DIRECCIONAMIENTO ESTRATÉGICO

DOCUMENTO TÉCNICO POLÍTICA Y METODOLOGÍA DE RIESGOS

DIES-DT-03

V.4

2026-04-17

Unidad Administrativa Especial de Catastro Distrital -UAECD-
AV. Carrera 30 N0. 25 90, Torre B Piso 2
+57 (601) 2347600
Código postal: 111311

ALCALDÍA MAYOR DE BOGOTÁ D.C.	**DOCUMENTO TÉCNICO POLÍTICA Y METODOLOGÍA DE RIESGOS**
	Proceso: Direccionamiento Estratégico

TABLA DE CONTENIDO

Listado de imágenes

Listado de tablas

1. OBJETIVO

Definir los lineamientos generales de la administración de riesgos de la Unidad, que guíen el accionar de los funcionarios, en el tratamiento de los riesgos de gestión o generales, seguridad de la información, fiscales y riesgos para la integridad pública.

2. DESARROLLO

Con el propósito de continuar con la implementación de la mejora permanente relacionada con la administración del riesgo en la UAECD, se ha elaborado esta metodología para dar claridad sobre las etapas en la gestión del riesgo que se deben abordar por cada uno de los responsables de procesos, la cual considera lo establecido en la normatividad aplicable, el modelo integrado de planeación y gestión MIPG, y el sistema de gestión de riesgos para la integridad pública (SIGRIP) de acuerdo a la guía para la gestión integral del riesgo en entidades públicas, del Departamento Administrativo de la Función Pública (DAFP), versión 7 de 2025.

En el modelo integrado de planeación y gestión-MIPG las siguientes políticas se relacionan con la administración de riesgos y diseño de controles por su relación o contribución a la gestión institucional: planeación institucional, gestión presupuestal y eficiencia del gasto público, compras y contratación pública, fortalecimiento organizacional y simplificación de procesos, servicio al ciudadano, seguridad digital, transparencia, acceso a la información pública y lucha contra la corrupción, integridad, seguimiento y evaluación del desempeño institucional y control interno.

A. CONSIDERACIONES GENERALES

- **Alcance de la metodología de riesgos**

Esta metodología aplica para riesgos de gestión, seguridad de la información, fiscales y riesgos para la integridad pública.

Para temas asociados a Seguridad y salud en el trabajo, Continuidad de negocio, Contratación, Proyectos de inversión, la gestión de riesgos deberá desarrollarse de acuerdo con los lineamientos normativos y legales específicos aplicables.

- **Marco normativo gestión del riesgo**

A continuación, se presenta un marco de referencia asociado a la gestión del riesgo.

Tabla 1. Normatividad relevante

SISTEMA	REGULACIÓN	OBSERVACIÓN
Gestión de Calidad	ISO 9001 – 2015	Sistemas de Gestión de la Calidad – Requisitos
	Ley 1753 de 2015, artículo 133	"Intégrense en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad de que trata la Ley 872 de 2003 y de Desarrollo Administrativo de que trata la Ley 489 de 1998. El Sistema de Gestión deberá articularse con los Sistemas Nacional e Institucional de Control Interno consagrado en la Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998, de tal manera que permita el fortalecimiento de los mecanismos, métodos y procedimientos de control al interior de los organismos y entidades del Estado. El Gobierno Nacional reglamentará la materia y establecerá el modelo que desarrolle la integración y articulación de los anteriores sistemas, en el cual se deberá determinar de manera clara el campo de aplicación de cada uno de ellos con criterios diferenciales en el territorio nacional."
	Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Control Interno	Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones
	Decreto 1499 de 2017 y en el Manual Operativo del MIPG	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
	Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Seguridad de la información	NTC/ISO/IEC 27001 de 2013	Sistema de Gestión de seguridad de la información.
	Norma ISO 31000:2011	Gestión del riesgo – principios y directrices.
	Norma ISO 27005:2011	Gestión del riesgo en la seguridad de la información.
	Documento	Política Nacional de Seguridad Digital

	CONPES 3854 de 2017	

	Ley estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentado por el Decreto 1377 de 2013.
	CONPES 3854 del 11 de abril de 2016, 3.2. Estrategia de gestión de Riesgos de seguridad digital	El Ministerio de Tecnologías de la Información y las Comunicaciones diseñará un modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco.
	Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 del 2015, decreto único reglamentario del sector de tecnologías de la información y las telecomunicaciones.
Integridad pública	Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública". En su Art. 73 establece la obligatoriedad.
	Decreto 124 de 2016	Por el cual se sustituye el Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano.
	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. Programa de Transparencia y Ética Pública.
	Decreto 1122 de 2024	Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.
Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT)	Ley 599 de 2000 modificado parcialmente por la Ley 1453 de 2011 y Ley 1762 de 2015	Por el cual se expide el código penal, en su capítulo quinto "Del Lavado de Activos" establece en su artículo 323 el delito de lavado de activos y las penas aplicables según las tipologías del hecho.
	Ley 964 de 2005	Establece los criterios y parámetros mínimos que las entidades vigiladas deben atender en el diseño, implementación y funcionamiento del mencionado sistema
	Ley 1121 de 2006	Por medio de la cual se dictan normas para la prevención, detección, investigación y sanción de la Financiación del Terrorismo, las responsabilidades de entidades o personas obligadas a cumplir con las normas del Estatuto Orgánico del Sistema Financiero (artículos 102 a

		107); la identificación plena de contratistas de entidades de Estado.
	Ley 1762 de 2015	Por medio de la cual se adoptan instrumentos para prevenir, controlar y sancionar el contrabando, el lavado de activos y la evasión fiscal, para personas naturales y servidores públicos.
	CONPES 4042 de 2021	Por medio de la cual se adoptan la "Política Nacional Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva" enfocado en mejorar la productividad del Sistema Antilavado de Activos y Contra la Financiación del Terrorismo (ALA/CFT) planteando cuatro objetivos específicos: 1) Promover la gestión del conocimiento permanente entre los actores del Sistema ALA/CFT, 2) Fortalecer el marco normativo ALA/CFT adaptando estándares internacionales, 3) mejorar la gestión de la información y lograra mejores estándares de calidad, seguridad y oportunidad, y 4) consolidar procesos de coordinación y cooperación que optimice las labores de prevención, detección, investigación, judicialización y persecución de los activos.
	Circular Externa No. 100-000016 de 2020	Por medio de la cual se establecen procedimiento para implementar SAGRILAFT, incluyendo sistema de autocontrol y gestión del riesgo LA/FT/FPADM, y procedimiento de Debida Diligencia y Debida Diligencia Intensificada.

