POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

PROCESO:

SISTEMA INTEGRADO DE GESTIÓN

VERSIÓN: 7

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE AMBIENTE
BOGOTÁ

TABLA DE CONTENIDO

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.

Teniendo en cuenta que la administración del riesgo es estratégica para el logro de los objetivos institucionales y de procesos, en este documento se enuncia la política marco de acción que permitirá tomar decisiones relativas a la administración del riesgo, el cual está alineado y armonizado con el Modelo Integrado de Planeación y Gestión MIPG y la Guía para la Gestión del Riesgo establecida por el Departamento Administrativo de la Función Pública.

Es así, como la Secretaría Distrital de Ambiente - SDA, define la Política de Administración del Riesgo para la identificación, el tratamiento, manejo, seguimiento y evaluación de los riesgos que afectan el logro de los objetivos institucionales y asegurar una gestión pública eficaz, atendiendo los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión (MIPG), la *"Guía para la Administración del riesgo y el diseño de controles en entidades públicas"* del DAFP Versión 6, la "*Guía Estrategias para la Construcción del Programa de Transparencia y Ética Pública", antiguo PAAC;* con el propósito de articularla a las demás normas y políticas aplicables a la Secretaría y a los objetivos estratégicos de la entidad gestionándolos en un nivel aceptable.

A su vez, en atención a la "Ruta Metodológica para la implementación del SARLAFT en las Entidades Distritales" emitida por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. la cual indica que las entidades privadas o públicas de índole nacional o territorial deben diseñar sistemas de administración de riesgos que les permita protegerse ante el riesgo asociado al lavado de activos (LA) y Financiación del Terrorismo (FT) y de esta forma dar cumplimiento a las obligaciones que se establecen en la normatividad vigente. Lo anterior, para evitar que sean utilizadas en el proceso de lavado de activos y financiación del terrorismo. Así entonces, la entidad se acoge a la recomendación como buena práctica para asociar y articularlos con los riesgos de gestión, los criterios para la identificación, análisis y evaluación de riesgos asociados a LA/ FT.

Se requiere del compromiso a todo nivel iniciando por la autoridad de la entidad, el equipo directivo y todos sus servidores, para el cumplimiento efectivo y eficiente del sistema SARLAFT.

2 OBJETIVO

Definir los lineamientos para la administración del riesgo de la Secretaría Distrital de Ambiente-SDA, a través de la implementación de mecanismos y herramientas que permitan la identificación, tratamiento, manejo, seguimiento y evaluación de los riesgos, así como la asignación de roles y responsabilidades de cada uno de los servidores y contratistas de prestación de servicios de la Entidad (esquema de las líneas de defensa), con el fin de contribuir al cumplimiento de la misión y al logro de los objetivos institucionales.

3 ALCANCE

La Política de Administración del Riesgo inicia con la identificación y definición de términos clave para abordar el texto, continua con la metodología establecida al interior de la entidad para la administración del riesgo, incluida la comunicación, monitoreo, responsables (líneas de defensa) y finaliza con las acciones pertinentes para abordar un riesgo, cuando se materializa.

La Política de Administración del Riesgo es aplicable a todos los procesos (estratégicos, misionales, de apoyo y de evaluación) del modelo de operación por procesos de la Secretaría Distrital de Ambiente.

4 NORMATIVIDAD

NORMA	DESCRIPCIÓN
Constitución Política de Colombia de 4 de julio de 1991	Adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno.
Ley 87 del 29 de noviembre 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 del 06 de junio 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 526 del 17 de agosto de 1999	Por medio de la cual se crea la unidad de información y análisis financiero.
Ley 610 del 15 de agosto de 2000	Por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías. Función Pública. Modificada y adicionada por el Decreto ley 403 de 2020.
Ley 1108 del 27 de diciembre de 2006	Por medio de la cual se aprueba la “Convención Interamericana Contra el Terrorismo”.
Ley 1121 de 2006 del 29 de diciembre de 2006	Por medio de la cual se dictan normas para prevención, investigación y sanción de la Financiación del Terrorismo y otras disposiciones.
Ley 1453 del 24 de junio de 2011	Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1474 del 12 de julio de 2011	Estatuto Anticorrupción.
Ley 1573 del 02 de agosto de 2012	Por medio de la cual se aprueba la convención para combatir el cohecho de servidores públicos extranjeros en transacciones comerciales internacionales.

NORMA	DESCRIPCIÓN
Ley 1708 del 20 de enero de 2014	Por medio de la cual se expide el Código de Extinción de Dominio.
Ley 1712 del 06 de marzo 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 1753 del 9 de junio de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país". Artículo 133. "Integra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998)".
Ley 1762 del 6 de julio de 2015	Por medio de la cual se adoptan instrumentos para prevenir, controlar y sancionar el contrabando, el lavado de activos y la evasión fiscal.
Ley 1778 del 02 de febrero de 2016	Por la cual se dictan normas sobre la responsabilidad de las personas jurídicas por actos de corrupción transnacional y se dictan otras disposiciones en materia de lucha contra la corrupción.
Ley 1819 del 29 de diciembre de 2016	Por medio de la cual se adopta una reforma tributaria estructural, se fortalecen los mecanismos para la lucha contra la evasión y la elusión fiscal, y se dictan otras disposiciones.
Ley 1849 del 19 de Julio de 2017	Por medio de la cual se modifica y adiciona la Ley 1708 de 2014 "Código de Extinción de Dominio" y se dictan otras disposiciones.
Ley 2195 del 18 de enero 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 1964 del 22 de septiembre de 1998	Por el cual se reglamenta el Parágrafo Primero del artículo 40 de la Ley 190 de 1995.
Decreto Nacional 3420 del 20 de octubre de 2004	Por el cual se modifica la composición y funciones de la Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos y se dictan otras disposiciones.
Decreto Nacional 1083 de 26 de mayo de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. (titulo 21)
Decreto Nacional 1499 del 11 de septiembre de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del 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. 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.

NORMA	DESCRIPCIÓN
Decreto Nacional 403 del 16 de marzo de 2020	Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
Decreto Distrital 221 del 6 de junio de 2023	Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones.
Resolución SDA 1017 del 15 junio de 2023	Por la cual se conforma el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Ambiente y se dictan otras disposiciones.
Circular 22 de Superintendencia Financiera, del 19 de abril 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, del 22 de diciembre 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 del 2 de septiembre de 2020	Instrucciones relativas a la administración del riesgo de lavado de activos y de financiación del terrorismo.

