2025

POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

SECRETARÍA DE DESARROLLO ECONÓMICO
Oficina Asesora de Planeación

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

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

La Secretaría Distrital de Desarrollo Económico adopta la presente Política de Gestión Integral de Riesgos, como un instrumento de direccionamiento estratégico que orienta la toma de decisiones, permite anticipar escenarios adversos y gestionar oportunidades, en coherencia con la plataforma estratégica (misión, visión y objetivos estratégicos), el modelo de operación por procesos y la planeación institucional. Así pues, dicha gestión comprende la apropiación de una cultura, capacidades y prácticas integradas al desempeño institucional, a través de las cuales la entidad busca preservar y crear valor agregado, para contribuir al logro de resultados sostenibles y al fortalecimiento del sector que lidera.

En este marco, la Política constituye la declaración institucional frente a la gestión del riesgo, definiendo las tipologías de riesgo a los que se ve expuesta la entidad, por una serie de factores internos y externos, y estableciendo lineamientos para su evaluación (identificación, análisis y valoración), niveles de desviación aceptables y tolerables, así como directrices para su tratamiento proporcional, monitoreo, seguimiento, actualización y publicación. Su implementación se fundamenta en una visión sistémica y preventiva, en la buena gobernanza del riesgo y en la adopción progresiva de estándares técnicos, articulando los instrumentos de los diferentes procesos de la Secretaría, los sistemas de gestión y los requisitos normativos vigentes nacionales y distritales.

Esto deriva en que la Política integre tipologías de riesgos generales de gestión, integridad pública (corrupción, fraude, soborno, inadecuada gestión de conflictos de interés, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva -LA/FT/FP-), así como los riesgos fiscales, de seguridad de la información, contractuales, medio ambiente y seguridad y salud en el trabajo, que pueden afectar el cumplimiento de la misión, el uso eficiente y transparente de los recursos públicos, la imagen institucional y la confianza de sus grupos de valor, y el logro de los compromisos del sector Desarrollo Económico y el Plan Distrital de Desarrollo.

La efectividad de esta Política exige el compromiso de la Alta Dirección y el liderazgo de los órganos de dirección y representación legal, quienes deben promover una cultura organizacional orientada a la integridad, transparencia y legalidad, y a la toma de decisiones bajo un enfoque basado en riesgos, en consonancia con el Ambiente de Control del Modelo Estándar de Control Interno. En este contexto, cada línea de aseguramiento asume un rol estratégico, aportando una visión multidisciplinaria y una respuesta oportuna y pertinente, con el propósito de evitar afectaciones y asegurar la continua creación de valor público en la gestión pública en el Distrito Capital.

2. DEFINICIONES Y SIGLAS

Activo de Información: 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 (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Apetito de 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 (Ídem).

Beneficiario final: Persona(s) natural(es) que finalmente posee(n) o controla(n) a un cliente o a la persona natural en cuyo nombre se realiza una transacción. Incluye también a la(s) persona(s) que ejerzan el control efectivo y/o final, directa o indirectamente, sobre una persona jurídica u otra estructura sin personería jurídica, es decir aquellos que se benefician económicamente de un vehículo jurídico, como una sociedad mercantil, un fideicomiso, una fundación, etc. (adoptado del documento preguntas frecuentes UIAF).

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 y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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

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

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

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

Conflicto de interés: Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho (a partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011).

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.

Contrapartes: Es cualquier persona natural o jurídica con la que la entidad tiene o planifica establecer algún tipo de relación comercial o profesional (Cartilla debida UIAF). En esta categoría se ubican contrapartes externas e internas como proveedores de bienes y servicios, empleados en cualquier modalidad de contratación y clientes.

Control: Medida que permite reducir o mitigar un riesgo. (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Corrupción: Todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Debida diligencia: Es el proceso mediante el cual la entidad adopta medidas para el conocimiento de la contraparte, de su negocio, operaciones, y productos y el volumen de sus transacciones (Superintendencia de Sociedades de Colombia, 2021). Asimismo, es el proceso de evaluar con mayor detalle la naturaleza y el alcance del riesgo de soborno, para ayudar a las organizaciones a tomar decisiones en relación con operaciones, proyectos, actividades, socios de negocios y personal específico (ISO 37001:2025 Sistemas de Gestión Antisoborno).

Debida Diligencia Reforzada: Es el proceso mediante el cual la entidad adopta medidas adicionales y con mayor intensidad para el conocimiento de la contraparte, de su negocio, operaciones, productos y el volumen de sus transacciones (Superintendencia de Sociedades).

Delito: se relaciona con una conducta humana típica punible que lesiona o pone efectivamente en peligro, sin justa causa, el bien jurídicamente tutelado por la ley penal, para los cual deberá reunir las condiciones de tipicidad, antijuridicidad y culpabilidad (adaptado del Código Penal).

Delito Fuente: De acuerdo con el Código Penal Colombiano existen 66 delitos tipificados como delitos fuente de lavado de activos. Los principales delitos fuente en Colombia son: Enriquecimiento ilícito, tráfico de drogas, los delitos contra la administración pública, secuestro extorsivo y el contrabando (Documento de Preguntas Frecuentes UIAF).

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

Enlaces de MIPG: Funcionarios o contratistas designados por las dependencias de la SDDE, los cuales constituyen el equipo de apoyo técnico y articulador de los líderes de política para la orientación y ejecución de las actividades tendientes a fortalecer la sostenibilidad del Modelo Integrado de Planeación.

Factores de Riesgo: Son las fuentes generadoras de riesgos. (Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 DAFP).

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).

Financiación de la Proliferación de Armas de Destrucción Masiva (FP): Es 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, trasferencia, deposito o uso dual para propósitos ilegítimos en contravención de las leyes nacionales u obligaciones internacionales, cuando esto último sea aplicable (UIAF).

Fraude: errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima (a partir de ISO37001:2025).

Función de cumplimiento: función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo. (Ídem)

Integridad de un activo de información: Propiedad de exactitud y completitud (ISO 27000).

Lavado de Activos - LA: Es la modalidad mediante la cual organizaciones criminales buscan dar apariencia de legalidad a los recursos que obtienen de sus actividades ilícitas, mediante la incorporación de estos en el circuito económico legal (Cartilla lavado de activos, UIAF).

Listas Restrictivas: Las listas son bases de datos nacionales o internacionales en los que se relaciona o se recoge información, reportes y antecedentes de personas naturales o jurídicas. Estas listas son utilizadas frecuentemente en el proceso de Debida Diligencia de LA/FT/FP (Documento preguntas frecuentes, UIAF).

Listas Vinculantes: Son aquellas listas de personas y entidades asociadas con organizaciones terroristas que son vinculantes para Colombia bajo la legislación y conforme al derecho internacional, de acuerdo con el artículo 20 de la Ley 1121 de 2016. Entre estas listas se encuentran las resoluciones del Consejo de seguridad de las Naciones Unidas (Cartilla debida diligencia SDDE).

Modelo Estándar de Control Interno (MECI): Herramienta que proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, con el

propósito de que las entidades puedan cumplir de manera razonable con los objetivos institucionales (adaptado del DAFP).

MIPG: Modelo Integrado de Planeación y Gestión.

Modelo de Líneas de Aseguramiento: constituyen un modelo de gobernanza que define y articula los roles y responsabilidades de los distintos actores de la entidad en la gestión de riesgos, el control interno y el aseguramiento, con el fin de proporcionar a la administración un aseguramiento razonable respecto al logro de los objetivos, prevenir la materialización de riesgos y evitar la duplicidad de esfuerzos (adaptado del DAFP).

Nivel de riesgo: A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), es decir los niveles de severidad (DAFP, 2025).

Operaciones Inusuales: Son las transacciones cuya cuantía o características no guardan relación con la actividad económica de los clientes o que por su número, cantidades transadas o características particulares, se salen de los parámetros de normalidad establecidos para determinado rango de mercado de los usuarios (Guía UIAF de buenas prácticas del ROS).

Operaciones Sospechosas: Cualquier acción o información relevante sobre manejo de activos, pasivos u otros recursos, cuya cuantía o características que no guarden relación con la actividad económica de sus asociados, o sobre las transacciones de asociados/contraparte o usuarios que por su número, por las cantidades transadas o por las características particulares de las mismas, puedan conducir razonablemente a sospechar que los mismos están usando a la organización para transferir, manejar, aprovechar o invertir dineros o recursos provenientes de actividades delictivas o destinados a su financiación. (Superintendencia de la Economía Solidaria, 2016).

Personas Expuestas Políticamente -PEP-: Servidores públicos de cualquier sistema de nomenclatura y clasificación de empleos de la administración pública nacional y territorial, cuando en los cargos que ocupen, tengan en las funciones del área a la que pertenecen o en las de la ficha del empleo que ocupan, bajo su responsabilidad directa o por delegación, la dirección general, de formulación de políticas institucionales y de adopción de planes, programas y proyectos, el manejo directo de bienes, dineros o valores del Estado. Estos pueden ser a través de ordenación de gasto, contratación pública, gerencia de proyectos de inversión, pagos, liquidaciones, administración de bienes muebles e inmuebles. Incluye también a las PEP Extranjeras y las PEP de Organizaciones Internacionales (Anexo 1 Circular externa Superintendencia de Sociedades - Modificación Integral al Capítulo X de la Circular Básica Jurídica de 2017).

Programa de Transparencia y Ética Pública – PTEP-: Conjunto de acciones que una entidad define e implementa para promover, al interior de la organización, una cultura de la legalidad e identificar, medir, controlar y monitorear los riesgos que se presentan en el desarrollo de su misionalidad.

Probabilidad: Se entiende como 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.

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 (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP). 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.

Riesgo de Contagio: Es la posibilidad de pérdida que una entidad puede sufrir, directa o indirectamente, por una acción o experiencia de un vinculado. El vinculado es el relacionado o asociado e incluye personas naturales o jurídicas que tienen posibilidad de ejercer influencia sobre la entidad. (Circular Externa Modificación Integral al Capítulo X de la Circular Básica Jurídica de la Supersociedades, 2017).

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. (Guía para la administración del riesgo y el diseño de controles en entidades públicas V6 DAFP)

Riesgo Legal: Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. Surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones. Circular Externa Modificación Integral al Capítulo X de la Circular Básica Jurídica de la Supersociedades, 2017). Incluyen posibles litigios, incumplimientos regulatorios, contratos problemáticos o infracciones legales previas que podrían afectar la operación (Cartilla debida diligencia, UIAF).

Riesgo Operativo: Es 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. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores. (Circular Externa Modificación Integral al Capítulo X de la Circular Básica Jurídica de la Supersociedades, 2017).

Riesgo Reputacional: Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales (Ídem).

Riesgo Residual: Nivel de riesgo que resulta de aplicar la efectividad de los controles existentes al riesgo inherente (adaptado del Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Riesgos de LA/FT/FP: Es la posibilidad de pérdida o daño que puede sufrir una persona natural o jurídica, al ser utilizada para cometer los delitos de lavado de activos, financiación del terrorismo. (Circular Externa Modificación Integral al Capítulo X de la Circular Básica Jurídica de la Supersociedades, 2017) y la financiación de proliferación de armas de destrucción masiva.

Reporte de Operación Sospechosa -ROS-: Describe las operaciones que por su número, cantidad o características no se enmarca dentro del sistema y prácticas normales del negocio, de una industria o de un sector determinado y, además, que de acuerdo con los usos y costumbres de la actividad que se trate, no ha podido ser razonablemente justificada. El envío del ROS a la UIAF debe ser inmediato al conocimiento de la operación sospechosa y debe hacerse a través del Sistema de Reporte en Línea SIREL (Guía de buenas prácticas UIAF).

Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

Sistema de Reporte en Línea -SIREL-: Plataforma para recepción de información en ambiente web, desarrollado por la UIAF como mecanismo principal para la centralización de la información reportada a partir de las obligaciones establecidas en la normativa de cada sector, de forma eficiente, oportuna y segura. (Documento preguntas frecuentes UIAF).

Soborno: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar (a partir de ISO37001:2025).

Tolerancia al 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 (Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

UIAF: Unidad de Información y Análisis Financiero creada mediante la Ley 526 de 1999.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP).