Fuente: Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP y Gerencia de Tecnología - GT.

- **Términos y definiciones**

Tomados de la Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, versión 7 y el documento CONPES 3854 de 2017.

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza cibernética:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).
- **Ataque cibernético:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (CONPES 3854).
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:
  a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
  b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata), pero se asocia a la misma causa inmediata.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
  Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, 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.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **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. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015)
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **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)
- **Gestión del Riesgo Fiscal:** Son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).
- **Gestor público:** Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales.
- **Gestor Fiscal:** Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en

orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique).

- **Integridad:** Propiedad de exactitud y completitud.
- **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
- **Lavado de activos:** El artículo 323 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien "adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades [relacionadas con un delito fuente], o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito". El Lavado de Activos puede darse por: colocación, ocultamiento e integración.
- **Patrimonio público:** Conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).
- **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.
- **Punto de riesgo:** Actividades en las que se genera riesgo.
- **Recurso público:** Los dineros comprometidos y ejecutados en ejercicio de la función pública.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo 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.
- **Riesgos para la integridad:** Toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas.
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **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.
- **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)

- **Soborno entrante:** Ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.
- **Soborno saliente:** Ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

B. POLÍTICA Y METODOLOGÍA DE RIESGOS

1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Como primer paso en la aplicación de la metodología, se define una Política para la administración del riesgo, la cual es aprobada por la Alta Dirección en el Comité Institucional de Coordinación de Control Interno de la Unidad.

1.1. Descripción de la política

La Unidad Administrativa Especial de Catastro Distrital se compromete a dar tratamiento, manejo y seguimiento de los riesgos de gestión, seguridad de la información, fiscales y riesgos para la integridad pública, que puedan afectar de manera negativa el alcance de los objetivos estratégicos y los objetivos de procesos de la cadena de valor; partiendo del análisis del contexto, la consideración de riesgos emergentes, la disposición de recursos y medidas requeridas y la determinación de los niveles de responsabilidad y autoridad para el manejo de los riesgos.

La gestión de riesgos se realizará bajo la metodología y procedimiento de la gestión del riesgo del proceso de direccionamiento estratégico, acorde con lo establecido por el sistema de gestión de riesgos para la integridad pública (SIGRIP) de acuerdo con la guía para la gestión integral del riesgo en entidades públicas del Departamento Administrativo de la Función Pública.

La Entidad también se compromete a gestionar otro tipo de riesgos como los de Seguridad y salud en el trabajo, continuidad de negocio, contratación, proyectos de inversión, desarrollando su gestión de acuerdo con los lineamientos normativos y legales específicos aplicables.

1.2. Objetivo de la política

Establecer los lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en la Unidad Administrativa Especial de Catastro Distrital que puedan afectar el logro de los objetivos institucionales, en concordancia con el modelo integrado de planeación y gestión (MIPG) y las mejores prácticas internacionales del sistema de gestión de riesgos para la integridad pública (SIGRIP) de acuerdo a la guía para la gestión integral del riesgo en entidades públicas del Departamento Administrativo de la Función Pública (DAFP).

Esta política tiene como propósito fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público, asegurando la integridad, transparencia y eficiencia en la administración de recursos. Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión

proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua y la confianza ciudadana en la entidad según su ámbito de operación.

1.3. Alcance

La presente política aplica a todas las dependencias, procesos y servidores de la entidad, en todos los niveles jerárquicos y áreas misionales, estratégicas y de apoyo. Incluye la gestión de riesgos en la planeación, ejecución presupuestal, prestación de servicios, adopción de tecnologías, fortalecimiento organizacional, así como en la implementación de proyectos y programas institucionales.

1.4. Análisis de contexto interno y externo

La Entidad cuenta con una herramienta DOFA (debilidades, oportunidades, fortalezas, amenazas) para la identificación del contexto, como factores externos se identifican aquellos que representen una amenaza o una oportunidad para la entidad en temáticas como lo: económico, social y cultural, tecnológico, político, legales y reglamentarios, medio ambientales y de comunicación externa; como factores internos aquellos en el que se tienen debilidades o fortalezas en temáticas como: funciones y responsabilidades (políticas, objetivos y estrategias), personas, tecnología, estructura organizacional, financieros, relaciones con partes involucradas, estructura organizacional, diseño y ejecución de los procesos.

El contexto institucional a través de este DOFA se revisa y actualiza anualmente, el cual se toma de referencia y se ajusta de forma específica por proceso, como uno de los insumos para la identificación de riesgos.

Como punto de partida en la identificación de riesgos se toman los objetivos estratégicos y los objetivos de los procesos, para identificar los posibles riesgos que afectan su cumplimiento; asimismo, la identificación de puntos de riesgo, es decir aquellas actividades o momentos del proceso en donde existe evidencia o indicios de situaciones que pueden generar riesgo y deben mantenerse bajo control.

Se podrá tomar de referente para la identificación de riesgos, información proveniente de fuentes como auditorías internas y externas (planes de mejoramiento), necesidades y expectativas de los grupos de valor, un análisis situacional, entre otros.

1.5. Roles y responsabilidades

La definición de los roles y responsables de la gestión del riesgo en la entidad parten de lo definido por el Modelo Integrado de Planeación y Gestión – MIPG en su Manual Operativo y la Guía para la Gestión Integral de Riesgos en Entidades Públicas, de lo cual se destaca:

Línea Estratégica – Alta dirección, Comité Institucional de Gestión y Desempeño, Comité Institucional de Coordinación de Control Interno:

- Esta línea define y aprueba la Política de Administración del Riesgo en el marco del Comité Institucional de Coordinación de Control Interno, realizando el monitoreo correspondiente a partir de la información suministrada por la segunda línea.
- Evalúa como se aplica en la entidad y los cambios en el entorno que puedan generar ajustes o

riesgos emergentes.