5 TÉRMINOS Y DEFINICIONES

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. (1)

AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. (ISO 27000:2013)

APETITO AL RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. (1)

ÁREAS DE IMPACTO: consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional. (1)

BIEN PÚBLICO: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.

b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc. (1)

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección que no sería posible el logro de los objetivos de la Entidad. (1)

CAUSA: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (1)

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

Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata (1)

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

Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño. (1)

CONFIDENCIALIDAD: Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (1)

La confidencialidad, cuando nos referimos a sistemas de información, permite a los usuarios autorizados acceder a datos confidenciales y protegidos. Existen mecanismos específicos garantizan la confidencialidad y salvaguardan los datos de intrusos no deseados o que van a causar daño. (1)

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.

Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos. (1)

CONTROL: Medida que permite reducir o mitigar un riesgo. (1)

CONTROL FISCAL INTERNO (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. (1)

CONTROL FISCAL MULTINIVEL: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación del control social. (1)

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada La disponibilidad, en el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto. (ISO 27000)

EVENTO: Riesgo materializado. Los eventos de riesgo son aquellos incidentes que generan o podrían generar pérdidas a la entidad. (1)

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.
Pueden ser: Procesos, Talento Humano, Tecnología, Infraestructura y Eventos externos (Terceros). (1)

FINANCIACIÓN DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA – FPADM: Todo acto que provea fondos o utilice servicios financieros, en todo o en parte, para la fabricación, adquisición, posesión, desarrollo, exportación, trasiego de material, fraccionamiento, transporte, transferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable (UNODC, 2021). (2)

FINANCIACIÓN DEL TERRORISMO (FT): La financiación del terrorismo está relacionada con los fondos, bienes o recursos a los que acceden las organizaciones terroristas o los terroristas para poder costear sus actividades (UIAF, 2013). (2)

GAFI: el Grupo de Acción Financiera Internacional (GAFI) es un ente intergubernamental establecido en 1989, cuyo objetivo es fijar estándares y promover la implementación efectiva de medidas legales, regulatorias y operativas para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, y otras amenazas a la integridad del sistema financiero internacional (UIAF, 2013). (2)

GESTOR PÚBLICO: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales". A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos. (1)

GESTIÓN DEL RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. La gestión de riesgos no es estática, se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana. (1)

GESTIÓN DEL RIESGO DE DESASTRES: Es el proceso social de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia de este, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe para prepararse y manejar las situaciones de desastre, así como para la posterior recuperación, entiéndase: rehabilitación y reconstrucción. Estas acciones tienen el propósito explícito de contribuir a la seguridad, el bienestar y la calidad de vida de las personas y al desarrollo sostenible. (Artículo 4° LEY 1523 DE 2012)

GESTIÓN DEL RIESGO FISCAL: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial). (1)

GESTOR FISCAL: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)4 ” . A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista (1)

IMPACTO: Las consecuencias que puede ocasionar a la organización la materialización del riesgo. (1)

INTEGRIDAD: Propiedad de la exactitud y la integridad (1)

INTERESES PATRIMONIALES DE NATURALEZA PÚBLICA: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

Ejemplos: Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal. (1)

Son todos los bienes, recursos y derechos susceptibles de valoración económica cuya titularidad corresponda a una entidad pública, y del carácter ampliamente comprensivo y genérico de la

expresión, que se orienta a conseguir una completa protección del patrimonio público (C-340-07 Corte Constitucional de Colombia)

LA/FT/FPADM Lavado de Activos, Financiamiento del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva (2)

LAVADO DE ACTIVOS (LA): El lavado de activos es un delito que consiste en dar una apariencia lícita o de legalidad a bienes, dinerarios o no, que en realidad son productos o "ganancias" de delitos como tráfico ilícito de drogas, trata de personas, corrupción, secuestros y otros (UNODC, 2021). (2)

MODELO DE TRES LÍNEAS DE DEFENSA (3LD): Realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de toda la organización.

I. Línea Estratégica Este nivel define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.
II. 1ª Línea de Defensa: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
III. 2ª Línea de Defensa: Asegura que los controles y procesos de gestión del riesgo implementado por la 1ª Línea de Defensa, estén diseñados apropiadamente y funcionen como se pretende.
IV. 3ª Línea de Defensa: Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. (1)

NIVEL DE RIESGO: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo es Probabilidad 1 Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto. (1)

PATRIMONIO PÚBLICO: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07)

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. (1)

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. (1)

PROGRAMA DE TRANSPARENCIA Y ÉTICA PÚBLICA: Programa que busca promover la cultura de legalidad y fortalecer el control del riesgo de corrupción, dándole tratamiento sistemático para identificar, medir, controlar y monitorear constantemente dicho riesgo, con el objetivo de incorporar en las entidades públicas un sistema integral de riesgos de corrupción. Igualmente, dichos Programas incluirán las acciones que las entidades adelanten para fortalecer su relación con la ciudadanía en desarrollo de la política pública de Estado Abierto (artículo 31 de la Ley 2195 del 18 de enero de 2022)

PUNTOS DE RIESGO: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales. Para facilitar el ejercicio de identificación de puntos de riesgo (1)

RECURSOS PÚBLICOS: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares (1)

Son los recursos que obtiene el sector público por concepto de impuestos, derechos, productos y aprovechamientos; ingresos derivados de la venta de bienes y servicios; e ingresos por financiamiento interno y externo. (https://www.minhacienda.gov.co/webcenter/portal/AtencionPublico/pages_glosario)

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. (1)

RIESGO DE CORRUPCIÒN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. (1)

RIESGO DEL LA/FT- FPADM: Es la posibilidad de pérdida o daño económico o reputacional que puede sufrir una persona natural o jurídica, al ser utilizada para el lavado de activos, financiación del terrorismo o de la proliferación de armas de destrucción masiva (DIAN, s.f.). (2)

RIESGO DE SEGURIDAD DE LA INFORMACIÒN: 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).

RIESGO FISCAL: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial. (1)

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. (1)

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente. (1)

ROS: Reporte de Operaciones Sospechosas. Es la comunicación mediante la cual los sujetos obligados reportan cualquier hecho u operación con independencia de su cuantía, por hechos o situaciones que posiblemente están relacionadas con el lavado de activos o la financiación del terrorismo. No se requiere la certeza de tales situaciones para efectuar el reporte correspondiente. El ROS no constituye denuncia penal y es absolutamente reservado conforme a la Ley. Debe ser reportado a la UIAF (Unidad de Información y Análisis Financiero). (2)

SISTEMA DE ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y DE LA FINANCIACIÓN DEL TERRORISMO (SARLAFT): Es un sistema pensado en consonancia con los estándares internacionales proferidos por el Grupo de Acción Financiera Internacional (GAFI), y fue expedido en el 2008 por la Superintendencia Financiera de Colombia (SFC), como base para que otras entidades de supervisión y reguladores emitieran normas referentes a esta materia.
Los requisitos establecidos para el SARLAFT se rigen por la circular 027 de 2020 expedida por la Superintendencia Financiera de Colombia, que otorgó el nombre al sistema de SARLAFT 4.0, el cual cuenta con unas actualizaciones normativas en cuanto a aspectos tales como: gestión de nuevos factores de riesgo, validación de nuevas listas vinculantes y mayor precisión en cuando al conocimiento del beneficiario final, entre otros. (2)

TOLERANCIA DEL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. (1)

UIAF: Unidad de Información y Análisis Financiero. Es una unidad administrativa especial del Estado colombiano, con personería jurídica, autonomía administrativa y financiera, de carácter técnico, adscrita al Ministerio de Hacienda y Crédito Público. Es el órgano de inteligencia financiera del país, creado por la Ley 526 de 1999 y reglamentado parcialmente por el Decreto Nacional 1497 de 2002, compilado en el Decreto 1068 de 2015, con el fin de prevenir, detectar y luchar contra el lavado de activos y la financiación del terrorismo (2)

VULNERABILIDAD: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas. (1)

(1) Fuente: definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.
(2) Fuente: Documento Técnico "Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital".