3. NORMATIVIDAD Y ESTÁNDARES

Ley 87 de 1993: Normas básicas para el ejercicio del control interno en las entidades del Estado; fundamento del autocontrol, la autorregulación y la gestión del riesgo (CICCI).

Ley 599 de 2000: Por la cual se expide el Código Penal y señala los delitos, incluyendo aquellos contra la administración pública, lavado de activos y la financiación del terrorismo.

Ley 970 de 2005: Por medio de la cual se aprueba la "Convención de las Naciones Unidas contra la Corrupción", adoptada por la Asamblea General de las Naciones Unidas. Ley mediante la cual se ratifica la adopción de la Convención de las Naciones Unidas contra la Corrupción -UNCAC, adelantada por la Asamblea General de las Naciones Unidas, con el propósito de exhortar a la adopción de políticas y prácticas con enfoque preventivo de la corrupción.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1474 de 2011: Estatuto Anticorrupción; establece medidas de prevención, investigación y sanción de actos de corrupción en la gestión pública.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 1072 de 2015: Decreto Único Reglamentario del Sector Trabajo; regula el Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST).

Decreto 1083 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.

Decreto 1499 de 2017: Adopta el Modelo Integrado de Planeación y Gestión – MIPG y articula la gestión institucional con el control interno y la administración del riesgo (CIGD).

Decreto 648 de 2017: Modifica el Decreto 1083 de 2015 y fortalece el Sistema de Control Interno, precisando funciones del Comité Institucional de Coordinación de Control Interno – CICCI.

Ley 1952 de 2019: Expide el Código General Disciplinario y regula el régimen disciplinario de los servidores públicos.

Decreto 403 de 2020: Fortalece el control fiscal y define principios y mecanismos para la vigilancia de la gestión de los recursos públicos.

Ley 2016 de 2020: Por la cual se adopta el código de integridad del Servicio Público Colombiano y se dictan otras disposiciones. Crea el Código de Integridad del Servicio Público, aplicable a los valores que orientan el comportamiento de los servidores públicos.

CONPES 4042 de 2021: Define la Política Nacional para la prevención del Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP).

Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Ley 2195 de 2022: Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones. Refuerza las medidas para la transparencia y la integridad pública. Establece la obligación de implementar Programas de Transparencia y Ética Pública (PTEP), articulando la gestión de riesgos de corrupción e integridad con el ciclo de planeación y control.

Decreto 1122 de 2024: Reglamenta los Programas de Transparencia y Ética Pública; incorpora lineamientos de debida diligencia y del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP).

Resolución 2277 de 2025: Actualiza el Anexo 1 de la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

CONPES Distrital 01 de 2019: Adopta la Política Pública Distrital de Transparencia, Integridad y No Tolerancia a la Corrupción; promueve medidas de prevención, detección, investigación y sanción de prácticas corruptas.

Circular 092 de 2020: Imparte lineamientos distritales en materia de integridad, transparencia y prevención de la corrupción en las entidades del Distrito Capital.

Guía para la Gestión Integral del Riesgo en Entidades Públicas (Versión 7, 2025): metodología para identificar, valorar, tratar, monitorear y comunicar riesgos en el sector público. Incluye tipologías de riesgo de gestión, integridad, corrupción y LA/FT/FP, y define criterios técnicos para el análisis de probabilidad e impacto, el diseño de controles y la valoración del riesgo residual.

Manual para la integridad pública de la OCDE (2020): aborda el enfoque basado en riesgos en la elaboración, implementación, monitoreo y evaluación de los riesgos más perjudiciales para la integridad pública.

40 Recomendaciones del GAFI: Marco global para la prevención del lavado de activos, la financiación del terrorismo y la proliferación de armas, incluyendo medidas de debida diligencia y control de riesgos.

Recomendación del Consejo de la OCDE sobre Integridad Pública (2017): Propone un enfoque basado en riesgos para la gestión de la integridad, promoviendo la coherencia institucional, la rendición de cuentas y la participación ciudadana.

ISO 9001:2015: Establece los requisitos para un Sistema de Gestión de la Calidad, orientado a la mejora continua, el enfoque por procesos y la satisfacción de las partes interesadas.

ISO 14001:2015: Define los requisitos para un Sistema de Gestión Ambiental, enfocado en la identificación, control y mitigación de impactos ambientales y el cumplimiento normativo.

ISO/IEC 27000: Familia de normas para la gestión de la seguridad de la información, orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información.

ISO 45001:2018: Establece los requisitos para un Sistema de Gestión de Seguridad y Salud en el Trabajo, orientado a la prevención de accidentes, incidentes y enfermedades laborales.

ISO 31000:2018: Establece los principios, el marco y el proceso para la gestión del riesgo, integrando la gestión de riesgos con la estrategia, la gobernanza y el desempeño organizacional.

ISO 37001:2025: Especifica los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión antisoborno, orientado a prevenir, detectar y abordar el soborno en las organizaciones.

4. GENERALIDADES

4.1. Objetivo general

Establecer los lineamientos para una adecuada identificación, valoración y tratamiento de los riesgos de gestión, soborno, fraude, inadecuada gestión de conflictos de interés, conductas asociadas a corrupción, lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, fiscales, seguridad de la información, ambientales, contratación y de seguridad y salud en el trabajo a los que se encuentra expuesta la Secretaría, con el fin de asegurar el cumplimiento efectivo de su plataforma estratégica y los procesos y procedimientos que la soportan.

4.2. Objetivos específicos

- Definir los roles en el marco del Modelo de las Tres Líneas, incluyendo la línea estratégica, en la gestión de riesgos de la Secretaría de Desarrollo Económico.
- Establecer las herramientas para la identificación, valoración, tratamiento y monitoreo de los riesgos para la integridad pública (fraude, soborno, conflictos de interés no declarados, corrupción o Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva – LA/FT/FP), gestión, seguridad de la información, seguridad y salud en el trabajo, contratación, fiscales y ambientales.
- Definir e implementar actividades de control que permitan realizar una adecuada gestión del riesgo y prevenir o mitigar su materialización.
- Definir los lineamientos para la información, comunicación y consulta de los riesgos institucionales de la Secretaría Distrital de Desarrollo Económico.

4.3. Alcance

La Política de Gestión Integral de Riesgos de la Secretaría Distrital de Desarrollo Económico es una herramienta institucional de prevención, detección y respuesta oportuna, frente a los eventos que se encuentra expuesta en razón del cumplimiento de su Plataforma Estratégica. Por esta razón, aplica de manera transversal a los 17 procesos institucionales y demás procedimientos que forman parte del Sistema de Gestión de Calidad, así como a los programas, estrategias, iniciativas y proyectos que se desarrollan, incluyendo aquellos que son tercerizados.

Además, será de obligatorio cumplimiento para todos los servidores públicos y contratistas, de acuerdo con lo establecido en los niveles de responsabilidad (Líneas de Aseguramiento), en concordancia de la Dimensión 7 “Control Interno” del Modelo Integrado de Planeación y Gestión y en cumplimiento de principios de integralidad, enfoque basado en riesgos, corresponsabilidad, mejora continua, proporcionalidad de los controles, transparencia y articulación con la planeación institucional.

5. DECLARACIÓN DE LA POLÍTICA

La Secretaría Distrital de Desarrollo Económico se compromete a prevenir y gestionar oportunamente los riesgos a los que se encuentra expuesta en la gestión administrativa, integridad pública (fraude, soborno, conflictos de interés no declarados, corrupción o Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva –LA/FT/FP-), gestión fiscal, seguridad de la información, contratación, seguridad y salud en el trabajo, y gestión ambiental, en la medida que pueden afectar el cumplimiento de su plataforma estratégica (misión, visión y objetivos estratégicos), la mejora continua, la correcta ejecución de los recursos y uso de los bienes, la legitimidad institucional, la confianza pública y el progreso del sector en el Distrito Capital.

En consecuencia, la operativización de los esfuerzos, en materia de gestión del riesgo, deberán alinearse con los compromisos suscritos por la Secretaría para fortalecer la integridad pública; asegurar la legalidad y la cero tolerancia a la corrupción; proteger los recursos públicos; asegurar la confidencialidad, integridad y disponibilidad de la información institucional; garantizar procesos contractuales transparentes y eficientes; promover el bienestar del talento humano; y cumplir con los estándares de sostenibilidad y responsabilidad ambiental.

En este sentido, la Secretaría dispondrá de los recursos necesarios (humano, técnico, tecnológico, financiero, entre otros) para garantizar oportunamente la evaluación (identificación, análisis y valoración del riesgo); tratamiento; información, comunicación y consulta; monitoreo y seguimientos periódicos; y la mejora continua. Para ello contará con la participación proactiva de la Alta Dirección y los demás roles que comprende el esquema de gobernanza en la Dimensión de Control interno del Modelo Integrado de Planeación y Gestión (Líneas de aseguramiento), dará cumplimiento a los lineamientos de los líderes de política nacional y distrital, y diseñará e implementará los procesos y procedimientos del Sistema de Gestión de la entidad.

6. CONTEXTO EXTERNO E INTERNO

El análisis del contexto se fundamenta en el DOFA institucional, el cual constituye un insumo para la identificación de factores de riesgo internos y externos, que pueden incidir en la gestión de la Secretaría:

6.1. Contexto externo

Abarca los factores fuera del control directo de la Secretaría Distrital de Desarrollo Económico que pueden influir en el desempeño de los procesos. Estos incluyen cambios en la normativa, situaciones económicas, sociales, políticas y otros factores que afectan el entorno operativo. A continuación, se detallan algunos de los aspectos externos relevantes:

Factor de riesgo político: La Secretaría Distrital de Desarrollo Económico desarrolla sus procesos en un entorno político definido por las prioridades del Plan Distrital de Desarrollo y las decisiones de política pública en materia de desarrollo económico, competitividad, empleo y fortalecimiento empresarial. Estas directrices inciden directamente en procesos estratégicos, misionales y de apoyo, al definir objetivos, metas, programas y esquemas de articulación interinstitucional que condicionan la planeación, ejecución y evaluación de la gestión institucional.

Factor de riesgo económico: El contexto económico, tanto distrital como nacional, influye de manera directa en la operación de los procesos de la entidad, especialmente en aquellos asociados a la gestión financiera, contractual y de proyectos (áreas misionales). Variables como la disponibilidad presupuestal, la ejecución de recursos públicos, el comportamiento del mercado laboral, la dinámica empresarial y las condiciones macroeconómicas inciden en el alcance de los programas, en la priorización de intervenciones y en la sostenibilidad de las acciones orientadas al desarrollo económico del Distrito.

Adicionalmente, algunas dinámicas territoriales y regionales pueden incrementar la exposición de algunos procesos de la Secretaría a riesgos de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (LA/FT/FP), particularmente en escenarios de presión fiscal, alta contratación directa, transferencia de recursos, estímulos económicos, subsidios, alianzas con terceros o participación de actores privados. Estos contextos pueden ser aprovechados por organizaciones o personas para intentar canalizar recursos de origen ilícito, desviar recursos públicos o instrumentalizar los programas y proyectos de la entidad con fines ilegales**.**

Factor de riesgo social: Los cambios en las condiciones sociales de la ciudad, tales como la demanda de servicios por parte de la ciudadanía, las brechas de empleo, informalidad y productividad, así como las expectativas de transparencia, eficiencia y participación, impactan transversalmente los procesos de la Secretaría. Este contexto exige que los procesos misionales y de apoyo respondan de manera oportuna,

articulada y con enfoque diferencial, garantizando la confianza ciudadana y el cumplimiento del propósito público de la entidad.

Factor de riesgo tecnológico: El avance y la adopción de tecnologías de la información y las comunicaciones influyen de manera significativa en los procesos institucionales, particularmente en la gestión de TIC, la gestión documental y los procesos de apoyo a la toma de decisiones. La dependencia de plataformas tecnológicas, sistemas de información y herramientas digitales operadas por terceros puede condicionar la continuidad operativa, la eficiencia de los procesos y la adecuada protección de los activos de información.