- Determina el apetito de riesgo, analiza la gestión del riesgo y define mejoras.
- Analiza eventos y riesgos críticos.
- Decide e implementa estrategias para la gestión del riesgo y la mejora continua.
- Analiza y decide sobre el Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP.
- Aprueba los indicadores clave de riesgo y sus tolerancias.

Primera línea de defensa – Líderes de programas, procesos y proyectos y sus equipos de trabajo (en general servidores públicos en todos los niveles):

- Realiza la identificación de riesgos y el establecimiento de controles en sus diferentes procesos, proyectos o iniciativas estratégicas, así como su seguimiento acorde con el diseño de los controles, evitando su materialización.
- Ejecuta los controles operativos en el día a día.
- Gestiona los riesgos y hace seguimiento y reporte teniendo en cuenta los lineamientos y la periodicidad establecida por la segunda línea.
- Les corresponde la ejecución y monitoreo de los elementos del sistema de gestión de riesgos para la integridad pública -SIGRIP.
- Identifica y formula los indicadores clave de riesgo, realiza el seguimiento y reporte correspondiente y realiza la mejora frente a las desviaciones.

Segunda línea de defensa – Jefe de la Oficina Asesora de Planeación y Aseguramiento de Procesos, Oficial de seguridad de la información, coordinadores de equipos de trabajo que respondan de manera directa por el aseguramiento de la operación:

- Asegura que los controles y procesos de gestión del riesgo de la primera línea sean apropiados y funcionen correctamente y supervisa la eficacia e implementación de las prácticas de gestión de riesgo.
- Consolida y analiza información para evitar materializaciones de riesgo.
- Asesora a la primera línea en la gestión de riesgos.
- Acompaña, recomienda y hace seguimiento con enfoque preventivo.
- Realiza presentación de la gestión del riesgo trimestral a la línea estratégica.
- Desarrolla la función de cumplimiento en relación con el sistema de gestión de riesgos para la integridad pública-SIGRIP, de la cual presentará información sobre los riesgos a la línea estratégica, así como de los elementos que en el marco de la gestión sobre lavado de activos y financiación del terrorismo se requieran.
- Asesora en la formulación de los indicadores clave de riesgo.

La Oficina Asesora de Planeación y Aseguramiento de Procesos consolida el mapa de riesgos institucional.

Para la Unidad, se ha identificado la segunda línea de los diferentes riesgos así:

Tabla 2. Resumen de responsables de segunda línea

Tema o tipo de riesgo	Segunda línea
Gestión o generales	Oficina Asesora de Planeación y Aseguramiento de Procesos
Integridad pública - SIGRIP	Oficina Asesora de Planeación y Aseguramiento de Procesos
Fiscales	Oficina Asesora de Planeación y Aseguramiento de Procesos
Seguridad de la información	Gerencia de Tecnología – Oficial de Seguridad
Otros riesgos	
Seguridad y salud en el trabajo	Subgerencia de Talento Humano
Continuidad de negocio	Gerencia de Tecnología – Oficial de Continuidad
Contratación	Gerencia de Gestión Corporativa -Subgerencia de Contratación - Supervisores
Proyectos de inversión	Oficina Asesora de Planeación y Aseguramiento de Procesos

Fuente: Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP

Asimismo, existen otros roles responsables que aportan a la gestión del riesgo como segunda línea en los siguientes aspectos específicos:

Tabla 3. Otros responsables de segunda línea

Segunda línea	Responsabilidad
Subgerencia de Participación y Atención al Ciudadano	Monitorear las Peticiones, Quejas, Reclamos, Denuncias, Sugerencias y Felicitaciones (PQRDSF) y generar alertas sobre incumplimientos, quejas en la prestación del servicio, u otras situaciones de riesgo detectadas.
Subgerencia de Talento Humano	Monitorear el ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), y generar alertas sobre incumplimientos, situaciones críticas que afectan en clima laboral y posibles afectaciones al código de integridad, entre otros.
Gerencia de Tecnología	Monitorear el Plan Estratégico de Tecnologías de la Información (PETI) y generar alertas sobre retrasos, incumplimientos o situaciones de riesgo detectadas en materia tecnológica.
Gerencia Jurídica	Monitorear la gestión jurídica, y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en la materia.

Fuente: Oficina Asesora de Planeación y Aseguramiento de Procesos -OAPAP

La segunda línea podrá utilizar la herramienta de diagnóstico de madurez de la Guía del DAFP para proponer ante el Comité Institucional de Coordinación de Control Interno mejoras para la gestión del riesgo de la entidad.

Tercera línea de defensa – Jefe Oficina de Control Interno:

Evalúa de manera independiente y objetiva los controles, monitorea la exposición al riesgo y realiza recomendaciones con alcance preventivo, asesora en materia de control interno y sobre responsabilidades

en materia de riesgos, audita en relación con el sistema de gestión de riesgos para la integridad pública-SIGRIP, con el propósito de asesorar y recomendar mejoras, lo cual desarrollará según lo contemplado en el plan anual de auditoría y criterios definidos por esta oficina y de lo cual surjan las mejoras a realizar por las otras líneas al sistema y realiza las observaciones para la mejora sobre los indicadores clave de riesgo.

Responsable de seguridad de la información:

Asimismo, el Anexo No 4 modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas señala las responsabilidades del funcionario designado para seguridad digital, en concordancia con lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Unidad delegará la responsabilidad de gestionar los riesgos de seguridad de la información al encargado de seguridad de la información con los siguientes compromisos:

"Responsable de seguridad de la información:

- Actualizar el procedimiento para la Identificación y valoración de activos de la entidad, de acuerdo con los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, análisis, evaluación y tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.[1]" Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

1.6. Esquema metodológico y lineamientos generales

- **Pasos generales**

La implementación de la gestión del riesgo en la entidad cumple con los aspectos metodológicos siguiendo los lineamientos de la guía para la gestión integral del riesgo en entidades públicas del DAFP, a saber:

Paso 1. Identificación y descripción del riesgo: Identificación de puntos de riesgo, áreas de impacto, áreas de factores de riesgo, descripción del riesgo.