6 RESPONSABILIDAD Y AUTORIDAD

Los roles y responsabilidades para la Administración del Riesgo por procesos, definidos en la Entidad, son las siguientes:

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Secretario (a) Distrital de Ambiente Comité Institucional de Coordinación de Control Interno Comité Institucional de Gestión y Desempeño	• Aprobar la Política de Administración 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. • 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. • Realizar monitoreo y análisis periódico a los riesgos institucionales y solicitar las actualizaciones correspondientes cuando las situaciones del entorno interno y externo lo ameriten. • 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 el Mapa de Riesgos consolidado • Revisar los informes presentados por lo menos cada cuatrimestre 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. • Solicitar las intervenciones e informes necesarios a las diferentes dependencias con el fin de facilitar la toma de decisiones. • Definir las líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. • Revisar los informes presentados por la segunda y tercera línea en lo relacionado a la materialización de riesgos en la entidad, así como la ejecución de los planes de acción establecidos para estos casos. • Aprobar el plan de tratamiento de riesgos de seguridad de la información. • Designar el equipo encargado del Sistema de Administración del Riesgo LA/FT/FPADM. • Aprobar el manual que desarrolla el Sistema de Administración del Riesgo LA/FT/FPADM.
Primera Línea de Defensa	Líderes de procesos, de programas, de	• Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
	proyectos y sus equipos de trabajo.	• 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 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 cuatrimestralmente 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. • Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando. • Formular los planes de manejo y de contingencia e implementarlos cuando se materialicen riesgos para asegurar la continuidad de las operaciones y reducir el impacto. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Revisar y hacer análisis y atención de los informes de evaluación y auditoria 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/FPADM y el Manual de Procedimientos.

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda Línea de Defensa	Subsecretario (a) General	• Asesorar y orientar a los responsables de procesos en el análisis del contexto interno y externo en coordinación con la tercera línea de defensa. • Asesorar y orientar a los responsables de procesos en la identificación, análisis y valoración del riesgo, así como en la aplicación de técnicas y metodologías de análisis e identificación en coordinación con la tercera línea de defensa. • Establecer directrices y lineamientos que faciliten la identificación, el análisis, la evaluación, el tratamiento de los riesgos. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos. • Consolidar el mapa de riesgos para su socialización y publicación en la página web. • Monitorear las actividades de control establecidas para la mitigación de los riesgos de los procesos verificando que se encuentren documentadas y actualizadas en los procedimientos. • Monitorear cuatrimestralmente 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, generando un informe del resultado para la primera y tercera línea de defensa, así como a la línea estratégica. • Proponer al Comité Institucional de Coordinación de Control Interno, las mejoras a la Política de Administración del Riesgo de la Secretaría Distrital de Ambiente y los demás instrumentos asociados. • Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento de los objetivos. • Verificar el análisis y atención de los informes de evaluación y auditoria para la actualización de los riesgos del proceso realizado por la primera línea de defensa. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Trabajar de manera coordinada con la Oficina de Control Interno, en el fortalecimiento del Sistema de Control Interno. • Establecer los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).

Línea de Defensa	Responsable	Responsabilidad frente al riesgo
		• Presentar para aprobación del Comité Institucional de Coordinación de Control Interno – CICCI la Política de Administración del Riesgo. • Presentar al CICCI el Mapa de Riesgos institucional
Tercera Línea de Defensa	Oficina de Control Interno	• Asesorar a la Secretaría Distrital de Ambiente acerca de las metodologías, herramientas y técnicas para la identificación y administración de los riesgos y controles en coordinación con la segunda línea de defensa. • Identificar y evaluar cambios que podrían tener impacto significativo en el sistema de control interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna. • Llevar a cabo la evaluación independiente de la gestión de los riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno CICCI y publicarlos en el sitio web. • Promover ejercicios de autocontrol para que cada proceso monitoree los niveles de eficiencia, eficacia y efectividad de los controles. • Proporcionar evaluación objetiva sobre la eficacia de la gestión del riesgo y control en todas sus etapas, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Revisar cuatrimestralmente el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos y registrar el resultado del seguimiento a la gestión de los riesgos en el sistema de información o herramienta disponible. • Revisar de manera independiente la adecuada definición y desdoblamiento de los objetivos estratégicos a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción.

Fuente: Elaboración propia, Secretaría General- SDA

7 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 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:

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de tratamiento
Riesgos de Gestión, Fiscal y de Seguridad Digital	Bajo	Se **ACEPTA** el riesgo, el proceso los monitorea una vez al año. Si hay mayor exposición al riesgo, se revalora la probabilidad y el impacto. Si se materializa se proponen acciones de contingencia inmediatas.
	Moderado	Se establecen mecanismos de control y acciones complementarias para **REDUCIR,** la probabilidad o el impacto de ocurrencia del riesgo. El proceso evalúa la posibilidad de sustituir las actividades que dan origen al riesgo o se diseñan y aplican otros controles. Se define un plan de contingencia ante la materialización que garantice la continuidad de las operaciones.
	Alto	
	Extremo	
Riesgos de Corrupción y LA/FT- FPADM	Moderada	Ningún riesgo de corrupción y de LA/FT- FPADM, 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.
	Alta	
	Extrema	

Fuente: Elaboración propia, Secretaría General- SDA

8 METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

La metodología para la gestión del riesgo está acorde con los lineamientos que entrega el Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.0, publicada en noviembre de 2022.

A partir de lo anterior y teniendo en cuenta que el adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, se establecieron las siguientes etapas que aseguran la mitigación de los riesgos:

8.1 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La Secretaría Distrital de Ambiente, se compromete a identificar y gestionar de manera efectiva los riesgos de gestión, corrupción, seguridad de la información y lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva - LA/FT-FPADM; en los procesos estratégicos, misionales, de apoyo y de control y 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.