Factor de riesgo ambiental: El contexto ambiental, enmarcado en las políticas distritales y nacionales, incide en los procesos de la Secretaría en cuanto al uso eficiente de recursos, la gestión ambiental institucional y el cumplimiento de los lineamientos del Plan Institucional de Gestión Ambiental – PIGA. Las condiciones ambientales y las exigencias regulatorias asociadas influyen en la operación cotidiana de los procesos y en la adopción de prácticas responsables en la Secretaría.

Factor de riesgo legal: La Secretaría opera en un entorno normativo amplio y dinámico, compuesto por disposiciones constitucionales, legales y reglamentarias que regulan la gestión administrativa, financiera, contractual, disciplinaria, documental, de control interno y de integridad pública. Cambios normativos y nuevos lineamientos emitidos por autoridades competentes inciden directamente en la forma en que se diseñan, ejecutan y controlan los procesos institucionales, exigiendo ajustes permanentes para asegurar el cumplimiento legal.

6.2. Contexto interno

En el caso del contexto interno, se identifican los siguientes factores dentro de la Secretaría que afectan directamente la operación de sus procesos, a saber:

Capacidad estratégica: La capacidad estratégica de la Secretaría se refleja en la forma en que sus procesos se articulan en la cadena de valor con la misión institucional, los objetivos estratégicos y el Direccionamiento Estratégico. Los 17 procesos contribuyen, desde sus diferentes roles, al logro de resultados institucionales, lo que exige coherencia entre la planeación, la gestión del riesgo, el seguimiento y la toma de decisiones, así como claridad en las responsabilidades y en la priorización de acciones.

Capacidad tecnológica: La entidad cuenta con procesos asociados a la gestión de TIC y la gestión documental, que soportan la operación de los demás procesos. La capacidad tecnológica interna, determinada por los sistemas de información, herramientas digitales y mecanismos de soporte tecnológico disponibles, incide en la eficiencia operativa, la confiabilidad de la información y la continuidad de los servicios institucionales.

Capacidad del talento humano: La ejecución de los procesos depende de la disponibilidad, competencias y desempeño del talento humano vinculado a la Secretaría. Procesos como la gestión del talento humano, el control disciplinario y el control interno evidencian la importancia de contar con servidores y contratistas con conocimiento técnico, claridad en sus funciones y compromiso con la integridad, el control y la mejora continua.

Capacidad financiera: La capacidad financiera interna está asociada a la planeación, ejecución y control de los recursos presupuestales, así como a la articulación entre los procesos financieros, contractuales, planeación estratégica y los relacionados con las áreas misionales. La disponibilidad y oportunidad de los recursos condicionan el alcance de los procesos y la implementación de controles para prevenir riesgos fiscales y asegurar el uso eficiente de los recursos públicos.

Infraestructura: La infraestructura física y tecnológica de la Secretaría constituye un elemento habilitante para la operación de los procesos. Espacios de trabajo, equipos, redes, sistemas de archivo y plataformas tecnológicas soportan la ejecución de actividades administrativas, misionales y de control, influyendo en la continuidad del servicio y en el cumplimiento de los objetivos de cada proceso. Actualmente, la Secretaría cuenta con dos sedes físicas en Bogotá, incluyendo la de Servicio a la Ciudadanía.

Diseño del proceso: El diseño y nivel de madurez de los procesos institucionales, incluidos sus objetivos, alcances, actividades, controles y responsables, determinan la capacidad de la Secretaría para gestionar adecuadamente sus riesgos. La estandarización, documentación y articulación de los 17 procesos permiten una visión sistémica de la operación institucional y facilitan la identificación, análisis y tratamiento de los riesgos que pueden afectar el cumplimiento de los objetivos y metas institucionales.

7. NIVELES DE RESPONSABILIDAD

El Modelo de las tres Líneas establece las Líneas de Aseguramiento como un modelo de gobernanza que define y articula los roles y responsabilidades de los distintos actores de la Secretaría en la gestión de riesgos y el control interno, con el fin de proporcionar a la administración un aseguramiento razonable respecto al logro de los objetivos, prevenir la materialización de riesgos y evitar la duplicidad de esfuerzos.

En esta medida, cada nivel de responsabilidad participa en la identificación, valoración, tratamiento y monitoreo de riesgos conforme a sus funciones, asegurando la trazabilidad de las decisiones y la articulación entre las Líneas así:

Línea estratégica: Esta línea está conformada por la Alta Dirección, el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno. La responsabilidad de esta Línea de Aseguramiento se centra en la emisión, revisión, validación y supervisión del cumplimiento de políticas en materia de control interno, gestión del riesgo, seguimientos a la gestión y auditoría interna para toda la entidad.

INSTANCIA	ROLES Y RESPONSABILIDADES
Comité Institucional de Coordinación de Control Interno	Someter a aprobación del representante legal de Secretaría Distrital de Desarrollo Económico la política de administración del riesgo previamente estructurada por parte de la Oficina Asesora de Planeación, como segunda línea de aseguramiento en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. (Tomado de la Resolución interna del Comité Institucional de Coordinación de Control Interno). Hacer seguimiento de las evaluaciones llevadas a cabo por los organismos de control a la Política de Administración del Riesgo de la entidad. Analizar las recomendaciones del Comité Institucional de Gestión y Desempeño en relación con las políticas de gestión y desempeño que puedan generar cambios o ajustes a la estructura de control de la entidad y su impacto en la gestión del riesgo, enfatizando en el análisis de eventos y riesgos críticos. Definir mejoras al Modelo de Gestión de Riesgo en el marco del Modelo Integrado de Planeación y Gestión implementado por la entidad, con especial énfasis en las actividades de control establecidas en todos los niveles de la organización, información que deberá ser suministrada al Comité de Gestión y Desempeño para su incorporación Evaluar, decidir y adoptar oportunamente las propuestas de mejoramiento del componente de administración del riesgo del sistema de control interno que presente en sus informes la Oficina de control Interno.
Comité Institucional de Gestión y Desempeño	En este comité se analiza la gestión del riesgo implementada y se aplican las mejoras, decidiendo los resultados que deben ser abordados en Comité institucional de Coordinación de Control Interno. Realizar el análisis del monitoreo de la gestión del riesgo y recomendar correctivos para su ajuste y mejora.

Primera Línea de Aseguramiento: Es la línea de gerencia operativa (Líderes de proceso y sus equipos) y se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos asociados a los riesgos y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

INSTANCIA	ROLES Y RESPONSABILIDADES
Líderes de Proceso - Gerentes de Proyectos de Inversión	Corresponde a los líderes de procesos asegurarse de implementar esta política y los instrumentos asociados para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. Los líderes de procesos, junto con sus equipos deben identificar, valorar y definir la opción de tratamiento a los riesgos que tiene alcance la presente política y que pueden afectar el logro de los objetivos de los procesos, programas o proyectos en los cuales participe, acorde con la política de administración del riesgo. En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción. (Guía para la administración del riesgo y el diseño de controles en entidades Públicas versión 6). Para los riesgos de seguridad de la información, son los líderes de proceso quienes deben identificar los activos de información de cada proceso, siendo orientados por el responsable de seguridad de la información de la entidad. Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información de cada proceso, siendo debidamente orientados por el responsable de seguridad de la información de la entidad.
Equipo de enlaces MIPG	Los enlaces de MIPG, apoyan a los líderes de proceso en la identificación y valoración de riesgos, definición de opción de tratamiento, valoración de controles, monitoreo a la gestión del riesgo e implementación de acciones de mejora. Son catalizadores en la recolección de información periódica de reportes, actualización de riesgos y multiplicadores de las socializaciones de la metodología vigente.
Servidores Públicos	Participar en cada una de las etapas de la implementación del modelo de administración del riesgo, desde la naturaleza de sus funciones y procesos relacionados, apoyando la construcción y actualización de mapas de riesgos, la caracterización de controles y seguimiento correspondiente. Informar la materialización de riesgos de corrupción, gestión y otros, siguiendo el conducto asociado para su tratamiento. Aplicar las medidas de control, para evitar la materialización de riesgos asociadas a la ejecución de sus actividades.

	Participar en las capacitaciones y/o sensibilizaciones que promueva la entidad en las temáticas asociadas a la administración del riesgo.
Contratistas	Participar en cada una de las etapas de la implementación del modelo de administración del riesgo, desde la naturaleza de sus obligaciones, el objeto de su contrato y procesos relacionados, apoyando la construcción y actualización de mapas de riesgos, la caracterización de controles y seguimiento correspondiente. Informar la materialización de riesgos de corrupción, gestión y otros siguiendo el conducto asociado para su tratamiento. Aplicar los controles diseñados en las matrices de riesgos, asociadas a la ejecución de sus contratos. Participar en las capacitaciones y/o sensibilizaciones que promueva la entidad en las temáticas asociadas a la administración del riesgo.

Segunda Línea de Aseguramiento: Esta Línea de Aseguramiento está conformada dependencias, instancias o roles que ejercen funciones de orientación, coordinación, monitoreo y supervisión especializada sobre la gestión de riesgos y controles implementados por la Primera Línea, sin asumir la ejecución directa de los procesos operativos ni la toma de decisiones propias de la gestión diaria. Para garantizar su efectividad, la Segunda Línea debe contar con independencia funcional, competencias técnicas especializadas y acceso oportuno a la información, actuando de manera permanente y preventiva en coherencia con el SIGRIP, el MIPG y el Sistema de Control Interno.

Entre sus responsabilidades se incluyen la definición de metodologías, lineamientos y herramientas para la administración del riesgo; el acompañamiento técnico a los líderes de proceso; la validación de la identificación, análisis y tratamiento de los riesgos; el seguimiento al desempeño de los controles y planes de acción; y la consolidación y reporte de información para la Alta Dirección (Línea Estratégica).

Entre los roles se pueden identificar el jefe de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), oficiales de seguridad, líderes de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de la Secretaría. A saber, al menos se contemplarán los siguientes:

INSTANCIA	ROLES Y RESPONSABILIDADES
Oficina Asesora de Planeación	Liderar metodológicamente el proceso de gestión del riesgo de gestión, corrupción y LA/FT/FP. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción y LA/FT/FP. Definir mecanismos y herramientas metodológicas para la implementación de la administración del riesgo y acompañar metodológicamente a la primera Línea de Aseguramiento en su implementación. Verificar la adecuada identificación de los riesgos en relación con los objetivos institucionales o estratégicos definidos desde el Direccionamiento Estratégico. Realizar el monitoreo de riesgos de gestión y corrupción y presentar sus resultados al Comité Institucional de Gestión y Desempeño.
Líderes de otros Sistemas de Gestión o metodologías de riesgo	Establecer, socializar y orientar a los procesos en la implementación de la metodología de gestión de riesgo, de acuerdo con los lineamientos legales vigentes o norma técnica aplicable al sistema de gestión correspondiente. Asimismo, en la generación de informes que contengan el monitoreo frente a la ejecución de los controles por parte de la Primera Línea de Aseguramiento así: **Oficina Asesora de Planeación:** riesgos para la integridad pública (fraude, soborno, inadecuada gestión del conflicto de intereses, corrupción y Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva -LA/FT/FP), gestión y fiscales. **Subdirección de Informática y Sistemas:** riesgos de seguridad de la información. **Subdirección Administrativa y Financiera:** riesgos de seguridad y salud en el trabajo y ambientales, así como financieros (transversal a las tipologías de riesgos). **Oficina Jurídica:** asignación de riesgos a los procesos contractuales. **Dirección de Gestión Corporativa:** de manera transversal, para el monitoreo de riesgos que se identifiquen de los canales institucionales de PQRSD (Ley 1712 de 2014, decretos 103 de 2015 y 1081 de 2015 y Resolución 1519 de 2020).

Tercera línea de aseguramiento: Esta Línea de Aseguramiento está conformada por la Oficina de Control Interno, que evalúa de manera independiente y objetiva los controles de Segunda Línea de Aseguramiento para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª Línea de Aseguramiento que no se encuentren cubiertos -y los que inadecuadamente son cubiertos por la Segunda Línea de Aseguramiento. (Manual Operativo MIPG DAFP. 2024) Los auditores internos proveen aseguramiento sobre la efectividad del gobierno corporativo, la gestión de riesgos y el control interno, incluyendo la manera en que la primera y Segunda Línea de Aseguramiento alcanzan sus objetivos de gestión de riesgos y

control (IIA Declaración de Posición: Las Tres Líneas de Aseguramiento para una Efectiva Gestión de Riesgos y Control).