Paso 2. Análisis del riesgo inherente: Determinación de la probabilidad, impacto y análisis de severidad.

Paso 3. Diseño y análisis de controles: Descripción valoración de controles.

Paso 4. Valoración de riesgo residual: Aplicación de la efectividad de los controles, desplazamiento en la matriz de severidad y consolidación del mapa de riesgos.

Estos pasos metodológicos se describen en detalle en el numeral de Metodología, en los cuales se encuentran entre otros: los factores de riesgo, las tablas de probabilidad e impacto, la matriz de severidad y la tabla de valoración de controles.

El tratamiento de los riesgos de gestión, fiscales y de seguridad de la información tendrá tres escenarios

posibles: reducir, aceptar y evitar. El tratamiento a los riesgos para la integridad pública sólo tendrá dos escenarios posibles que corresponden a reducir o evitar el riesgo.

El seguimiento de los Planes de Manejo de Riesgo – PMR se realizará con periodicidad trimestral. Si bien no se desarrolla Plan de Manejo de Riesgo a aquellos riesgos situados en zona de riesgo residual baja, estos se monitorean con el seguimiento periódico.

En el caso de los riesgos de seguridad de la información, estos se gestionan siguiendo los lineamientos para la gestión de riesgos en entidades públicas, basados en el modelo de seguridad y privacidad de la información, la guía de orientación para la gestión de riesgos de seguridad digital en el gobierno nacional, territoriales y sector público y el modelo de gestión de riesgos de seguridad digital del Ministerio de tecnologías de la información y las comunicaciones.

1.7. Niveles de aceptación del riesgo – apetito del riesgo

Los riesgos ubicados en zonas de riesgo residual: extremo, alto y moderado, no permiten aceptación del riesgo, razón por la cual la Unidad generará planes de tratamiento.

Los riesgos para la integridad pública no admiten aceptación del riesgo, siempre debe conducir a realizar el tratamiento correspondiente.

Sobre los riesgos ubicados en zona baja, la opción de tratamiento será aceptar el riesgo, entendiendo que luego de su valoración inherente y la aplicación de controles, el riesgo está en un nivel aceptable; no obstante, pese a no generar plan de manejo o tratamiento del riesgo – PMR, trimestralmente se deberá identificar si se presentó o no materialización identificando si requiere realizar ajustes o mejoras.

Adicional a esta determinación, los riesgos de gestión cuentan con indicadores clave de riesgo con límites de tolerancia establecidos por los responsables de proceso, a los cuales se realiza seguimiento trimestral dentro del reporte de las matrices de riesgo.

1.8. Comunicación y consulta de la política

La Política para Administración del Riesgo es aprobada por la alta dirección en el Comité Institucional de Coordinación de Control Interno y seguirá el trámite de gestión de documentos que establece el Manual del Sistema de Gestión Integral del proceso Direccionamiento Estratégico, por esta razón, se encontrará disponible para consulta a través del Sistema de Gestión Integral –SGI- y también para consulta en la página web de la Unidad.

1.9 Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP

En cumplimiento de los lineamientos para la gestión de riesgos establecidos en los programas de transparencia y ética pública, el SIGRIP en la Unidad considera a la política de administración del riesgo, como un compromiso que integra, los riesgos de gestión, fiscales, de seguridad de la información y los riesgos para la integridad pública.

Adicionalmente y de forma específica, la Unidad aprueba la siguiente política complementaria:

Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de armas de destrucción masiva (ALA/CFT/CFP), antisoborno y antifraude

La Unidad se compromete a:

- Generar una cultura de prevención y mitigación del **lavado de activos, la financiación del terrorismo y la proliferación de armas de destrucción masiva y del delito de soborno y fraude.**
- Prohibir y rechazar cualquier práctica asociada.
- Cumplir la normatividad en la materia.
- Actuar con debida diligencia en el conocimiento de las contrapartes.
- Promocionar la denuncia de cualquier actividad asociada a las señales de alerta que la entidad defina.
- Informar las consecuencias del incumplimiento de esta política.

El SIGRIP se articula con los lineamientos del presente documento de política y metodología, su contexto, roles y responsabilidades.

El SIGRIP contempla como elementos: La presente política de administración del riesgo, la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo, en relación con lo cual, este documento se complementa con la documentación específica en que se desarrollen el principio de debida diligencia, la gestión de conflictos de interés, el reporte de operaciones sospechosas y los canales de denuncias de corrupción.

Los registros que se generen derivados de la operación de procedimientos o instructivos relacionados, se conservarán de acuerdo con los lineamientos de gestión documental y las normas en la materia.

2. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

PASO 1. Identificación y descripción del riesgo

Los riesgos se identifican a partir del análisis de los objetivos de los procesos, sus actividades clave y los productos o resultados generados, los cuales pueden consultarse en el documento de caracterización.

Se identifica además el área de impacto, la cual puede ser económica y/o reputacional, a la que se ve expuesta la entidad en el caso de materializarse un riesgo.

Se determinan los factores de riesgo, que son fuentes generadoras o circunstancias que aumentan la probabilidad de que ocurra un evento de riesgo.

