación y adquisición de insumos, maquinaria, personal y equipos necesarios para dar cumplimiento a la misionalidad de la entidad.

c. **Gestión del riesgo de corrupción, soborno y antifraude**

La Oficina Asesora de Planeación en coordinación con los procesos realizará el mapa de riesgos, de tal manera que se articulen a los mapas de riesgos de integridad, se formalicen, aprueben, se identifiquen, traten y controlen en el marco de la metodología sugerida aquí aprobada.

17. VIGENCIA

La presente Política de Gestión Integral del Riesgo entrará en vigor a partir de su aprobación por el Comité Institucional de Coordinación de Control Interno y será revisada cada dos (2) años o antes, si el marco normativo o institucional lo requiere.

HISTORIAL DE CAMBIOS		
VERSIÓN	FECHA	RAZÓN DEL CAMBIO
1	10/Jul/2026	<p>Política aprobada mediante acta del Comité Institucional de Coordinación de Control Interno del 25 de junio de 2026. En el marco de la adopción del Mapa de Procesos versión 7 y de la unificación del proceso de Direccionamiento Estratégico con el proceso Sistema Integrado de Gestión, se acoge el presente documento en el proceso de Direccionamiento Estratégico en versión 1. Esta actualización incorpora, la modificación integral del documento basada en la “Guía para la Gestión Integral del Riesgo en Entidades Públicas V7 emitida por el DAFP, se incluye sección de vigencia, actualización normativa, se amplía alcance a terceros, incluye seguimiento obligatorio y roles más explícitos, se incorpora la denominación de riesgos de integridad pública como categoría explícita, la segunda línea de defensa pasa a la Oficina Asesora de Planeación, se reordenan sus capítulos, se refuerzan las etapas, fechas de seguimiento, materialización del riesgo y mejora la claridad metodológica. Adicionalmente de modifica el nombre pasando de: “Política de administración del riesgo” a “Política de Gestión Integral de Riesgos”. Finalmente, en atención a la activación automática de la codificación en Isolución, el código de este documento cambia de PE03-PO01 a DE-PO-001.</p>

ELABORÓ	REVISÓ	APROBÓ
Nombre: Dora Cristina Suárez Macías Cargo: Contratista Fecha: 10/Jul/2026	Nombre: Andrés Felipe Rojas Castiblanco Cargo: Contratista Fecha: 10/Jul/2026 Nombre: Claudia Milena Gordillo Rodríguez Cargo: Jefe Oficina Asesora de Planeación Fecha: 10/Jul/2026	Nombre: Claudia Milena Gordillo Rodríguez Cargo: Jefe Oficina Asesora de Planeación Fecha: 10/Jul/2026

COPIA CONTROLADA