INSTANCIA	ROLES Y RESPONSABILIDADES
Oficina de Control Interno	Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I. Revisar la efectividad y aplicación de controles, planes de contingencia y actividades de monitoreo vinculados a riesgos clave en la entidad. Alertar sobre la probabilidad de riesgo de fraude, corrupción o LA/FT/FP significativo en las áreas auditadas. Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos o unidades auditables que tienen mayor nivel de exposición al riesgo Comunicar regularmente al Comité de Coordinación de Control Interno, y como resultado de la evaluación independiente, cambios e impactos en la evaluación del riesgo. Brindar asesoría y acompañamiento a la primera y segunda línea de aseguramiento, sin que ello derive en acciones de obligatorio cumplimiento para la administración (Tomado de Guía de Roles Oficina de Control interno 2018) En materia de seguridad de la información, realiza seguimiento a través de la auditoría interna, mecanismo para evaluar de manera integral, independiente y objetiva la efectividad de la gestión de riesgos realizada por la primera y segunda Línea de Aseguramiento. Las evidencias correspondientes a los controles y al plan de acción deben ser consultadas en el repositorio designado específicamente para este propósito.

8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

De acuerdo con los lineamientos de la séptima versión (2025) de la Guía para la Gestión Integral de Riesgos en Entidades Públicas, el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP se concibe como un mecanismo orientado a articular los distintos elementos de la Política de Gestión Integral de Riesgos de cada entidad. En este marco, el SIGRIP integra la gestión de los riesgos generales de la gestión, los riesgos fiscales y los riesgos de seguridad de la información, junto con un conjunto de herramientas e instrumentos específicos para la prevención y mitigación de los riesgos para la integridad pública.

Lo anterior obedece a que estas tipologías pueden tener como causa o estar asociadas a prácticas indebidas como el soborno, el fraude, los conflictos de interés gestionados de manera inadecuada y otras formas de corrupción, así como facilitar el lavado de activos, la financiación del terrorismo o la financiación

de la proliferación de armas de destrucción masiva, lo que exige un abordaje integral y articulado de la gestión del riesgo institucional, como se puede evidenciar en la siguiente figura:

Gráfica 1. Sistema de Gestión de Riesgos para la Integridad Pública

Fuente: figura 28, Guía para la Gestión Integral de Riesgos en Entidades Públicas (DAFP, 2025).

En coherencia con lo anterior, la Secretaría Distrital de Desarrollo Económico adoptará el SIGRIP como parte de su marco de gobernanza de la gestión del riesgo, incorporando de manera coordinada los instrumentos de gestión del riesgo definidos institucionalmente, la actuación diligente en el conocimiento de sus contrapartes y la integración de una función de cumplimiento en su operación. Estos elementos, junto con la identificación, el análisis y la valoración de los riesgos conforme a la metodología establecida en el presente acápite de la Política, interactúan para asegurar que la gestión pública se desarrolle con integridad, entendida como el cumplimiento pleno de la ley, la observancia de los principios éticos y la protección del interés general en todas las actuaciones institucionales (DAFP, Secretaría de Transparencia y MinTIC, 2025).

8.1. Apetito, tolerancia y capacidad del riesgo

Para la correcta toma de decisiones frente a la gestión institucional de los riesgos a los que se encuentra expuesta la Secretaría, se toma como base la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del DAFP, para adoptar el siguiente marco de referencia:

8.1.1. Apetito de riesgo

De acuerdo con el Instituto de Auditores IIA Global, es el nivel de riesgo que una organización está dispuesta a aceptar. Teniendo presente los objetivos, el marco legal y las disposiciones de la Alta dirección, en la Secretaría se define un apetito de riesgo nulo frente a los riesgos que comprometen la integridad pública, es decir aquellos relacionados con fraude, soborno, conductas relacionadas con corrupción, inadecuada gestión de la declaración de conflictos de interés y LA/FT/FP. Las demás tipologías de riesgos

procederán con un enfoque cuantitativo o cualitativo o su combinación para gestionarlo de forma adecuada.

8.1.2. Tolerancia al riesgo

Se define como el valor de la máxima desviación admisible del nivel de riesgo, con respecto al valor del apetito de riesgo determinado por la entidad. Así como en el apetito, se establece una tolerancia cero frente a los riesgos contra la integridad pública, especialmente los relacionados con LA/FT/FP, dado el nivel de impacto en la gestión de la Secretaría.

Además, en el caso de los riesgos de seguridad de la información, se define cero tolerancia frente a la pérdida, alteración no autorizada o divulgación de información asociada a los sistemas de información misionales y de apoyo, tales como GESDOC, así como de cualquier otro sistema que soporte procesos estratégicos, misionales o de apoyo, de acuerdo con su nivel de criticidad tecnológica; y tolerancia baja referente a la indisponibilidad de los servicios digitales y sistemas de información considerados críticos para la operación institucional, entendiendo que afectaciones prolongadas pueden comprometer la continuidad del servicio, el cumplimiento de objetivos institucionales y la confianza de los grupos de valor.

8.1.3. Capacidad de riesgo

Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la Alta dirección considera que no sería posible el logro de la plataforma estratégica (misión, visión y objetivos institucionales). Teniendo en cuenta lo establecido anteriormente, como cero apetito y tolerancia frente a los riesgos para la integridad pública, se deberán tomar las acciones correspondientes del plan de contingencia para responder inmediatamente, por cuanto representa una amenaza directa a la gestión y reputación de la Secretaría. En el caso de los riesgos de LA/FT/FP, se activarán los mecanismos razonables que permitan los límites de la Ley.

8.2. Identificación y descripción de los riesgos

La identificación de riesgos es un componente esencial del Sistema de Gestión Integral del Riesgo, en tanto permite analizar y anticipar los eventos que podrían afectar el cumplimiento de la plataforma estratégica de la Secretaría. Para este propósito, la Primera Línea de Aseguramiento puede apoyarse en una serie de fuentes de información internas y externas, que incluyan elementos estratégicos, normativos, operativos, financieros, tecnológicos y de contexto, teniendo presente que las matrices de riesgos deben identificar eventos por proceso y comprendiendo el interrelacionamiento de las diferentes dependencias en la cadena de valor de los mismos.

Entre las fuentes internas se encuentra la comprensión del objetivo mismo del proceso hasta los planes distritales e institucionales; cumplimiento normativo y lineamientos nacionales y distritales aplicables a la Secretaría; alertas de los informes de monitoreo de riesgos de las segundas Líneas; resultados de los informes de evaluación independiente de la Tercera Línea (hallazgos, acciones de mejora y riesgos materializados no administrados); planes de mejoramiento; seguimiento a los indicadores de gestión; resultados de encuestas internas; monitoreo de las declaraciones de conflictos de interés y de bienes y

rentas; PQRSD recurrentes en la entidad; resultados de las pruebas de vulnerabilidad; causas de litigiosidad de la entidad; análisis DOFA y puntos de riesgo, entre otras.

Por su parte, las fuentes externas pueden comprender resultados de mediciones del Departamento Administrativo de la Función Pública, la Procuraduría General de la Nación, la Veeduría Distrital, la Secretaría General de la Alcaldía Mayor de Bogotá y organizaciones como Transparencia por Colombia con sus respectivos planes de cierre de brechas; auditorías de los entes de control externo; informes de nuevas tipologías de LA/FT/FP en el sector y el país, entre otros.

La verificación de estas fuentes puede ser parte del ejercicio de análisis de riesgos (incluyendo causas, valoración de la probabilidad e impacto, definición de controles, entre otros), para lo cual se podrán combinar varias técnicas:

Tabla 1. Técnicas de identificación del riesgo

Técnicas de identificación de riesgos	
Análisis de Árbol de Decisiones	Método que evalúa distintas alternativas de acción frente a un riesgo, considerando probabilidades y consecuencias para apoyar la toma de decisiones.
Análisis de árbol de eventos (AAE)	Método inductivo que analiza las posibles consecuencias de un evento inicial, considerando la efectividad o falla de los controles existentes.
Análisis de árbol de fallas (AAF)	Técnica deductiva que identifica las combinaciones de fallas que pueden conducir a la materialización de un evento de riesgo.
Análisis de causa y efecto (Diagrama de Ishikawa o Fishbone)	Técnica gráfica que organiza y clasifica las causas potenciales de un riesgo en categorías para facilitar su análisis.
Análisis de escenarios	Método que identifica riesgos mediante la construcción y evaluación de escenarios alternativos, considerando variaciones en el contexto interno y externo.
Análisis de impacto en el negocio (BIA)	Técnica que evalúa las consecuencias operativas, financieras, legales y reputacionales derivadas de la materialización de riesgos críticos.
Análisis de la causa principal (ACP)	Herramienta que permite identificar las causas raíz de un evento de riesgo, evitando enfoques centrados únicamente en sus efectos.
Análisis de modos y efectos de fallas (AMEF) y análisis de modos, efectos y criticidad (AMEFC)	Metodologías preventivas que identifican fallas potenciales en procesos o sistemas, evalúan sus efectos y priorizan los riesgos según su criticidad.

Análisis de Monte Carlo	Técnica cuantitativa avanzada que utiliza simulaciones para estimar el comportamiento del riesgo bajo múltiples escenarios probabilísticos.
Análisis DOFA	Herramienta para identificar las Debilidades y Fortalezas (factores internos) y las Oportunidades y Amenazas (factores externos) que inciden en el cumplimiento de los objetivos institucionales.
Análisis en esquema de corbatín (Bow Tie)	Herramienta visual que integra el análisis de causas, eventos y consecuencias de un riesgo, junto con los controles preventivos y mitigantes.
Análisis PESTEL	Técnica que identifica riesgos derivados de factores Políticos, Económicos, Sociales, Tecnológicos, Ambientales y Legales del entorno.
Benchmarking	Método que compara los riesgos y prácticas de gestión con entidades o sectores similares para identificar brechas y oportunidades de mejora.
Clipping (análisis de medios)	Herramienta que identifica riesgos reputacionales, estratégicos o emergentes a partir del seguimiento sistemático de noticias y publicaciones relevantes.
Estructura "¿Qué pasaría si?" (What if?)	Técnica exploratoria que analiza posibles riesgos a partir de preguntas hipotéticas sobre fallas, desviaciones o cambios en un proceso.
Listas de verificación (Checklists)	Herramienta que facilita la identificación de riesgos recurrentes mediante la revisión sistemática de eventos previamente identificados o estándares aplicables.
Lluvia de ideas (Brainstorming)	Técnica participativa que permite identificar riesgos potenciales a partir de la generación libre y estructurada de ideas por parte de los actores involucrados en un proceso.
Método Delphi	Técnica de consulta iterativa a expertos que busca alcanzar consenso sobre riesgos emergentes o escenarios futuros, minimizando sesgos individuales.
Process Mapping (Mapeo de procesos)	Herramienta que permite identificar riesgos asociados a interrupciones, cuellos de botella o ineficiencias a partir de la representación gráfica de los procesos.
Segmentación por clústers	Técnica que agrupa riesgos, procesos o eventos con características similares para facilitar su análisis y priorización.

Fuente: elaboración propia con base en estándares aplicables a la Secretaría.

Ahora bien, una vez se tienen presente las posibles fuentes, es necesario analizar las tipologías de riesgos a las que está expuesta el proceso. A continuación, se describen cada una de estas con base en los lineamientos aplicables, las orientaciones técnicas de las autoridades distritales competentes y su articulación con los sistema de gestión aplicables a la Secretaría. Asimismo, se indican los responsables; los lineamientos mínimos aplicables; los líderes de política, entes u organismos; y las herramientas documentales mínimas internas:

8.2.1. Riesgos generales de gestión

Partiendo de que un riesgo es el efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales, se catalogan los riesgos de gestión como riesgos operativos, en la medida que se refieren 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" (Anexo 2, Guía para la gestión integral del riesgo en entidades públicas V7 DAFP), por ser propios o intrínsecos a las procesos, funciones y misionalidad de cada entidad.