Tabla 4. Factores de riesgo

Factor	Definición	Descriptores ejemplo
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización.	Falta de aplicación de los procedimientos Falta segregación de funciones Falta de supervisión o interventoría Alta rotación o insuficiencia de personal Acciones contrarias a las leyes o acuerdos contractuales Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP)	Eventos relacionados con transacciones y operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.	Contrapartes de la entidad (naturales o jurídicas) Productos (bienes o servicios) que oferta/requiere Canales utilizados para la operación jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude interno Soborno Gestión inadecuada de conflictos de interés Corrupción Hurto de activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos Caída de sistemas de información y aplicaciones Caída de redes Errores en hardware o software Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes Incendios Inundaciones Daños a activos fijos
Eventos externos	Eventos por situaciones externas que afectan la entidad.	Fraude externo Suplantación de identidad Atentados,

		vandalismo , orden público

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7, con ajustes

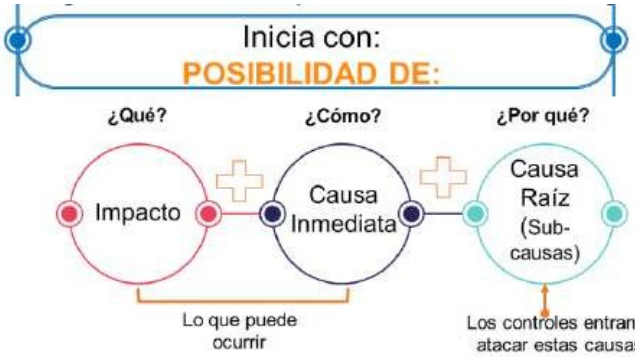
Descripción del riesgo

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

Inician con la frase “Posibilidad de” ya que son eventos potenciales.

La estructura propuesta para la redacción del riesgo es la siguiente:

Imagen 1. Estructura para la redacción del riesgo



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

El impacto corresponde a las consecuencias (económica y/o reputacional) que puede ocasionar la materialización del riesgo.

La causa inmediata corresponde a circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, no son la causa principal.

La causa raíz corresponde a la razón principal por la cual se puede presentar el riesgo. De esta causa raíz pueden surgir subcausas.

Dentro de las recomendaciones para la redacción del riesgo dadas por el DAFP, se tienen:

- No describir como riesgos omisiones ni desviaciones del control. Ejemplo: errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos. Ejemplo: Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- No describir riesgos como la negación de un control. Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que puede existir son causas transversales. Ejemplo: Pérdida de

expedientes. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

En el formato de matriz de riesgos se cuenta con un árbol de problemas como apoyo en la identificación de los riesgos de gestión, fiscales y para la integridad pública.

Descripción de riesgos fiscales

El riesgo fiscal se define como el efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Efecto dañoso: El daño que se generaría sobre los recursos, bienes y/o intereses patrimoniales de naturaleza pública al ocurrir un evento potencial.

Evento potencial: Hechos inciertos, potencial acción u omisión que podría generar daño sobre los recursos, bienes y/o intereses patrimoniales de naturaleza pública.

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño)

- Identificar puntos de riesgo y circunstancias inmediatas

Para esta tipología de riesgos, es importante analizar en qué procesos se realiza gestión fiscal, entendida como las actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado.

En los procesos en los que se realice gestión fiscal, se deben identificar los puntos de riesgo, que son situaciones/actividades sobre los bienes, recursos o patrimonio en donde potencialmente hay riesgo, para lo cual es útil el análisis de advertencias, alertas, hallazgos o fallos con responsabilidad fiscal en firme relacionados con la entidad de los últimos 5 años, a través de la consulta de los planes de mejoramiento de la Contraloría de Bogotá u otros documentos en los que se hayan encontrado hallazgos y/o fallos con responsabilidad fiscal de los últimos años.

También se deberán identificar las circunstancias inmediatas, que son las situaciones en las que se presenta el riesgo, para lo cual existe como apoyo un Catálogo Indicativo y Enunciativo de Puntos de Riesgo Fiscal y Circunstancias Inmediatas de la Guía DAFP.

- Identificar áreas de impacto

Los riesgos fiscales se relacionan con tres expresiones según DAFP: bienes públicos, recursos públicos e intereses patrimoniales de naturaleza pública:

Bienes públicos: Son todos aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público (aquellos cuyo uso pertenece a todos los habitantes del territorio nacional) y bienes

fiscales (aquellos que están destinados al cumplimiento de las funciones o servicios públicos).

Recurso público: Son los dineros comprometidos y ejecutados en ejercicio de la función pública.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

- Identificar el efecto económico

Para los riesgos fiscales el área de impacto o afectación siempre es económica.

No todos los riesgos con afectación económica son fiscales por lo que se requiere realizar el análisis, por ejemplo, riesgos como los de daño antijurídico (pago de condenas y conciliaciones) y aquellos generados por causas exógenas no relacionadas con acción u omisión de los gestores públicos, que son hechos de fuerza mayor, caso fortuito o hecho de un tercero, multas por hechos que no comportan gestión fiscal, pérdida de bienes por riesgo normal o aceptable.

- Identificar la causa raíz o potencial hecho generador

Según la Auditoría General de la República la causa raíz es cualquier evento potencial (acción u omisión) que de presentarse provocaría menoscabo, disminución, perjurio, detrimento, pérdida o deterioro.

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. Los controles deben apuntar a atacar esta causa.

Para los riesgos fiscales la estructura propuesta por DAFP es:

Imagen 2. Descripción riesgo fiscal y ejemplo 1

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **recursos de la entidad**	por la generación de intereses moratorios en contrato de arrendamiento	a causa de la omisión en el pago oportuno del canon pactado.

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Administración de inmuebles en arrendamiento al servicio de la entidad
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Pago de intereses moratorios en contrato de arrendamiento
Área de Impacto: (patrimonio público afectado)	Recursos públicos de la entidad
Efecto económico: (potencial daño al patrimonio)	Disminución de recursos disponibles equivalente al monto pagado por concepto de intereses moratorios
Causa raíz: (potencial acción u omisión)	Omisión de pago oportuno del canon de arrendamiento

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

Como sugerencia para la estructuración del riesgo, estos inician con “Posibilidad de”.

El impacto corresponde al que, al efecto dañoso sobre el área de impacto (bienes, recursos, intereses patrimoniales de naturaleza pública).

La circunstancia inmediata corresponde al cómo, aquella situación en la que se presenta el riesgo, pero no es su causa principal.

La causa raíz corresponde al por qué, es el evento (acción u omisión) que de presentarse genera directamente el daño, si el hecho no se presenta no se genera el daño.