Para el cumplimiento de esta política, la Entidad ha dispuesto de un software como herramienta para el desarrollo de la metodología de riesgos, denominado ISOLUCION, este aplicativo en sus módulos de riesgos permite y facilita la implementación del sistema de administración de riesgos en todos los niveles de la entidad, para acceder a esta opción se debe seguir la ruta: Riesgos DAFP V5/Administración/Riesgos o Riesgos Corrupción /Administración/Riesgos.

8.2 RIESGO DE GESTIÓN

8.2.1 Identificación del Riesgo de Gestión

- Análisis de objetivos estratégicos y de los procesos:

Análisis de objetivos estratégicos	Análisis de objetivos del proceso
La entidad debe analizar los objetivos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso	Los objetivos de los procesos deben estar alineados con los objetivos estratégicos, así como de su misión y visión

Fuente: Elaboración propia, Secretaría General- SDA

- Área de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la Secretaría Distrital de Ambiente en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, para algunos riesgos puede presentarse que la afectación sea de tipo económica y reputacional a la vez.

- Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea de fácil entendimiento tanto para el líder del proceso como para personas ajenas al proceso.

Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

RIESGO (Lo que puede ocurrir) **Es la suma de**
¿QUÉ? Impacto
¿CÓMO? Causa inmediata
¿POR QUÉ? Causa Raíz

Ejemplo:
Posibilidad de afectación reputaciones debido a la desarticulación, inoportunidad y desacierto en la implementación de lineamientos e instrumentos asociados al mantenimiento y mejora del SIG-MIPG, por el desconocimiento de la normativa vigente objetivos y metas institucionales relacionadas.

Fuente: definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6. .

- Clasificación del riesgo

Permite agrupar los riesgos identificados, los cuales se clasifican en las siguientes categorías:

Categoría	Definición
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales están involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

8.2.2 Valoración del Riesgo de Gestión

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia e impacto, con el fin de estimar la zona del riesgo inicial (RIESGO INHERENTE).

- **Tabla de probabilidad**:

Teniendo en cuenta el nivel de probabilidad, la exposición al riesgo estará asociado al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, la cual se describe en la siguiente tabla, que establece los criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta de 501 a 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6

Para el ejemplo de riesgo:

"Posibilidad de afectación reputacional debido a la desarticulación, inoportunidad y desacierto en la implementación de lineamientos e instrumentos asociados al mantenimiento y mejora del SIG-MIPG, por el desconocimiento de la normativa vigente objetivos y metas institucionales relacionadas"

Se define la probabilidad de: media, debido a que la actividad de implementar lineamientos e instrumentos asociados al mantenimiento y mejora del SIG-MIPG es una actividad que se realiza de manera diaria.

- **Tabla de impacto**:

Los criterios para determinar el impacto se realizan conforme a dos variables principales: impactos económicos relacionados con afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, entre otros, e impactos reputacionales entendidos como la afectación a la imagen institucional.

En esta tabla se definen los impactos económicos y reputacionales como las variables principales, y cuando se presenten ambos impactos para un riesgo, con diferentes niveles, se debe tomar el nivel más alto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, desconocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderada 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.

	Afectación Económica	Reputacional
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional ,con efecto publicitario sostenido a nivel país

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6

Para el ejemplo de riesgo:

"Posibilidad de afectación reputacional debido a la desarticulación, inoportunidad y desacierto en la implementación de lineamientos e instrumentos asociados al mantenimiento y mejora del SIG-MIPG, por el desconocimiento de la normativa vigente objetivos y metas institucionales relacionadas"

Se define el impacto como menor 40%, debido a que la actividad de implementar lineamientos e instrumentos asociados al mantenimiento y mejora del SIG-MIPG, afecta la imagen de la entidad internamente, desconocimiento general nivel interno, de la Alta Dirección y/o de proveedores.

- **Valoración del riesgo**

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Se determinan los niveles de severidad a través de la combinación entre la probabilidad y el impacto y se establecen 4 zonas de severidad, que se muestran en la siguiente matriz de calor

		Impacto				
Probabilidad	Muy Alta 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy Baja 20%					
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6

8.2.3 Valoración de Controles del Riesgo de Gestión

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso si aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo
- Estructura para la descripción del control: Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración, la estructura es la siguiente:

Control: Es la suma de
Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
Acción: Se determina mediante verbos que indican la acción que deben realizar como parte del control.
Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.
Ejemplo: Los profesionales del equipo SIG verifican la normativa relacionada con la implementación, seguimiento y mejora del SIG-MIPG a través de consulta en las páginas web de los entes que regulan el tema a nivel nacional y distrital, que se verá reflejado en nomograma del proceso cuando se requiera.

Fuente: Definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.

Tipologías de controles:

- Control preventivo: Control accionado en la entrada del proceso y antes de que se realice la actividad en la que potencialmente se origina el riesgo. Estos controles buscan establecer las condiciones que aseguren atacar la causa raíz y así evitar que el riesgo se concrete.
- Control detectivo: Control accionado durante la ejecución de la actividad en la que potencialmente se origina el riesgo. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: Control accionado en la salida de la actividad en la que potencialmente se origina el riesgo y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

8.3 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 Controles en entidades Públicas. Este modelo pertenece al habilitador transversal de seguridad y privacidad de la Política de Gobierno Digital, 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 2021-2024.

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[1]. 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 27005:2001, estas ofrecen un marco de referencia para la identificación, manejo y mitigación de los riesgos.

Para definir los riesgos de seguridad de la información, hay que plantear un alcance sobre los procesos estratégicos, misionales, de apoyo y control y mejora; luego, hay que inventariar sus activos (con sus respectivos propietarios) y posteriormente, realizar una evaluación de estos teniendo en cuenta los criterios de seguridad de la información: confidencialidad, disponibilidad e integridad.

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.

8.3.1 Identificación del Riesgo de Seguridad de la Información

Se debe identificar los activos de información de cada proceso, teniendo en cuenta que un activo de información es cualquier elemento que tenga valor para la organización.

La identificación de activos se realizará teniendo en cuenta el modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas, en el cual se identifican las amenazas y vulnerabilidades a las que la entidad puede estar expuesta al momento de llevar a cabo actividades socioeconómicas en el entorno digital (prestación de trámites, servicios internos y externos, transacciones en línea entre otros) para así, fomentar y mantener la confianza de las múltiples partes interesadas (proveedores, ciudadanos, entidades públicas y privadas) en el uso del entorno digital en su interacción con Estado.

Los riesgos de seguridad de la información se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”, es decir se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información en función de sus pilares:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

[1] ISO/IEC 27001:2013

Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información (MSPI) de la estrategia de gobierno digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

Para a clasificación de los activos de información se tomará como base la Guía para Identificación de Activos de Información de la entidad, en el procedimiento interno adoptado para ello. Por lo que se determina que solo se gestionarán los riesgos asociados a los activos de información más críticos.