8.2.2. Riesgos para la integridad pública

Son aquellos eventos a los que se expone la entidad, "como consecuencia de los diferentes intereses que pueden confluir en la toma de decisiones, en la medida que se privilegian intereses propios sobre el interés general de la organización" (DAFP, Secretaría de Transparencia y MinTIC, 2025, pág. 114). En este sentido, existen cinco amenazas principales para la integridad pública:

Corrupción: Como riesgo, es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Además, es necesario aclara que los riesgos de corrupción serán identificados en la racionalización de trámites, respondiendo a las directrices de la Secretaría General de la Alcaldía Mayor de Bogotá.

Soborno: Tipificado en el Código Penal colombiano como el delito de cohecho propio o impropio, en la norma ISO 37001:2025 se define como "ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar (…)".

Fraude: Comprende errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima (a partir de ISO37001:2025).

Inadecuada gestión del conflicto de intereses: Un conflicto de interés se presenta cuando un servidor público, en el ejercicio de sus funciones y propia de la vida social y económica, interviene, influye o participa en la gestión, control o toma de decisiones frente a asuntos en los cuales puede tener un interés particular o directo de personas con las que mantiene vínculos personales, familiares, económicos o jurídicos relevantes, de tal manera que puede entrar en tensión con el interés general que orienta la función pública. Así, el riesgo no se configura por la situación en sí misma, sino que se origina por la falta de gestión desde

su identificación, declaración y gestión oportuna o adecuada, y, por tanto, incrementar la opacidad y equidad en la toma de decisiones.

La SDDE implementará los siguientes instrumentos metodológicos para la gestión de estos riesgos:

Tabla 2. Marco de implementación de los riesgos para la integridad pública

Marco de implementación de los riesgos para la integridad pública	
Responsables	• Primera Línea: todas las dependencias (identificación e implementación) • Segunda Línea: Oficina Asesora de Planeación (lineamientos metodológicos y monitoreo). Apoyan la Dirección de Gestión Corporativa y Oficina Jurídica (lineamientos estratégicos y operativos) • Tercera Línea: Oficina de Control Interno (seguimiento)
Lineamientos mínimos	• Guía para la gestión integral de riesgos en entidades públicas versión 7 (2025) • Guía de lineamientos antisoborno para el Distrito (2018) • Disposiciones de las Políticas de Gestión y Desempeño de Integridad, Compras y Contratación Pública, Transparencia, acceso a la información pública y lucha contra la corrupción, Talento humano y Control Interno del MIPG, sin exclusión del alcance de las otras.
Líderes de política	• Departamento Administrativo de la Función Pública • Secretaría de Transparencia • Secretaría General de la Alcaldía Mayor de Bogotá • Secretaría Jurídica Distrital • Departamento Administrativo del Servicio Civil Distrital • Veeduría Distrital
Herramientas documentales internas	• Procedimiento para gestionar el Riesgo • Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos • Formato Matriz de Gestión de Riesgos • Formato Seguimiento de riesgos materializados

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva -LA/FT/FP: Los riesgos asociados a estas conductas se administran con el fin de prevenir que la entidad llegue a ser utilizada por terceros para dar apariencia de legalidad a recursos ilícitos originados de actividades delictivas o de cualquiera de sus delitos fuente, para canalizar recursos hacia la realización de actividades terroristas o para la financiación de armas de destrucción masiva. Dada la complejidad en la materia y el nivel de impacto en la gestión de la Secretaría, es necesario señalar sus propias herramientas:

Tabla 3. Marco de implementación de los riesgos LA/FT/FP

Marco de implementación de los riesgos de LA/FT/FP	
Responsables	• Primera Línea: todas las dependencias y Equipo de debida diligencia (identificación e implementación) • Segunda Línea: Oficina Asesora de Planeación (monitoreo riesgos), Gestor de cumplimiento (lineamientos, monitoreo y reporte externo) y Equipo SARLAFT (lineamientos) • Tercera Línea: Oficina de Control Interno (seguimiento al SARLAFT)
Lineamientos mínimos	• Guía para la gestión integral de riesgos en entidades públicas versión 7 (2025) • Anexo técnico del Decreto 1122 de 2024. • Documento técnico de adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital (2022). • Lineamiento para implementar el Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo en las Entidades del Distrito (2021) • Disposiciones de las Políticas de Gestión y Desempeño de Integridad, Compras y Contratación Pública, Transparencia, acceso a la información pública y lucha contra la corrupción, Talento humano y Control Interno del MIPG • 40 recomendaciones del GAFI • Disposiciones de la UIAF
Líderes de política, instancias u organismos	• Departamento Administrativo de la Función Pública • Secretaría de Transparencia • UIAF • Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos -CCICLA- • Secretaría General de la Alcaldía Mayor de Bogotá • Secretaría Jurídica Distrital • Red de Oficiales de Cumplimiento del Distrito Capital • Grupo de Acción Financiera Internacional • Oficina de las Naciones Unidas contra la Droga y el Delito
Herramientas documentales internas	• Procedimiento para gestionar el Riesgo • Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos • Formato Matriz de Gestión de Riesgos • Manual SARLAFT • Procedimiento Debida diligencia • Cartilla Metodológica para la Debida Diligencia y consulta de listas vinculantes y restrictivas de la SDDE • Reporte de Operaciones Sospechosas

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

Lo anterior se enmarca en lo establecido por los artículos 12 y 31 de la Ley 2195 de 2022, las acciones estratégicas 3 y 4 del anexo técnico del Decreto 1122 de 2024 y los lineamientos institucionales mencionados anteriormente, mediante los cuales se orienta la implementación y gestión de las etapas de: a) identificación, b) medición y evaluación, c) control y d) monitoreo, para la administración de los riesgos LA/FT/FP y sus riesgos asociados: a) reputacional, b) legal, c) operativo y d) contagio.

8.2.3. Riesgos fiscales

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 (DAFP, Secretaría de Transparencia y MinTIC, 2025). Estos riesgos se identifican y gestionan para prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representado en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (artículo 6, Decreto 403 de 2020).

La SDDE implementará los siguientes instrumentos metodológicos para la gestión de estos riesgos:

Tabla 4. Marco de implementación de los riesgos fiscales

Marco de implementación de los riesgos fiscales	
Responsables	• Primera Línea: todas las dependencias y gestores fiscales (identificación e implementación) • Segunda Línea: Oficina Asesora de Planeación (lineamientos metodológicos y monitoreo). Apoya la Dirección de Gestión Corporativa (lineamientos estratégicos y operativos) • Tercera Línea: Oficina de Control Interno (seguimiento)
Lineamientos mínimos	• Guía para la gestión integral de riesgos en entidades públicas versión 7 (2025) • Disposiciones de la Política de Gestión y Desempeño de Gestión Presupuestal y eficiencia del gasto público, Control Interno y Defensa Jurídica
Líderes de política	• Departamento Administrativo de la Función Pública • Contraloría General de la República • Contraloría de Bogotá • Secretaría Distrital de Hacienda
Herramientas documentales internas	• Procedimiento para gestionar el Riesgo • Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos • Formato Matriz de Gestión de Riesgos • Formato Seguimiento de riesgos materializados

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

8.2.4. Riesgos de seguridad de la información

De acuerdo con la norma ISO/IEC 27000, los riesgos asociados a la seguridad de la información se describen como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad, para causar una pérdida o daño en un activo de información. Es así que la identificación deberá partir obligatoriamente de la identificación y clasificación de los activos de información asociados a cada proceso, considerando su importancia para la confidencialidad, integridad y disponibilidad de la información, teniendo presente:

- Los activos de información clasificados como críticos, de acuerdo con los criterios definidos por la SDDE.
- Aquellos activos de información que, aun sin contar con una valoración de criticidad alta, sean determinados por el responsable del proceso como relevantes, en función del impacto sobre la operación, el cumplimiento de los objetivos del proceso, la continuidad del servicio o la exposición a incidentes de seguridad de la información.

En ningún caso la identificación y gestión de los riesgos de seguridad de la información estará supeditada únicamente a la existencia de una valoración previa alta del activo, sino que deberá considerar el juicio técnico del responsable del proceso, orientado por el responsable de seguridad de la información de la entidad.

La SDDE implementará los siguientes instrumentos metodológicos para la gestión de estos riesgos:

Tabla 5. Marco de implementación de los riesgos de seguridad de la información

Marco de implementación de los riesgos de seguridad de la información	
Responsables	• Primera Línea: todas las dependencias (identificación e implementación) • Segunda Línea: Oficial de seguridad de la información de la Subdirección de Informática y Sistemas (lineamientos metodológicos y monitoreo) • Tercera Línea: Oficina de Control Interno (seguimiento)
Lineamientos mínimos	• Guía para la gestión integral de riesgos en entidades públicas versión 7 (2025) • Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas -MSPI- (2025) • Disposiciones de las Políticas de Gestión y Desempeño de Gobierno Digital y Seguridad Digital del MIPG
Líderes de política	• Ministerio de Tecnologías de la Información y las Comunicaciones • Consejería Distrital de Tecnologías de la Información y las Comunicaciones (Secretaría General de la Alcaldía Mayor de Bogotá)

Herramientas documentales internas	• Procedimiento para gestionar el Riesgo • Guía para la gestión de riesgos de seguridad y privacidad de la información • Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos • Formato Matriz de Gestión de Riesgos • • Política de tratamiento y protección de datos personales • Procedimiento de gestión de incidentes de seguridad de la información • Inventario de Activos de información con criticidad alta • Índice de información clasificada y/o reservada

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

8.2.5. Riesgos contractuales

De conformidad con lo dispuesto en el artículo 4 de la Ley 1150 de 2007, en los procesos de contratación se debe incorporar la estimación, tipificación y asignación de los riesgos previsibles en los pliegos de condiciones o en los documentos que hagan sus veces, como un mecanismo orientado a garantizar la satisfacción oportuna de las necesidades de contratación, la transparencia en la adquisición de bienes y servicios y el fortalecimiento de la reputación y legitimidad institucional de la Secretaría.

En este marco, y en ejercicio de la autonomía administrativa, la Secretaría adopta las herramientas y metodologías que considere pertinentes para identificar y gestionar la exposición a eventos que puedan afectar la ejecución de los procesos contractuales, desde la etapa de planeación hasta la terminación del contrato, su liquidación, el vencimiento de las garantías o la disposición final del bien o servicio contratado. Esta gestión no se limita exclusivamente a la tipificación, estimación y asignación de los riesgos que puedan alterar el equilibrio económico del contrato, sino que comprende una visión integral de los riesgos contractuales, conforme a los lineamientos de Colombia Compra Eficiente. Asimismo, cuando aplique, dichos riesgos serán reforzados y validados en la audiencia de asignación de riesgos.

En la Secretaría, el liderazgo metodológico para la gestión de estos riesgos está a cargo de la Oficina Jurídica, como líder del proceso de contratación, responsable de definir los lineamientos, instrumentos y metodologías aplicables, los cuales se incorporan en los procedimientos internos, los formatos de estudios previos y los anexos técnicos correspondientes.

Tabla 6. Marco de implementación para la asignación de riesgos a los procesos contractuales

Marco de implementación para la asignación de riesgos a los procesos contractuales	
Responsables	• Primera Línea: enlaces de contratación de todas las dependencias y Supervisores del contrato. • Segunda Línea: Oficina Jurídica • Tercera Línea: Comité de Contratación (cuando aplique)
Lineamientos mínimos	• Manual para la identificación y cobertura del riesgo en los procesos de contratación

	• Disposiciones de la Política de Gestión y Desempeño de Compras y Contratación del MIPG
Líderes de política, entes o instancias	• Colombia Compra Eficiente • Ministerio de Hacienda y Crédito Público • Contraloría General de la República • Contraloría de Bogotá • Secretaría Distrital de Hacienda • Observatorio Distrital de Contratación y Lucha Anticorrupción
Herramientas documentales internas	• Guía metodológica para identificar, asignar y diligenciar la matriz de riesgos asociados a los procesos de contratación que adelante la Secretaria Distrital de Desarrollo Económico • Tablero de control contractual • Matriz de riesgos identificados del proceso de contratación

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

8.2.6. Riesgos de seguridad y salud en el trabajo

Para identificar los peligros y valorar los riesgos de Seguridad y Salud en el trabajo, los cuales están integrada al Sistema de Salud y Seguridad en el trabajo, se aplican las disposiciones del Decreto 1072 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo", en su Título 4: Riesgos Laborales.