Imagen 3. Descripción riesgo fiscal y ejemplo 2

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **intereses patrimoniales**	por prescripción de los términos para la exigibilidad de obligaciones tributarias en mora	a causa de errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Gestión de cobro a contribuyentes en mora del pago de sus obligaciones tributarias.
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Prescripción de los términos para la exigibilidad de las obligaciones tributarias.
Área de Impacto: (patrimonio público afectado)	Intereses patrimoniales de la entidad
Efecto económico: (potencial daño al patrimonio)	Menor recaudo de ingresos tributarios establecidos a favor de la entidad
Causa raíz: (potencial acción u omisión)	Errores en la ejecución de los procedimientos de cobro persuasivo y coactivo.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

Imagen 4. Otros ejemplos de redacción de riesgos fiscales

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

- **Descripción de Riesgos de seguridad de la información**

- Identificación de activos de seguridad de la información

Como punto de partida para los riesgos de seguridad de la información se tendrán los activos de información. La identificación de los activos de seguridad de la información corresponde a la primera línea de defensa y se realizará según lo descrito en el documento asociado a la Gestión de Activos en el Marco de la Seguridad de la Información.

Los activos en un contexto de seguridad digital son elementos como: Información, software, hardware, servicios, intangibles, infraestructura crítica cibernética nacional, recursos humanos, instalaciones, aplicaciones, servicios web, redes, información física o digital, tecnologías de la información, tecnologías de operación, que utiliza la entidad para funcionar en un entorno digital.

Para la formulación de riesgos de seguridad de la información se debe partir de la identificación de los activos de información que fueron identificados con criticidad alta y aquellos activos identificados como Infraestructura Crítico Cibernética (ICC). El responsable del proceso podrá incorporar en su mapa, riesgos sobre activos de información con criticidad diferente a alta.

En el evento de presentarse un incidente de seguridad sobre un activo o grupo de activos de información se debe tener presente lo siguiente:

a) Si el activo o grupo de activos no se encuentran identificados en el inventario general de activos o instrumento de gestión de la información pública es necesaria la actualización de estos, su valoración y su correspondiente análisis de riesgos.

b) Si no existe ningún riesgo asociado con el incidente presentado es necesario incluir el riesgo actualizando la matriz de riesgos del proceso.

Para cada activo o grupo de activos de información se podrán identificar los siguientes tres riesgos inherentes de seguridad digital: Pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos.

Para los riesgos de seguridad de la información se tomará como guía para la identificación de amenazas y vulnerabilidades lo descrito en el anexo C y Anexo D de la ISO27005:2009 las cuales se presentan al final de este documento como anexos y en donde se definen los ejemplos más comunes de amenazas y vulnerabilidades que pueden afectar un activo de información.

Se aclara que se pueden identificar amenazas y vulnerabilidades que no se encuentren asociadas en las tablas anteriormente mencionadas.

Se recomienda realizar la identificación de hasta 3 amenazas por grupo de activos de información; y para cada amenaza hasta 3 vulnerabilidades asociadas.

La descripción de riesgos de seguridad de la información parte de la identificación de los tres siguientes riesgos:

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

En la descripción de los riesgos de seguridad de la información se deben identificar las consecuencias económicas y/o reputacionales a las que se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

- **Descripción de Sistema de Riesgos para la Integridad Pública (SIGRIP)**

En la identificación de riesgos para la integridad pública se contemplan aquellos relacionados con soborno, fraude, inadecuada gestión del conflicto de interés, corrupción y Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de armas LA/FT/FP.

- Identificación de puntos de riesgo

Para LA/FT/FP, teniendo en cuenta las actividades que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio.

Para lo relacionado con corrupción y sus manifestaciones como soborno, fraude e inadecuada gestión del conflicto de interés, pueden generarse puntos de riesgo según el análisis del proceso.

- Identificación de áreas de impacto

Adicional al impacto económico y reputacional, pueden generarse consecuencias legales y de contagio.

La consecuencia legal corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños.

El contagio se expresa cuando a partes relacionadas se les materializa un riesgo de integridad pública que tiene el potencial de afectar a la entidad.

Las consecuencias legales y de contagio se analizan dentro de la afectación económica.

La consecuencia reputacional surge cuando la entidad se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción.

- Identificación de factores de riesgo

Como factores del riesgo LA/FT/FP se tiene a las contrapartes, los productos, los canales y las jurisdicciones.

Para lo relacionado con corrupción, dentro de las causas inmediatas se encuentran el soborno, el fraude, la inadecuada gestión de conflictos de interés.

La descripción del riesgo incluye la “posibilidad de”, el impacto, la causa inmediata y la causa raíz.

Imagen 5. Ejemplos referente factores de riesgo para la integridad pública

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	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 […]".	
	Soborno Saliente	Ofrecer, prometer o dar 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	
Impacto	**Causa inmediata**		**Causa raíz**
		persona actúe o se abstenga de actuar […]".	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere 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	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7

Como ejemplos específicos aplicados, DAFP relaciona:

- *Posibilidad de afectación económica por Corrupción en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico*
- *Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios.*
- *Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa*

de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la entidad.

- *Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.*
- *Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.*

Imagen 6. Ejemplos referente riesgos LA/FT/FP

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

Como ejemplos específicos aplicados a temas de LA/FT/FP, DAFP relaciona:

- *Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.*
- *Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.*
- *Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.*

PASO 2. Análisis del riesgo inherente

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, lo cual permite establecer la zona de Riesgo Inherente.

- **Determinar la probabilidad**

La probabilidad es la posibilidad de ocurrencia del riesgo y está asociada a la exposición al riesgo, del proceso o actividad que se está analizando. Está dada al evaluar con qué frecuencia se realiza la actividad que conlleva el riesgo por año, es decir, con base en el producto/activo seleccionado identificar con qué frecuencia se genera según el número de veces que se realiza en un año.

A continuación, se presentan los Criterios para definir el nivel de probabilidad:

Imagen 7. Criterios para definir la probabilidad

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

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7, con ajustes propios

- **Análisis del impacto**

Son las consecuencias que se pueden ocasionar por la materialización de un riesgo. Las variables principales de análisis son los impactos: económicos, reputacionales, legales y de contagio.

La consecuencia legal corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños.

El contagio corresponde a la posibilidad de que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando a partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar a la entidad.