- Descripción del riesgo de Seguridad de la Información

La descripción del riesgo de seguridad de la información debe contener todos los detalles que sean necesarios y que sea de fácil entendimiento tanto para el líder del proceso como para personas ajenas al proceso.

Se propone una estructura que facilita su redacción y claridad que inicia con la frase PERDIDA DE…. (Se incluye allí uno de los pilares de la seguridad de la información: Confidencialidad, Disponibilidad o Integridad) y se analizan los siguientes aspectos:

RIESGO DE SEGURIDAD DE LA INFORMACIÓN **Es la suma de**
Perdida de… (Confidencialidad, Disponibilidad, Integridad) +
ACTIVO DE INFORMACIÓN +
VULNERABILIDAD (Causa Raíz) +
CONSECUENCIA
Ejemplo: Perdida de Confidencialidad de la Información personal de los Colaboradores de la entidad debido a inadecuados controles de acceso causando afectación reputacional a la entidad y reprocesos.

Fuente: Definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.

8.3.2 Descripción de los Activos de Información

Los activos de información son archivos, bases de datos, contratos, acuerdos, documentación de los sistemas, manuales de los usuarios, material de formación, aplicaciones, software equipos de cómputo, equipos de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales, por ejemplo: iluminación, energía, aire acondicionado y las personas que son al fin y al cabo producen, transmiten o destruyen información.

Los activos de información pueden clasificarse en los siguientes:

- Datos/Información: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización. Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
- Software / Aplicaciones Informáticas: El software que se utiliza para la gestión de la información. Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
- Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización. Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.
- Servicios: Aquí se consideran servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo, la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo, la comercialización de productos). Funciones que permiten suplir una necesidad de los usuarios del servicio (internos o externos)
- Hardware / Infraestructura: Los equipos utilizados para gestionar la información (servidores, PC´s, teléfonos, impresoras, routers, cableado, etc.) Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
- Soportes de Información: Dispositivos físicos o electrónicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo y que posteriormente permiten recuperar la información contenida en ellos.
- Redes de Comunicaciones: Infraestructuras dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro. Ejemplo: Red Telefónica, Red Inalámbrica, Telefonía Móvil, Satelital, Red Local (LAN), Red Metropolitana (MAN), Internet, Radio Comunicaciones, Punto a Punto, ADSL, Red Digital (RDSI).
- Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.) y comunicaciones.
- Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.), otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
- Bases de Datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, puede ser utilizada en un formato de motor ya sea SQL, SQL Server, MySQL o en formato Excel.

8.3.3 Valoración del Riesgo de Seguridad de la Información

La valoración del riesgo de seguridad de información se realiza teniendo en cuenta la determinación de la probabilidad (posibilidad de ocurrencia del riesgo) mediante la frecuencia de

la actividad, y la determinación del impacto según como la consecuencia económica y reputacional que se genera por la materialización del riesgo, tal y como se indica en el numeral *"8.2.2 Valoración del riesgo de gestión"*

Para el análisis del riesgo inherente, se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la misma matriz de calor establecida en el numeral *"8.2.2 Valoración del riesgo de gestión"*

La probabilidad y el impacto de determinan con base a la amenaza, y no en las vulnerabilidades, dado que, la sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

8.3.4 Valoración de Controles de Seguridad de la Información

Los controles para mitigar o tratar los riesgos de seguridad de la información serán los establecidos conforme al Anexo A de la ISO/IEC 27001:2022, estos controles se encuentran en el anexo del Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas, identificando la numeración conforme al dominio, el objeto de control y el control que pertenezca. Si después de validar la entidad identifica que cuenta con controles adicionales a los establecidos en el Anexo A de la ISO/IEC 27001:2022 se pueden incluir.

Por ejemplo:

A.5 Políticas de seguridad de la información (Dominio)

A.5.1 Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes (Objetivo de control)

A.5.1.1 Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes (Control)

8.3.5 Plan de Tratamiento de Riesgos de Seguridad de la Información

Se definirá anualmente el plan el tratamiento de riesgos de seguridad de la información, el cual hace parte del Plan de Acción Institucional de la entidad [2].

En el plan de tratamiento de riesgos de seguridad de la información se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad[3]. Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados debe estar aprobados por el responsable de cada proceso.

[2] Artículo 1, Decreto 612 de 2018
[3] Guía 8 - Controles de Seguridad de la Información del Modelo de Seguridad y Privacidad de la Información (MSPI) de Min TIC

8.4 RIESGO FISCAL

La construcción del presente ítem tiene como finalidad prevenir la constitución de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas.

Teniendo en cuenta la estructura y elementos de la definición de riesgos, se define riesgo fiscal, así:

Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Los elementos que componen la definición de riesgo fiscal:

- Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.
- Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, el evento potencial es equivalente a la causa raíz.

8.4.1 Identificación del Riesgo Fiscal:

Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal y las circunstancias inmediatas.

Los puntos de riesgos son situaciones en las que potencialmente se genera riesgo fiscal, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas (Artículo 3 Ley 610 de 2000).

Los riesgos fiscales son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

- Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- Los riesgos de daño antijurídico -riesgo de pago de condenas y conciliaciones.
- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público. Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública

- Identificación de la causa raíz o potencial hecho generador

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro (Auditoría General de la República, 2015).

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio esta tal.

Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños fiscales.

- Descripción del Riesgo Fiscal

Para redactar un riesgo fiscal se debe tener en cuenta:

- Iniciar con la oración: POSIBILIDAD DE, debido a que nos estamos refiriendo al evento potencial.
- Impacto: Corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública (área de impacto).

- Circunstancia inmediata: Corresponde al cómo. Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica -causa raíz- para que se presente el riesgo.
- Causa Raíz: Corresponde al por qué; que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera (El control y la responsabilidad fiscales en Colombia. Luz Jimena Duque Botero y Fredy Céspedes Villa. Ibáñez 2018)

De acuerdo con lo indicado, la estructura propuesta para la redacción de riesgos fiscales es la siguiente:

RIESGO (Lo que puede ocurrir) - **Es la suma de:**		
¿QUÉ? Impacto	**¿CÓMO?** Causa inmediata	**¿POR QUÉ?** Causa Raíz
Ejemplo 1: Posibilidad de efectos dañoso sobre **bienes públicos**, por pérdida, extravío o hurto de bienes muebles de la entidad, a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén. **Ejemplo 2: Bienes Públicos:** Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas **Ejemplo 2: Recursos Públicos:** Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado. **Ejemplo 2: Intereses patrimoniales de naturaleza pública** Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes se amparan con dicho contrato.		

Fuente: Definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 6.