Tabla 7. Marco de implementación de los riesgos de seguridad y salud en el trabajo

Marco de implementación de los riesgos de seguridad y salud en el trabajo	
Responsables	• Primera Línea: todas las dependencias (identificación e implementación) • Segunda Línea: Subdirección Administrativa y Financiera (lineamientos metodológicos y monitoreo) con apoyo externo de las Administradoras de riesgos laborales ARL • Tercera Línea: Oficina de Control Interno (seguimiento)
Lineamientos mínimos	• Guía Técnica Colombiana GTC 45 "Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional"
Líderes de política	• Consejo Nacional de Riesgos Laborales (Ministerio del Trabajo) • Comité nacional de seguridad y salud en el trabajo
Herramientas documentales internas	• Formato Matriz de identificación de peligros, valoración y control de riesgos

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

Se basa en las orientaciones de la Guía Técnica Colombiana GTC 45 "Guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional", para ello, se diligenciará la información en la GTH-P28-F4 Matriz de identificación de peligros, valoración y control de riesgos.

Adicionalmente, el responsable de la Seguridad y Salud en el Trabajo estará a cargo del subdirector(a) de Administrativa y Financiera y las responsabilidades que deberá cumplir respecto a la gestión del riesgo serán las siguientes:

- Adoptar disposiciones para desarrollar las medidas de identificación de peligros, evaluación y valoración de los riesgos y establecimiento de controles que prevengan daños en la salud de los trabajadores
- Incluir en los procesos de inducción y reinducción, actividades relacionadas a la identificación de peligros y control de riesgos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

8.2.7. Riesgos ambientales

La intención de gestionar riesgos ambientales pretende que la Secretaría esté en la capacidad de lograr los resultados previstos en el Sistema de Gestión Ambiental o Plan Institucional de Gestión Ambiental, prevenir o reducir los efectos indeseados al ambiente y lograr la mejora continua. Dichos riesgos pueden estar relacionados con los aspectos ambientales identificados, los requisitos legales y otros requisitos. (NTC ISO 14001:2015).

Los instrumentos de identificación y análisis de riesgos ambientales se soportan en lo dispuesto por la Secretaría Distrital de Ambiente, específicamente lo mencionado en la Resolución 3179 de 2023 "Por la cual se adopta la guía técnica para la formulación del Plan Institucional de Gestión Ambiental (PIGA), y se dictan lineamientos para su concertación, implementación, evaluación, control y seguimiento, y otras disposiciones", cuya ubicación se encuentra en la intranet de la entidad.

Tabla 8. Marco de implementación de los riesgos ambientales

Marco de implementación de los riesgos ambientales	
Responsables	• Primera Línea: Todas las dependencias y líderes de proceso (identificación, gestión e implementación de controles ambientales en sus actividades, proyectos y contratos) • Segunda Línea: gestor ambiental de la Subdirección Administrativa y Financiera (lineamientos metodológicos, acompañar técnicamente y realizar monitoreo transversal del riesgo ambiental) • Tercera Línea: Oficina de Control Interno
Lineamientos mínimos	• Guía técnica para la formulación del Plan Institucional de Gestión Ambiental (PIGA) • Normativa ambiental vigente (obligaciones y estándares aplicables)

	• Lineamientos del MIPG relacionados con sostenibilidad ambiental • Enfoques de gestión del riesgo ambiental alineados con ISO 14001 e ISO 31000 (cuando aplique)
Líderes de política	• Ministerio de Ambiente y Desarrollo Sostenible • Secretaría Distrital de Ambiente
Herramientas documentales internas	• Política Ambiental SDDE • Plan Institucional de Gestión Ambiental – PIGA • Inventario de aspectos e impactos ambientales

Fuente: elaboración propia con base en los lineamientos aplicables a la Secretaría.

8.3. Valoración del riesgo inherente

8.3.1. Probabilidad

Para efectos de la metodología propuesta, la probabilidad se entenderá como la posibilidad de que un riesgo ocurra dentro del periodo de gestión de los procesos institucionales, mientras que el impacto refleja la magnitud de las consecuencias que dicha ocurrencia podría generar.

Esta Política acoge las escalas de valoración definidas en la Guía de Gestión Integral del Riesgo, ajustadas a su contexto. Estas escalas permiten clasificar los riesgos de acuerdo con los criterios de probabilidad e impacto, representados en tablas y mapas de calor que facilitan su priorización y tratamiento dentro del ciclo de gestión.

Tabla 9. Criterios para definir el nivel de probabilidad

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025)

8.3.2. Impacto

En atención a los lineamientos vigentes de Gestión de Riesgo del DAFP versión 7, la entidad define el impacto en dos variables: impactos económicos y reputacionales que se definen a continuación:

- Impacto Económico: Posible pérdida o detrimento económico de la entidad, frente a la materialización de un riesgo
- Impacto reputacional: Posible nivel de pérdida o merma en la reputación de una entidad de forma que afecte de forma negativa a la percepción que el entorno social tiene sobre la misma, cuando se materializa un riesgo

La escala de impacto para el impacto económico y reputacional de la SDDE es el siguiente:

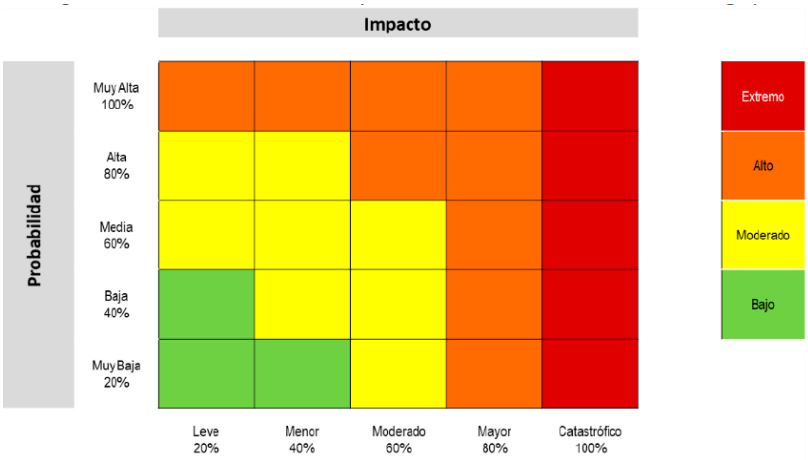
Tabla 10. Criterios para definir el nivel de impacto

Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y accionistas y/o de proveedores.
Moderado-60%	Mayor a 50 SMLMV y Menor a 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor-80%	Mayor a 100 SMLMV y Menor a 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 Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025).

Frente a los riesgos para la integridad pública, el impacto siempre es significativo. Esto significa que en su valoración se consideran tres niveles (moderado, mayor y catastrófico); por lo cual no aplican los niveles de impacto "insignificante" y "menor". Además, cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se debe definir o priorizar el nivel más alto.

La combinación entre la probabilidad e impacto determinará el nivel de severidad del riesgo inherente así:



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025).

8.4. Valoración de controles y planes de acción

Los controles son las medidas, actividades o procedimientos que permiten incidir en el nivel de probabilidad o impacto de los eventos identificados, para que se puedan prevenir, detectar o corregir oportunamente. En este sentido, de acuerdo con la Guía de Gestión Integral del Riesgo (versión 7, DAFP), en el sistema de gestión del riesgo el diseño adecuado de un control requiere una estructura estandarizada, que garantice un diseño pertinente y facilite su implementación. Se estipulan entonces los siguientes atributos que deben ser incluidos en el diseño de los controles:

Responsable: identifica el cargo o rol del encargado de ejecutar el control. Debe corresponder con la estructura organizacional de la entidad e incluir, cuando aplique, a los grupos de trabajo o equipos técnicos responsables del proceso. En el caso de controles automáticos, se especificará el sistema o aplicativo que realiza la función.

Acción: determina la acción o la actividad concreta a realizar para mitigar el evento identificado, por ejemplo, se va a verificar, validar, cotejar, comparar. Este atributo permite precisar la naturaleza del control y facilita su trazabilidad con el riesgo y la causa que pretende mitigar. Para ello se debe establecer la frecuencia de su ejecución (diariamente, mensualmente, semestralmente, cada vez que…).

Complemento: describe los detalles, evidencias o situaciones (como las desviaciones) que puedan llegar a surgir en el curso de la ejecución del control y lo que se haría en cada caso. En ese sentido, se deben mencionar cuáles serán los soportes que se presentarán como evidencia de la ejecución y permitan su seguimiento o verificación posterior. Esto implica que haya una base documental clara, para que sea consistente con los puntos de control de los procedimientos o que al menos se encuentren en proceso de formalización.

Por otro lado, los controles se clasifican de la siguiente manera:

Controles preventivos: su propósito es evitar la ocurrencia del riesgo antes de que genere efectos negativos. Incluyen mecanismos como la separación de funciones, validaciones previas, listas de chequeo, protocolos de actuación, procesos de debida diligencia sobre contrapartes, y capacitaciones en integridad y conflicto de intereses. Su efectividad se refleja en la disminución de la probabilidad del riesgo.

Controles detectivos: tienen como objetivo identificar oportunamente desviaciones, incumplimientos o señales de alerta que puedan anticipar la materialización del riesgo. Comprenden actividades de monitoreo continuo, revisiones documentales, auditorías internas, trazabilidad de registros, y uso de indicadores de alerta temprana. Su adecuada implementación permite tomar decisiones correctivas a tiempo y evitar mayores afectaciones institucionales.

Controles correctivos: se aplican una vez ocurrido el evento o se materializa el riesgo, con el propósito de corregir, compensar o prevenir su repetición. Incluyen ajustes de procesos, sanciones, revisiones de protocolos y fortalecimiento de los mecanismos de control interno. Aunque son necesarios, su ejecución implica que el riesgo ya se materializó, por lo que el énfasis de la gestión debe mantenerse en los controles preventivos y detectivos, que son los que realmente mitigan y evitan los impactos.

En esta línea y de acuerdo con la forma como se ejecutan los controles, se pueden proponer controles manuales, que son aquellos ejecutados por personas, y controles automáticos, que son ejecutados por un sistema o software previamente programado o diseñado. En casos como el de debida diligencia, existirá la combinan de ambos porque se hará uso de un sistema de información que genera alertas de riesgo (automático) y un servidor público o contratista que valida y aprueba las acciones correctivas (manual).

Una vez definidos y clasificados los controles según su naturaleza y forma de aplicación, es necesario valorar su eficiencia y efectividad dentro del sistema de gestión del riesgo. Para ello, se determina en qué medida los controles contribuyen a reducir la probabilidad o el impacto de los eventos de riesgo identificados, así como establecer si se requiere fortalecerlos o diseñar nuevos mecanismos. Dicha valoración se realiza con base en criterios objetivos y medibles que permiten evidenciar su diseño, aplicación, frecuencia y trazabilidad, garantizando una evaluación homogénea en todos los procesos institucionales.

A continuación, se referencia los cálculos correspondientes para llegar al riesgo residual:

Tabla 11. Valoración de Controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
***Implementación** *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025).

Así, la valoración del nivel de severidad del riesgo residual corresponde al resultado de aplicar la efectividad de los controles al riesgo inherente. Para dicha aplicación, se debe tener en cuenta que los controles preventivos y detectivos atacan la probabilidad y los controles correctivos el impacto y que pueden ser acumulativos si existe más de un control para un mismo riesgo. El riesgo residual será aceptable únicamente cuando su nivel se encuentre dentro de los umbrales de tolerancia definidos y los indicadores clave de riesgo correspondientes.

8.5. Tratamiento de los riesgos

Teniendo en cuenta la ubicación final en la Matriz de riesgos, se establecen las medidas de respuesta, a través de la identificación de las opciones de manejo para el tratamiento de los riesgos. Las opciones de manejo a tomar son las siguientes y se pueden considerar cada una de manera independiente o en conjunto:

Evitar el Riesgo: Se toman medidas encaminadas a evitar la materialización del riesgo.