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de afectación económica.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se toma el nivel más alto.

La consecuencia reputacional, por ejemplo, surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general.

Para los riesgos fiscales el impacto siempre es económico.

A continuación, se presentan los criterios para definir el nivel de impacto:

Imagen 8. Criterios para definir el impacto

Nivel de impacto	Afectación económica	Afectación reputacional
Leve – 20%	Afectación menor a 100 SMLMV	El riesgo afecta la imagen de alguna área de la organización.
Menor – 40%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva y/o de proveedores.
Moderado – 60%	Entre 500 y 1000 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor – 80%	Entre 1000 y 5000 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 5000 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitarios sostenible a nivel país.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7, con ajustes propios

Tanto en el análisis de probabilidad como el de impacto se considera el conocimiento y experiencia del responsable y funcionarios del proceso como conocedores de este.

El nivel de impacto para los riesgos de seguridad de la información deberá ser determinado con la presencia de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo (reputacional) o cuantitativo (económico).

Para los riesgos de seguridad de la información, la probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Impacto con enfoque de derechos fundamentales

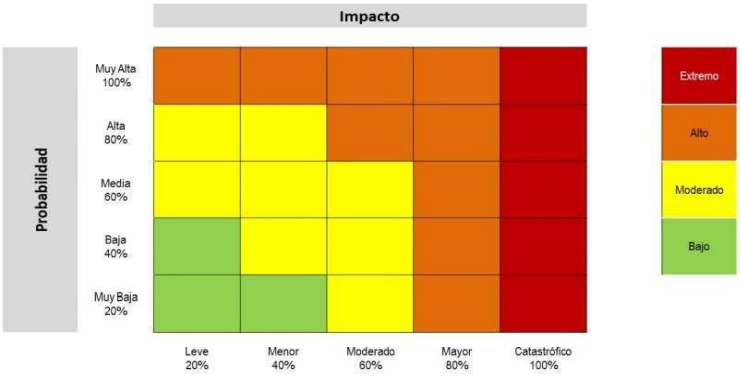
La ejecución de la actividad misional la Unidad no asegura directamente ningún derecho fundamental, sino que, en cumplimiento de su objeto, garantiza la prestación de un servicio público que podría indicarse relacionado al derecho de la propiedad por la labor misional y su aporte para mantener la información actualizada de la propiedad inmueble. Asimismo, como entidad pública, debe garantizar el derecho de toda persona de presentar consultas, solicitudes, sugerencias y reclamos frente al ejercicio de sus funciones.

Este impacto no se identifica de manera específica en el mapa de riesgos para la integridad pública, sino que, siguiendo la metodología establecida por el DAFP y la Secretaría de Transparencia, busca ser mitigado con la gestión general del riesgo.

- **Análisis de severidad – Riesgo inherente**

Se busca determinar los niveles de severidad o la zona de riesgo inherente a partir del análisis de la probabilidad y el impacto.

Imagen 9. Matriz de calor (niveles de severidad del riesgo)



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

PASO 3. Diseño y análisis de controles

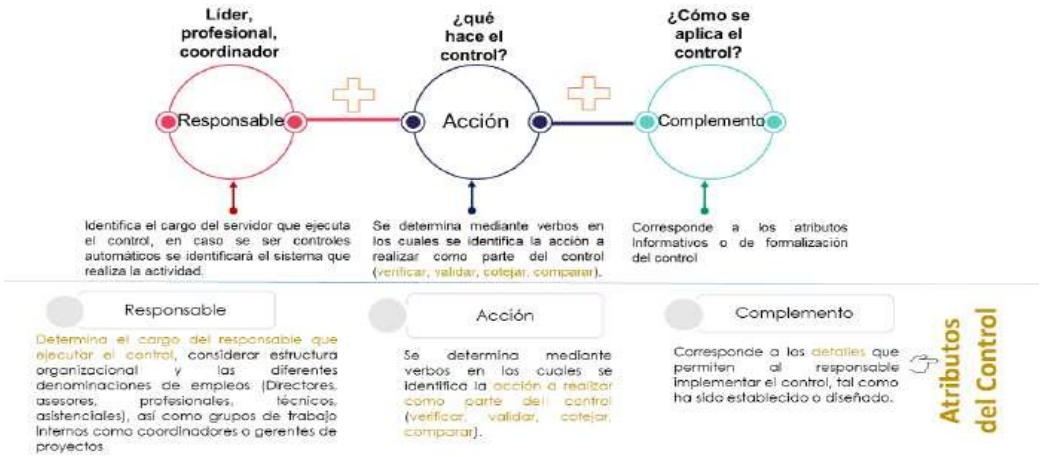
Las actividades de control son acciones con atributos específicos, documentadas a través de políticas, procedimientos u otros documentos institucionales que permiten reducir o mitigar el riesgo.

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer o en el análisis de los procedimientos, manuales, guías o documentación del proceso.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo. Las actividades de control deben tratar la causa raíz y causas identificadas y enfocarse a los factores de riesgo.

- **Estructura para la descripción del control:**

Imagen 10. Estructura para la redacción de controles



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

La identificación de controles debe tener en cuenta:

- **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identifica el sistema que realiza la actividad y el responsable de su calibración
  o parametrización.
- **Acción:** Se determina mediante verbos que indican la acción que deben realizar como parte del control, con verbos fuertes tales como: verificar, validar, cotejar, comparar, revisar, conciliar, detectar.
- **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control:

Documentación: Se refiere a la fuente del control en los documentos del proceso.
Frecuencia: Corresponde a la periodicidad con la cual se ejecuta la actividad de control, la cual puede ser periódica o por evento.

Tal como se establece en el Manual del Sistema de Gestión Integral, la periodicidad con la que se realiza el control, en la documentación del Sistema de Gestión si no se especifica, se entiende que cada vez que se desarrolle el procedimiento o instructivo se ejecuta la actividad de control.

Evidencia: Registro físico o electrónico que permite contar con la trazabilidad de la ejecución del control.
Ejecución: Establece cómo se ejecuta el control y qué acciones se toman en caso de desviaciones o las situaciones que se detecten.