8.4.2 Valoración del Riesgo Fiscal

Evaluación de riesgos: Se busca establecer la probabilidad inherente de ocurrencia del riesgo fiscal y sus consecuencias o impacto inherentes.

Probabilidad: La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.

Teniendo esto presente, para definir el nivel de probabilidad, se utilizará la tabla establecida para el riesgo de gestión *"8.2.2 Valoración del riesgo de gestión"*

Impacto: Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública.

Toda potencial consecuencia económica sobre los bienes, recursos o intereses patrimoniales públicos es relevante para la adecuada gestión fiscal y prevención de riesgos fiscales, sin perjuicio de ello, existen diferentes niveles de impacto, según la valoración del potencial efecto dañoso, es decir, del potencial daño fiscal, se aplicará la tabla establecida para riesgos de gestión *"8.2.2 Valoración del riesgo de gestión"*

8.4.3 Valoración de Controles del Riesgo Fiscal

Se aplican los lineamientos establecidos en el numeral *"8.2.3 Valoración de Controles del Riesgo de Gestión".*

8.5 RIESGO DE CORRUPCIÓN

Para evitar confusiones sobre la naturaleza de un Riesgo por Proceso y un Riesgo de Corrupción el DAFP brinda la siguiente definición de un riesgo de corrupción:

Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. "Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma decisiones y la administración de los bienes públicos". (CONPES No 167 de 2013).

El riesgo debe estar descrito de manera clara y precisa.

Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

8.5.1 Identificación del Riesgo de Corrupción

Las preguntas clave para la identificación del riesgo son:

- ¿Qué puede suceder?
- ¿Cómo puede suceder?
- ¿Cuándo puede suceder?
- ¿Qué consecuencias tendría su materialización?

Dado lo anterior, para que un riesgo sea clasificado como un Riesgo de Corrupción debe cumplir con la siguiente estructura:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

8.5.2 Valoración del Riesgo de Corrupción

La valoración del riesgo se realiza teniendo en cuenta la determinación de la probabilidad (posibilidad de ocurrencia del riesgo) mediante la frecuencia de la actividad, se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia** o **factibilidad**, donde **frecuencia** implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Criterios para calificar la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos una vez en el último año
3	Posible	El Evento podrá ocurrir en algún momento	Al menos una vez en los últimos dos años
2	Improbable	El Evento puede ocurrir en algún momento	Al menos una vez en los últimos cinco años
1	Rara Vez	El Evento puede ocurrir solo en circunstancias excepcionales (poco comunes)	No se ha presentado en los últimos cinco años

Fuente: definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4.

Y la determinación del impacto se analiza únicamente en los niveles moderado, mayor y catastrófico, conforme a las siguientes preguntas:

Nº Pregunta: Si el riesgo de corrupción se materializa podría:	Respuesta (SI/NO)
1. ¿Afectar al grupo de funcionarios del proceso?	
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?	
3. ¿Afectar el cumplimiento de misión de la Entidad?	
4. ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?	
5. ¿Generar pérdida de confianza de la Entidad, afectando su reputación?	
6. ¿Generar pérdida de recursos económicos?	
7. ¿Afectar la generación de los productos o la prestación de servicios?	
8. ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?	
9. ¿Generar pérdida de información de la Entidad?	
10. ¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?	
11. ¿Dar lugar a procesos sancionatorios?	
12. ¿Dar lugar a procesos disciplinarios?	
13. ¿Dar lugar a procesos fiscales?	

Nº Pregunta: Si el riesgo de corrupción se materializa podría:	Respuesta (SI/NO)
14. ¿Dar lugar a procesos Penales?	
15. ¿Generar pérdida de credibilidad del sector?	
16. ¿Ocasionar lesiones físicas o pérdida de vidas humanas?	
17. ¿Afectar la imagen regional?	
18. ¿Afectar la imagen nacional?	
19. ¿Generar daño ambiental?	

Si responde afirmativamente entre 1 a 5 preguntas generan un impacto moderado.
Si responde afirmativamente de 6 a 11 preguntas genera un impacto mayor.
Si responde afirmativamente de 12 a 19 preguntas genera un impacto catastrófico.

Fuente: definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4.

8.5.3 Valoración de Controles del Riesgo de Corrupción

La valoración de controles se realiza acorde con los parámetros señalados en la "Guía para la administración del riesgo y el diseño de controles versión 6.0, publicada en noviembre 2022"

A continuación, se encuentra la Tabla de Análisis y evaluación de los controles para la mitigación de los riesgos, teniendo en cuenta las seis variables establecidas

CRITERIO DE EVALUACIÓN	ASPECTO PARA EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir o detectar	No es un control
Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	No confiable
Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.

CRITERIO DE EVALUACIÓN	ASPECTO PARA EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
	la ejecución del control son investigadas y resueltas de manera oportuna?		
Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta / no existe

Fuente: definiciones Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4.

A partir de lo anterior, el peso o participación de cada variable en el diseño del control para la mitigación del riesgo se describen a continuación:

CRITERIO DE EVALUACIÓN.	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Asignación del responsable	Asignado	15
	No Asignado	0
Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
Periodicidad	Oportuna	15
	Inoportuna	0
Propósito	Prevenir	15
	Detectar	10
	No es un control	0
Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
Evidencia de la ejecución del control	Completa	10
	Incompleta	5
	No existe	0

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 4

8.6 RIESGOS DE LAVADO DE ACTIVOS, FINANCIAMIENTO DEL TERRORISMO Y FINANCIAMIENTO DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA - LA/FT- FPADM

El Sistema de Administración de Riesgos - SARLAFT comprende todas las actividades a ser realizadas por la Entidad en desarrollo de su misión y deberá contener, adicionalmente, los

procedimientos y metodologías para que esté protegida de ser utilizada en forma directa, es decir a través de sus vinculados o contrapartes, como instrumento para el lavado de activos, ocultamiento de activos provenientes de dichas actividades y/o canalización de recursos hacia la financiación de actividades terroristas o la financiación de la proliferación de armas de destrucción masiva.

Con la finalidad de evitar reprocesos y prevenir la multiplicación de herramientas, la metodología que se empleará para el ciclo de administración del riesgo para LA-FT-FPADM será la expuesta en la "Guía para la administración del riesgo y el diseño de controles en las entidades públicas" expedida por el Departamento Administrativo de la Función Pública – DAFP V6, específicamente en lo relacionado con riesgos de gestión.

Para lograr la participación activa en la prevención del Lavado de Activos - LA, Financiación del Terrorismo – FT y Financiación de la Proliferación de Armas de Destrucción Masiva - FPADM, la Secretaría Distrital de Ambiente definió los lineamientos para la identificación y valoración de los Riesgos (LA/FT/FPADM).
A continuación, se describen los elementos para la identificación y valoración de los riesgos (LA/FT/FPADM) en la Secretaría Distrital de Ambiente – SDA.