Reducir el Riesgo: Incluye medidas orientadas a disminuir tanto la probabilidad (medidas de prevención) como el impacto (medidas de detección).

Compartir o Transferir el Riesgo: Reducen los efectos de los riesgos, a través del traspaso de las pérdidas a otras organizaciones. No aplica para riesgos LA/FT/FP.

Asumir el Riesgo: En este caso, no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. No aplica para riesgos LA/FT/FP.

El tratamiento del riesgo implica la preferencia para la modificación de los riesgos y la aplicación del mismo, dependiendo la zona en la que estos se encuentren ubicados se define una opción de tratamiento de acuerdo con lo establecido a continuación:

Nota: Para los riesgos de LA/FT/FP no se permite asumir ni transferir el riesgo. Elaboración propia con base en la Guía para la Gestión Integral de Riesgos en Entidades Públicas (DAFP, 2025).

Una vez definida la opción de tratamiento del riesgo y establecidos o ajustados los controles correspondientes, la entidad deberá considerar de manera sistemática las actividades de análisis, evaluación, diseño, ejecución e implementación necesarias para asegurar que dicho tratamiento resulte efectivo y proporcional al nivel de riesgo identificado.

Cuando la opción de tratamiento seleccionada sea la reducción del riesgo, se deberá formular un Plan de Acción, el cual permitirá gestionar de manera estructurada la implementación y seguimiento de las actividades de control. Este plan deberá incluir, como mínimo, la descripción de la acción a ejecutar, las fechas previstas de implementación y seguimiento, los responsables, los indicadores clave de riesgo (KRI) y la definición de una acción de contingencia que permita responder de manera oportuna ante una eventual materialización del riesgo.

Los indicadores clave de riesgo (KRI) constituyen una herramienta fundamental para el monitoreo preventivo, en tanto permiten establecer umbrales y niveles de alerta temprana que facilitan la identificación oportuna de desviaciones, cambios en la exposición al riesgo o incrementos en su severidad. Estos indicadores apoyan la toma de decisiones informadas y el fortalecimiento de los controles, en concordancia con el enfoque preventivo promovido por el Modelo Integrado de Planeación y Gestión – MIPG y permitan precisar los parámetros de auditoría de la Tercera Línea de Aseguramiento.

Adicionalmente, a partir del análisis integral de los procesos y su interrelación dentro de la cadena de valor institucional, la entidad podrá identificar riesgos potenciales o emergentes, así como nuevas amenazas que puedan afectar el logro de los objetivos estratégicos, lo que contribuye a una gestión del riesgo dinámica y prospectiva.

En este sentido, los riesgos que, por su nivel de exposición, impacto o criticidad, así lo requieran, deberán contar con indicadores clave de riesgo, que permitan monitorear la exposición al riesgo, desviaciones, generar alertas tempranas frente a variaciones significativas y facilitar la toma oportuna de decisiones frente a la efectividad de los controles, especialmente, por parte de los líderes de proceso. La formulación de los KRI procederá en los siguientes términos:

Fuente: elaboración con base en la figura 31 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025).

9. MONITOREO, SEGUIMIENTO Y MATERIALIZACIÓN DE RIESGOS

Para la gestión del riesgo, es necesario realizar un continuo monitoreo, seguimiento y control de uno de los planes de tratamiento del riesgo donde se determinen cuáles serán los controles que permitirán mitigar los riesgos y solucionarlos por medio de mantenerlos, de reducir su nivel, eliminarlos o transferirlos. Así mismo, variables externas e internas pueden modificar el riesgo, su valoración o controles para su mitigación. A continuación, se establecen las directrices para el monitoreo asociado a primera y segunda Línea de Aseguramiento, el seguimiento asociado a tercera línea y las acciones a emprender cuando se identifica materialización de riesgos.

9.1. Monitoreo

El monitoreo se llevará a cabo desde primera y segunda Línea de Aseguramiento así:

Monitoreo Primera Línea de Aseguramiento (Líderes de proceso y sus equipos)

Una vez identificado, valorado y establecido el tratamiento de los riesgos, el líder del proceso, junto con su equipo, realizará el monitoreo permanente estos y haciendo un reporte como mínimo de **manera trimestral** para la Segunda Línea en riesgos de gestión, integridad pública, fiscales y seguridad de la información. Este deberá incluir el reporte cualitativo de avance de las acciones de tratamiento frente al nivel de riesgo residual, la verificación de la continuidad y efectividad de los controles establecidos, y la identificación de posibles eventos de materialización, incluyendo las respectivas evidencias.

El líder debe considerar modificaciones sobre el riesgo identificado, si en el monitoreo se presentan cambios relevantes, tales como aplicación de nuevos controles, materialización del riesgo, mayor exposición del riesgo u otras situaciones que impacten la probabilidad o impacto. Las actualizaciones deben ser comunicadas a la Oficina Asesora de Planeación y Subdirección de Informática y Sistemas (cuando aplique), para su incorporación en la matriz de riesgos.

Fechas clave: Reporte de monitoreo primera Línea de Aseguramiento en los **10 primeros días hábiles**, al corte de cada trimestre.

Para la tipologías de riesgos ambientales, seguridad y salud en el trabajo y de contratación, los líderes de procesos deben considerar las actualizaciones en los mismos términos mencionados anteriormente y comunicarlas al responsable líder del sistema de gestión del riesgo ambiental y seguridad y salud en el trabajo (Dirección de Gestión Corporativa) o de contratación (Oficina Jurídica), según sea el tipo de riesgo, que funja como Segunda Línea.

Fechas clave: De acuerdo con la normatividad técnica o legal de cada sistema de gestión.

Monitoreo/evaluación Segunda Línea de Aseguramiento

Oficina Asesora de Planeación y Subdirección de Informática y Sistemas

La Oficina Asesora de Planeación realizará reporte y consolidación del **monitoreo trimestral** de los riesgos de gestión, para la integridad pública y fiscales, y la Subdirección de Informática y Sistemas de los riesgos de seguridad de la información, previo reporte de los líderes de proceso. De acuerdo con la tipología de riesgo, evaluarán el avance de acciones de los controles, el plan de acción o tratamiento de riesgos y materializaciones, y analizarán las deficiencias del modelo para realizar las recomendaciones sobre la mejora y ajuste del mismo.

Fechas clave: Consolidación y análisis del reporte de monitoreo enviado por Primera Línea de Aseguramiento, **en la última semana del mes posterior al cierre del trimestre**. Se presentará en las sesiones de la Alta Dirección (Comité Institucional de Gestión y Desempeño y/o Comité Institucional de Coordinación de Control Interno), de acuerdo con la agenda establecida para la vigencia.
Líderes de otros Sistemas de Gestión y categorías de riesgo (Ambiental, Contratación y Seguridad y Salud en el Trabajo) Los responsables de la gestión de riesgos ambientales, de contratación y de Seguridad y Salud en el Trabajo Salud realizan el monitoreo y el reporte ante la autoridad competente, conforme a la normatividad específica de cada uno y definen las acciones correspondientes en caso de materialización del riesgo.
Fechas clave: De acuerdo con normatividad técnica o legal de cada sistema de gestión.

9.2. Seguimiento

El seguimiento corresponde a la auditoría o evaluación independiente que adelanta la Tercera Línea de Aseguramiento, es decir, el/la Jefe de la Oficina de Control Interno y su equipo técnico, respecto a los riesgos que administra la Secretaría y lo definido en la presente Política:

- El seguimiento al mapa de riesgos de gestión se realizará trimestralmente, a través de un informe que la Oficina de Control Interno puede incluir en sus auditorías internas como la revisión de riesgos institucionales, dado su enfoque basado en el riesgo.
- El seguimiento a los riesgos de corrupción y LA/FT/FP, atenderá los términos de la Guía del DAFP vigente, donde se realiza un seguimiento cuatrimestral que debe ser publicado en el botón de Transparencia de la sede electrónica de la Secretaría, en los diez (10) primeros días hábiles siguientes al corte de cuatrimestre.
- Adicionalmente, el/la Jefe de la Oficina de Control Interno evaluará, de manera independiente y bajo un esquema de auditoría interna basada en riesgos, los avances sobre el diseño, implementación y efectividad de las herramientas del Sistema de Gestión de Riesgos para la Integridad Pública (SIGRIP), señaladas en el acápite 8 de la presente Política y desarrolladas a partir el Programa de Transparencia y Ética Pública y en armonía con el Modelo de Gestión Jurídica Anticorrupción o el que lo sustituya: Política para la Gestión Integral de Riesgos de la entidad; Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP); Política Antisoborno; Política Antifraude; Procedimiento para la gestión de los conflictos de intereses; Manual de Debida Diligencia en el Conocimiento de las Contrapartes; Procedimiento para el reporte de operaciones sospechosas; y el Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

9.3. Materialización del riesgo

Se indican a continuación acciones y mecanismos frente a la materialización de riesgos, asociados a la fuente de la identificación y categoría de riesgos.

Tipología de riesgos	Acciones a emprender
Riesgos de Gestión y fiscales	**Primera Línea de Aseguramiento**: Activar y ejecutar inmediatamente el plan de contingencia frente a materialización de riesgos. Informar en el reporte trimestral de monitoreo a la Oficina Asesora de Planeación la materialización de riesgos y la revaloración del riesgo analizando cambios en probabilidad e impacto, controles y tratamiento. **Segunda Línea de Aseguramiento** Verificar que la primera Línea de Aseguramiento implementó el plan de contingencia Incorporar la materialización en informe de monitoreo y comunicar al Comité Institucional de Gestión y Desempeño. Acompañar metodológicamente la revaloración del riesgo si aplica. **Tercera Línea de Aseguramiento** Identificar posibles cambios o inclusión de seguimientos o auditorías en el plan anual de auditorías, dada la materialización y la actualización de mapa de riesgos si aplica.
Riesgos para la Integridad Pública	**Primera Línea de Aseguramiento** Informar a las autoridades de la ocurrencia del hecho de corrupción. Activar y ejecutar inmediatamente el plan de contingencia frente a materialización de riesgos. Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles, para su ajuste si aplica. Llevar a cabo un monitoreo permanente. **Segunda Línea de Aseguramiento** Incorporar la materialización en informe de monitoreo y comunicar a la Alta Dirección (Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno). Acompañar metodológicamente la revaloración del riesgo si aplica.