8.6.1 Identificación del Riesgo LA/FT- FPADM

- Análisis del Contexto

A través del análisis de contexto de la entidad con respecto al LA/FT/ FPADM, se determina la línea de base y los enfoques prioritarios para la gestión de los riesgos.

El análisis del contexto externo, nos permite determinar la relación entre la entidad y el ambiente en el que opera, identificando las oportunidades y amenazas de la entidad. En la etapa de definición del contexto, se deben determinar los elementos cruciales que podrían sustentar o dificultar la administración de los riesgos asociados al LA/FT que la entidad enfrenta, para lo cual debe llevarse a cabo un análisis estratégico. Debe existir una estrecha relación y alineación entre la misión, los objetivos estratégicos de la entidad y la administración de los riesgos asociados al LA/FT, a los cuales está expuesta.

Frente al análisis del contexto interno, es necesario conocer el contexto organizacional, entender y conocer la empresa en su interior, debilidades, sus objetivos y estrategias.

Así mismo es importante diligenciar la siguiente matriz de autodiagnóstico de exposición al riesgo del LA/FT/FPADM que puede tener la entidad, con el fin de identificar de manera general el grado de vulnerabilidad al que puede estar expuesta la entidad en el desarrollo de sus funciones. El resultado obtenido permitirá determinar el grado de exposición relacionado con los riesgos asociados a LA/FT/FPADM.

PREGUNTAS	SI	NO	N.A

¿La entidad recibe recursos de entidades privadas?			
¿La entidad genera recursos propios derivados de bienes, productos o servicios ofrecidos?			
¿La entidad realiza operaciones internacionales en divisas?			
¿La entidad realiza operaciones en efectivo en el desarrollo de sus actividades?			
¿Los usuarios objetivo de la entidad son personas naturales entre las que se encuentran las personas expuestas políticamente (PEP's)?			
¿En algún momento un proveedor de la entidad se ha negado a suministrar la información que se le solicita?			
¿La entidad emplea terceros (contratistas o personas jurídicas) para llevar a cabo alguna de las funciones en el cumplimiento de sus objetivos?			
¿Se han presentado anomalías en la ejecución de contratos firmados por la entidad?			

Fuente: Secretaría General- Dirección Distrital de Desarrollo Institucional

Para analizar el nivel de exposición al riesgo de LA/FT/ FPADM por parte de la entidad, se realizará teniendo cuenta el número de respuestas positivas obtenidas al diligenciar la matriz de autodiagnóstico, como se muestra en la siguiente tabla:

NIVEL DE EXPOSICIÓN DEL RIESGO	
Responder positivamente de UNA a DOS preguntas genera una exposición al riesgo	BAJO
Responder positivamente de TRES a CINCO preguntas genera una exposición al riesgo	MEDIO
Responder positivamente de SEIS a OCHO preguntas genera una exposición al riesgo	ALTO

Fuente: Elaboración propia, Secretaría General- SDA.

La anterior encuesta debe ser resuelta por los Líderes de Procesos como mínimo una vez al año para garantizar el desarrollo periódico que permita obtener los diferentes cambios que se presenten en la entidad y obtener el grado de exposición al Riesgo. Si el grado de exposición aumenta en el autodiagnóstico de la vigencia, se debe revisar la pertinencia de ajustes de controles o creación de controles, en aras de aportar a la prevención del LA/FT/ FPADM en la entidad.

- Clasificación del riesgo

A continuación, se muestra las tipologías de riesgos asociados a los Riesgos de LA/FT/ FPADM:

  - Riesgo reputacional: es la posibilidad de pérdida, disminución de ingresos o incremento en procesos judiciales en que incurre una entidad por desprestigio, mala imagen, publicidad negativa respecto de la institución y sus prácticas de negocios.
  - Riesgo legal: es la posibilidad de pérdida en que incurre una entidad por sanciones o indemnizaciones de daños como resultado del incumplimiento normativo o de obligaciones contractuales. Se presenta de igual forma cuando existen fallas en los contratos y transacciones por actuaciones, negligencia o actos involuntarios.

- Riesgo operativo: es la posibilidad de incurrir en pérdidas por fallas, deficiencias o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de eventos externos.
- Riesgo de contagio: es la posibilidad de pérdida en que incurre una entidad por una acción o experiencia de un vinculado, entendido este como el relacionado o asociado, incluyendo a las personas naturales y/o jurídicas que ejercen influencia sobre la entidad.

(Fuente: Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital).

- Factores de riesgo

Los factores de riesgos, son las posibles causas (fuentes o agentes) generadoras del riesgo de LA/FT/FPADM. En la siguiente tabla se encontrará el listado de los factores de riesgos.

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
		Productos y servicios ofertados a la ciudadanía y los grupos de valor con los que interactúa una Entidad.
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
		Contrapartes - SARLAFT
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público
		Las áreas geográficas o jurisdicciones: son las zonas o áreas en los que opera la entidad o en donde se encuentra el cliente o contraparte.

Factor	Definición	Descripción
Canales de distribución	Eventos relacionados con los medios mediante los cuales se ofrece el producto o servicio.	Son las oficinas o puntos de atención de la entidad. Centro de atención telefónica (Call Center, Contact Center) Internet, entre otros.

Fuente: Documento Técnico "Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital.

- Identificar el evento y descripción del riesgo:

Cuando se habla de los eventos, estos se pueden identificar teniendo en cuenta la fuente de los riesgos y las áreas afectadas, pero además la presencia de circunstancias, ocurrencias y sucesos asociados al riesgo de LA/FT, que se pueden obtener aplicando herramientas como las entrevistas, los cuestionarios, la experiencia colectiva sobre el contexto y el desarrollo del negocio respecto de la interacción entre entradas, salidas y responsabilidades de los procesos de la entidad.

Frente a la descripción del riesgo, se debe iniciar con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

RIESGO (Lo que puede ocurrir) **Es la suma de**
¿QUÉ? Impacto
¿CÓMO? Causa inmediata
¿POR QUÉ? Causa Raíz
Ejemplo: **Posibilidad de afectación reputacional debido a la adquisición de bienes o activos provenientes de actividades relacionadas con el LA/FT o que puedan ser objeto o estar dentro de un proceso de extinción del derecho del dominio, por la débil verificación de la información relacionada en el certificado de existencia y representación de legal y el RUT de la contraparte.**

Fuente: Elaboración propia, Secretaría General- SDA

8.6.2 Valoración del Riesgo LA/FT- FPADM

- Probabilidad:

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociado a la factibilidad. De este modo, la probabilidad inherente implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata de un hecho que no se ha presentado, pero es posible que suceda.