Tipología de riesgos	Acciones a emprender
	Verificar si se tomaron las acciones, entre ellas los controles de reporte ante autoridades correspondientes y si se actualizó el mapa de riesgos de corrupción. **Tercera Línea de Aseguramiento** Verificar que se haya gestado el reporte ante autoridades cuando aplique. Si el/la jefe de Control Interno es quien detecta materializaciones de riesgos de corrupción en el desarrollo de su ejercicio, deberá realizar el reporte ante autoridades y ante la Secretaría de Transparencia de acuerdo con el Decreto 338 de 2019: Por el cual se modifica el decreto 1083 de 2015, Único reglamentario del Sector de Función Pública y se crea la Red Anticorrupción. Identificar posibles cambios a inclusión de seguimientos o auditorías en el plan anual de auditorías, dada la materialización y la actualización de mapa de riesgos si aplica. **Nota:** Se deben analizar y considerar como para la materialización de riesgos de gestión, corrupción y los informes y evaluaciones de los organismos de control, que pueden indicar la ocurrencia tanto de un riesgo identificado, como la identificación de nuevos riesgos en los procesos de la entidad.
Riesgos LA/FT/FP	**Línea Estratégica** Promover y apropiar la cultura de prevención de riesgos LA/FT/FP. **Primera Línea de Aseguramiento** Identificar y reportar la inusualidad al responsable establecido en el esquema de gobernanza LA/FT/FP vigente en la entidad. Ejecutar los controles de LA/FT/FP que se les asigne, entre ellos la aplicación de la debida diligencia y reporte de operación inusual (ROI). Llevar a cabo un monitoreo permanente. **Segunda Línea de Aseguramiento** Acompañar metodológicamente la revaloración del riesgo LA/FT/FP si aplica. Gestión de alertas reportadas por la Primera Línea. Validar si el ROI tiene mérito suficiente para ser considerado ROS. Realizar el Reporte de Operaciones Sospechosas (ROS) a la UIAF. Realizar el monitoreo periódico a la gestión de la Primera Línea. **Tercera Línea de Aseguramiento**

Tipología de riesgos	Acciones a emprender
	Realizar seguimiento y evaluar de manera independiente el cumplimiento de lo establecido en la presente Política para la gestión integral de riesgos y presentar los respectivos reportes a la Alta Dirección.
Seguridad y Salud en el Trabajo	**Primera Línea de Aseguramiento** Informar oportunamente al responsable de la gestión del riesgo (Subdirector (a) Administrativo y Financiero) acerca de los peligros y riesgos latentes en su proceso. **Segunda Línea de Aseguramiento** Verificar si se tomaron las acciones, entre ellas los controles de reporte ante autoridades correspondientes y si se actualizó la matriz de identificación de peligros y valoración de riesgos. **Tercera Línea de Aseguramiento** Verificar que se haya gestado el reporte ante autoridades cuando aplique.
Riesgos ambientales	**Primera Línea de Aseguramiento** Informar oportunamente al responsable de la gestión del riesgo (Subdirector (a) Administrativo y Financiero). **Segunda Línea de Aseguramiento** Verificar si se tomaron las acciones, entre ellas los controles de reporte ante autoridades correspondientes. **Tercera Línea de Aseguramiento** Verificar que se haya gestado el reporte ante autoridades cuando aplique.
Riesgos Contractuales	Se gestionan atendiendo la matriz de riesgos de cada proceso contractual y lineamientos de Colombia Compra Eficiente. **Primera Línea de Aseguramiento** Informar oportunamente al responsable de la gestión contractual (Jefe Oficina Jurídica). **Segunda Línea de Aseguramiento** Verificar si se tomaron las acciones, entre ellas los controles de reporte ante autoridades correspondientes. **Tercera Línea de Aseguramiento** Verificar que se haya gestado el reporte ante autoridades cuando aplique.

Tipología de riesgos	Acciones a emprender
Riesgos de seguridad de la información	**Primera Línea de Aseguramiento** Informar del incidente de seguridad de la información que haya ocurrido al responsable de Seguridad de la Información. Informar en el reporte trimestral de monitoreo a la Subdirección de Informática y Sistemas. Revalorar el riesgo analizando cambios en probabilidad e impacto, controles y tratamiento. **Segunda Línea de Aseguramiento** Incorporar la materialización en informe de monitoreo y comunicar al Comité Institucional de Gestión y Desempeño. Acompañar metodológicamente la revaloración del riesgo si aplica. En caso de ser necesario se debe reportar la materialización del riesgo como incidente de seguridad ante la instancia correspondiente (Csirt Gobierno, Csirt Distrito o Superintendencia de Industria de Comercio -SIC-) en concordancia con el procedimiento de gestión de incidentes de seguridad de la información GT-P8 **Tercera Línea de Aseguramiento** Identificar posibles cambios o inclusión de seguimientos o auditorías en el plan anual de auditorías, dada la materialización y la actualización de mapa de riesgos si aplica.

En el caso de los riesgos de seguridad de la información, la materialización del riesgo se entenderá como la ocurrencia de un incidente de seguridad de la información, el cual deberá ser gestionado conforme al procedimiento institucional de gestión de incidentes de seguridad de la información vigente. Así, la atención del incidente no sustituye la gestión del riesgo; por el contrario, los incidentes de seguridad deberán ser utilizados como insumo obligatorio para la actualización de las matrices de riesgos, la reevaluación del riesgo residual y la definición o fortalecimiento de controles, con el fin de prevenir su recurrencia. Finalmente, es importante señalar que las lecciones aprendidas derivadas de la gestión de incidentes de seguridad de la información deberán ser consideradas por la Primera y Segunda Línea de Aseguramiento, como parte del proceso de mejora continua del Sistema de Gestión Integral del Riesgo.

Por otra parte, cuando la materialización de cualquier tipo de riesgo comprenda hechos que puedan constituir una presunta falta disciplinaria, un incumplimiento de los deberes funcionales o una infracción al régimen legal aplicable a servidores públicos o contratistas, el líder del proceso, en su calidad de Primera Línea de Aseguramiento, y los gestores de riesgos como Segunda Línea, deberán documentar de manera completa el evento y remitir o compulsar copias a la Oficina de Control Disciplinario Interno, para que esta, en ejercicio de sus competencias, evalúe la procedencia de iniciar una actuación disciplinaria conforme a lo establecido en la Ley 1952 de 2019 y demás normas que la modifiquen o sustituyan o inicie la adopción de medidas correctivas a las que haya lugar.

Cabe mencionar que esto no supone de manera automática la determinación de responsabilidad, sino que busca garantizar la trazabilidad del evento, la coordinación entre instancias y la observancia de los principios de legalidad, debido proceso, transparencia e integridad que rigen la gestión pública.

10. LINEAMIENTOS PARA LA INFORMACIÓN, COMUNICACIÓN Y CONSULTA

El componente de información, comunicación y consulta respalda de manera transversal el Modelo Integrado de Gestión y particularmente la Gestión del riesgo en la dimensión 7 asociada al Sistema de Control Interno, procurando el conocimiento generalizado y sostenibilidad en la apropiación del modelo en la Secretaría Distrital de Desarrollo Económico. Con este propósito se definen las siguientes líneas operativas:

- Deberá ser un proceso participativo, teniendo en cuenta las necesidades de las partes interesadas, de modo tal que las acciones emprendidas para mitigar los riesgos identificados, contribuyan a mejorar el desempeño de la entidad.
- El Mapa de Riesgos de Corrupción se debe publicar en la sede electrónica de la Secretaría o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año. Durante el año de su vigencia se podrá modificar o ajustar las veces que sea necesario. Para tal fin el líder del proceso deberá informar a la Oficina Asesora de Planeación y ésta a su vez a la Oficina de Control Interno. Considerando la criticidad del riesgo, se debe analizar su socialización en Comité Institucional de Gestión y Desempeño o Comité Institucional de Coordinación de Control Interno.
- Se realizará también la publicación de la gestión de riesgos en la Intranet, en el módulo de Sistema de Gestión de la Entidad.
- El proceso de socialización se llevará a cabo mediante distintos mecanismos de comunicación institucional como correo electrónico, intranet, sede electrónica, mesas de trabajo, entre otros, promoviendo el despliegue y conocimiento de los roles de las líneas de Aseguramiento y resultados periódicos de la gestión de riesgo.
- Los gestores de riesgo, o quien deleguen los líderes de proceso, deberán participar de manera proactiva en instancias distritales y nacionales para la socialización de buenas prácticas en materia de gestión de riesgos.
- Los líderes de proceso que requieran acompañamiento técnico en la gestión de riesgos, deberán solicitar el acompañamiento a través del/de la jefe del área en la que se ubica el rol de Segunda Líneas de Aseguramiento que aplique para la tipología de riesgo en cuestión.
- Las necesidades de sensibilización deberán integrarse al Plan Institucional de Capacitación y demás herramientas de gestión que se consideren, para el fortalecimiento de capacidades de la suma del talento humano: servidores públicos y contratistas.

11. EVALUACIÓN DE LA MADUREZ DE LA GESTIÓN DEL RIESGO

Los niveles de madurez en un modelo de gestión del riesgo constituyen un mecanismo de autoevaluación institucional que permite a la entidad medir, de manera sistemática y progresiva, el grado de integración, consistencia y efectividad de la gestión del riesgo en la estrategia, los procesos, la cultura organizacional

y la toma de decisiones, con base en los componentes y principios del marco COSO ERM (2017). Para tal efecto, la Secretaría deberá realizar un diagnóstico periódico de madurez, mediante la evaluación de los componentes de Gobierno y Cultura; Establecimiento de la estrategia y los objetivos; Desempeño; Revisión y monitorización; e Información, Comunicación y Reporte, a partir de criterios estructurados de acuerdo con las disposiciones de Función Pública e implementados progresivamente:

Tabla 12. Criterios evaluación del madurez de la gestión de riesgos

Componente	Principios
Gobierno y Cultura	Supervisión de riesgos a través del consejo de administración.
	Establece estructuras operativas
	Define la cultura deseada
	Demuestra compromiso con valores clave
	Atrae, desarrolla y retiene a profesionales capacitados
Establecimiento de la estrategia y objetivos	Analiza el contexto (externo e interno)
	Define el apetito del riesgo
	Evalúa estrategias alternativas
	Formula objetivos estratégicos y operacionales
Desempeño	Identifica y describe el riesgo
	Evalúa el riesgo inherente
	Diseña controles efectivos
	Prioriza riesgos
	Desarrolla visión integral
Análisis y monitorización	Evalúa los cambios significativos
	Revisa el riesgo y el desempeño
	Persigue la mejora de la gestión del riesgo
Información, Comunicación y Reporte	Aprovecha la información y la tecnología
	Comunica información sobre riesgos
	Informa sobre el riesgo, la cultura y el desempeño

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del Departamento Administrativo de la Función Pública (versión 7, 2025).

Esta evaluación será liderada por la Segunda línea de Aseguramiento o la función de gestor de cumplimiento, con el acompañamiento de la Oficina de Control Interno en su rol de aseguramiento, para que sea presentada a la Alta Dirección en el marco del Comité Institucional de Coordinación de Control Interno, al menos una vez al año o cuando se presenten cambios significativos en el contexto institucional, con el fin de identificar brechas, definir acciones de mejora y fortalecer de manera continua la gestión del riesgo de la entidad.

Versión	ELABORÓ	REVISÓ	APROBÓ	FECHA
08	Paola Andrea Pardo Cuervo Contratista Oficina Asesora de Planeación	Lady Sorany Laiton Linares Jefe de Oficina Oficina Asesora de Planeación Jimmy Alejandro Escobar Castro Coordinador Equipo MIPG Oficina Asesora de Planeación	Comité Institucional Coordinación de Control Interno	29/12/2025

CONTROL DE CAMBIOS

CAMBIOS EN EL DOCUMENTO	RESPONSABLE	FECHA	VERSIÓN
Estandarización de la guía por resolución 184	Jefe Oficina Asesora de Planeación	29/04/2015	01
1 Modificación por resolución No 751	Jefe Oficina Asesora de Planeación	16/11/2017	02
Ajuste de la Guía por cambio de la metodología del DAFP	Jefe Oficina Asesora de Planeación	11/2018	03
Se ajustaron definiciones alineándolas a las presentes en la ISO 31000:2018, se incluye numeral 3.3 Criterios que Debe Contener un Control, se incluye nota en valoración de Jefe Oficina Asesora de Planeación	Jefe Oficina Asesora de Planeación	03/04/2020	04
Actualización numeral 6.1 seguimiento al incluir la necesidad de elaboración de un plan de mejoramiento luego de la materialización de un riesgo	Jefe Oficina Asesora de Planeación	01/2021	05
Adecuación y adaptación de lineamientos de 2020 Guía para la administración del riesgo y el diseño de controles en entidades públicas v5. La Política se establece como una orientación estratégica en la administración de riesgos de la entidad y se desliga de elementos operativos frente a la antigua Guía de administración de riesgo PE-P5-GU1 Versión: 5 que incorporaba la Política de Riesgos.	Jefe Oficina Asesora de Planeación Comité Institucional Coordinación de Control Interno- Sesión del 19/08/2022	19/08/2022	06
Inclusión de las categorías de riesgos ambientales, fiscales y seguridad de la información. Armonización del documento en los diferentes capítulos de la Política, relacionados con los objetivos, alcance, niveles de responsabilidad, metodologías y monitoreo, por cada tipo de riesgo. Ajuste en el numeral de monitoreo, respecto a los plazos para generar el informe por parte de la segunda línea de defensa. Vinculación de las acciones por cada línea de defensa en el capítulo de materialización del riesgo. Eliminación del capítulo de articulación estratégica.	Jefe Oficina Asesora de Planeación	19/06/2024	07
Actualización de los componentes con base en la expedición de la séptima versión de la Guía para la gestión integral de riesgos en entidades públicas del Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones.	Jefe Oficina Asesora de Planeación	29/12/2025	08


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