Teniendo esto presente, para definir el nivel de probabilidad, se utilizará la tabla establecida para el riesgo de gestión *"8.2.2 Valoración del riesgo de gestión"*

- Impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Teniendo esto presente, para definir el nivel de probabilidad, se utilizará la tabla establecida para el riesgo de gestión *"8.2.2 Valoración del riesgo de gestión"*

9 COMUNICACIÓN Y CONSULTA

Esta política debe ser publicada por la segunda línea de defensa en el aplicativo ISOLUCIÓN, en la página web de la entidad y comunicada a todos los servidores públicos de la entidad a través de las herramientas de comunicación interna con las que cuenta la entidad, encaminadas a la apropiación de esta política por parte de todos los servidores públicos.

En todo caso, todas las dependencias de la entidad realizarán la socialización y capacitación de esta política y sus componentes a los servidores adscritos a cada una de ellas a fin de dinamizar la cultura del riesgo en todas las operaciones institucionales.

10 MONITOREO Y SEGUIMIENTO DEL RIESGO

El monitoreo y seguimiento a los riesgos por parte de las líneas de defensa, se realizará especialmente a los riesgos que se encuentran en niveles de aceptación en los colores amarillo, naranja y rojo, por lo cual, los riesgos que se encuentren dentro del color verde, tendrán seguimiento únicamente en el segundo cuatrimestre del año.

El monitoreo y seguimiento se realizará así:

Primer seguimiento: Con corte al 22 de abril de 2024. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de mayo de 2024.
Segundo seguimiento: Con corte al 22 de agosto de 2024. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre de 2024.
Tercer seguimiento: Con corte al 20 de diciembre de 2024. La publicación deberá surtirse dentro de los diez (10) primeros días hábiles del mes de enero de 2025.

Los monitoreos les corresponden a la línea estratégica, primera y segunda línea de defensa, 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 Administración del Riesgo.

- **Primera Línea de Defensa:** Realiza monitoreo cuatrimestral a los controles y acciones tendientes a controlar y gestionar los riesgos y enviará a la Subsecretaría General los resultados de esos monitoreos, realizando el registro en la herramienta establecida los tres (3) días hábiles siguientes a la fecha corte establecida en cada cuatrimestre.

- **Segunda Línea de Defensa:** Realizará monitoreo cuatrimestral a través de los reportes por proceso, asegurando que los controles y acciones implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende. La segunda línea de defensa realizará el registro en la herramienta establecida los tres (3) días hábiles siguientes a la primera línea.

- **Tercera Línea de Defensa:** Realizará seguimiento cuatrimestral a través de los reportes de la segunda línea de defensa y solicitudes independientes a la primera línea de defensa, en caso de requerirse, registrándolo en la herramienta establecida, durante los cinco (5) primeros días hábiles del mes siguiente al mes de corte; remitiendo informe a los líderes de proceso durante los primeros diez (10) días hábiles de los meses de mayo y septiembre de 2024 y enero de 2025.

11 MATERIALIZACIÓN DEL RIESGO

En la siguiente tabla se encuentran las acciones a emprender ante los riesgos materializados:

RESPONSABLE	ACCIÓN

Línea Estratégica	• Corrupción y LA/FT/FPADM:
	  ○ Analizar las causas y tomar las decisiones para iniciar la investigación de los hechos.
	  ○ De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.
	• Gestión y Fiscal:
	  ○ Analizar las causas y tomar las decisiones para iniciar la investigación de los hechos.

Primera Línea de Defensa	• Corrupción:
	  ○ Informar a la segunda y tercera línea de defensa sobre el hecho encontrado.
	• Gestión y Fiscal
	  ○ Analizar las causas
	  ○ Ajustar los controles establecidos inicialmente.
	  ○ Analizar del impacto que tuvo la materialización.
	  ○ Informar a la segunda y tercera línea de defensa sobre el hecho encontrado.
	• LA/FT/FPADM
	  ○ Informar al Oficial de cumplimiento, a la segunda y tercera línea de defensa sobre el hecho encontrado.

Segunda Línea de Defensa	• Corrupción
	  ○ Asesorar al proceso para la implementación del plan de contingencia.
	  ○ Informar a la línea estratégica y tercera línea de defensa.
	• Gestión y Fiscal

RESPONSABLE	ACCIÓN
	○ Asesorar al proceso en el análisis de causas ○ Asesorar al proceso en el ajuste en controles establecidos inicialmente. • LA/FT/FPADM ○ El Oficial de cumplimiento debe reportar a las autoridades competentes. Por ejemplo, el Reporte de Operaciones Sospechosas (ROS) que se convierte en el medio de comunicación dirigido a la Unidad de Información y Análisis Financiero – UIAF.
Tercera Línea de Defensa	• Corrupción y LA/FT/FPADM: ○ Informar a la línea estratégica en el marco del Comité Institucional de Coordinación de Control Interno, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. • Gestión y Fiscal ○ Asesorar al proceso en el análisis de causas ○ Asesorar al proceso en el ajuste en controles establecidos inicialmente. ○ Informar a la línea estratégica en el marco del Comité Institucional de Coordinación de Control Interno. ○ Coordinar con la Subsecretaría General – SG, la actualización del mapa de riesgos.

Fuente: Elaboración propia, Secretaría General- SDA

CONTROL DE CAMBIOS

Versión	Descripción de la modificación	Acto Administrativo
6	Se ajusta el tratamiento a riesgos, se ajustan las fechas de presentación de informe cuatrimestral, se ajustan responsabilidades, se insta a asignar una menor frecuencia de seguimiento a aquellos riesgos con color verde, sin que ello implique su desatención y a realizar su seguimiento solo una vez al año, se ajusta el nombre a Política de Administración del Riesgo	Aprobada mediante acta del Comité Institucional de Coordinación de Control Interno del 30 de noviembre del 2022
7	Se mantiene estructura conceptual para la administración del riesgo. Se incluye capítulo específico sobre riesgo fiscal, en lo relacionado con conceptos claves, se actualiza normatividad, definiciones, se actualiza lo referente a Riesgos de Seguridad de la Información en lo referente al formato para el inventario de activos de información, se incluyen los criterios para la identificación, análisis y evaluación de riesgos asociados a lavado de activos y financiación del terrorismo	Aprobada mediante acta del Comité Institucional de Coordinación de Control Interno de 25 de septiembre de 2023.

RESPONSABLES DE ELABORAR O ACTUALIZAR

Elaboró	Revisó	Aprobó
Nombre: Integrantes Equipo SIG -SDA Cargo: N.A. (funcionarios y Contratistas) Fecha:	Nombre: Julio Cesar Pulido Puerto Cargo: Subsecretario General Fecha: 25 de septiembre de 2023	Nombre: Comité Institucional de Coordinación de Control Interno Cargo: N.A. Directivos de la SDA Fecha: 25 de septiembre de 2023