- **Tipología de controles:**

Es posible identificar una tipología de controles según el momento en que se activan dentro del ciclo del proceso.

- **Control preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
  Va hacia las causas del riesgo. Buscan evitar el riesgo o reducir su probabilidad de ocurrencia.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Contribuyen a mitigar o reducir el impacto de los riesgos después de su materialización.

De acuerdo con la forma como se ejecutan:

- **Control manual:** Controles que son ejecutados por personas.
- **Control automático:** Son ejecutados por un sistema.

Para los riesgos de seguridad de la información, se podrán emplear los controles tomados del Anexo A del estándar ISO/IEC 27001:2013 y los dominios a los que pertenecen, siempre y cuando se ajusten al análisis de riesgos.

- **Valoración de controles**

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización, también se presentan su descripción y pesos asociados.

Imagen 11. Valoración de los 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 DAFP, v.7.

Imagen 12. Atributos de formalización de los controles

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
Características de Eficiencia		**Descripción**
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

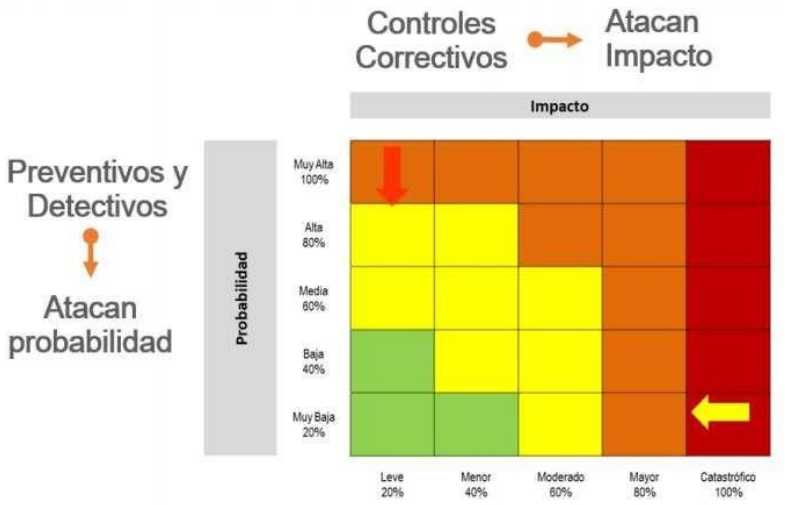
- **Aplicación de controles en la matriz de severidad**

Para cada control, dependiendo su tipo y su implementación se realiza una valoración, que resulta de sumar el peso del tipo por el peso de la implementación, con lo que, por ejemplo, si un control es preventivo y manual, se suma 25% más 15% con lo que su valoración da 40%.

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

A continuación, se presenta como se genera desplazamiento en la matriz de calor según el tipo de control.

Imagen 13. Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

PASO 4. Valoración del riesgo residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Los controles mitigan el riesgo de manera acumulativa, es decir, una vez se aplica el valor de uno de los controles, el siguiente valor se aplica con el valor resultante luego de la aplicación del primer control.

Imagen 14. Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Valoración de Probabilidad				
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2º control				36%
	Valoración control 2 detectivo			30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual				25,2%
	Valoración de Impacto				
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual				80%

Fuente: Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP, v.7.

Los controles preventivos y detectivos afectan la probabilidad, mientras que los correctivos el impacto. En caso de no contar con controles correctivos, el impacto residual es el mismo al inherente.

En el ejemplo de la gráfica, teniendo un control preventivo y asumiendo que la probabilidad inherente fue de 60% (media) y la valoración del primer control fue de 40%, se multiplica la probabilidad 60% por la valoración del control 40%, luego se le resta la probabilidad inherente de 60% a ese resultado de 24%, con lo que la valoración de probabilidad termina en 36%. Pero ese riesgo tiene adicionalmente un control detectivo con un peso de 30%, por lo que de esa valoración residual de 36% se le empieza a calcular la mejora con este segundo control, con lo que se obtiene un 36% por el 30% del control lo que da 10,8% y luego al 36% se le resta el 10.8% resultante, con lo que la valoración de la probabilidad queda en 25.2%, la cual es la probabilidad residual o final después de controles.

En el mismo ejemplo del gráfico, no se tienen controles correctivos, los cuales son aquellos que afectan el impacto, razón por la cual, el impacto inherente de 80% (mayor) no se modifica y el impacto residual resulta igual a 80%. En el caso que haya controles correctivos se sigue el mismo ejercicio del ejemplo para los controles preventivos y detectivos, es decir, se multiplicaría el valor del impacto por la valoración del control y luego a la valoración del impacto inicial se le restaría ese resultado, con lo que se genera el impacto residual, si se tuvieran más controles correctivos, se seguiría la misma lógica disminuyendo progresivamente la valoración de impacto.

- **Tratamiento del riesgo**

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser reducir, aceptar o evitar. Se analiza frente al riesgo residual.

Reducir: Implica tomar medidas encaminadas a disminuir la probabilidad (medidas de prevención) y el impacto (medidas de protección) o ambas.

Cuando el nivel de riesgo residual es moderado, alto o extremo se determina tratarlo mediante transferencia o mitigación de este. Transferir corresponde a la estrategia de tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas, la responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad reputacional. Mitigar corresponde a implementar acciones que mitiguen el nivel de riesgo, no necesariamente un control adicional.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: actividades, recursos, responsables y fecha de implementación.

Aceptar: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. Es una decisión informada de tomar un riesgo en particular. Los riesgos asumidos deben estar sujetos a monitoreo y revisión. Esta opción opera cuando la zona de riesgo residual es baja.

Evitar: No asumir la actividad que genera el riesgo o se elimina el activo fuente del riesgo para el caso de los riesgos de seguridad de la información.

El tratamiento a los riesgos para la integridad pública sólo tendrá dos (2) escenarios posibles que corresponden a reducir o evitar el riesgo.

- **Monitoreo y seguimiento**

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión 7 de MIPG de Control Interno, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual parte del Esquema de líneas de defensa.

Reportes periódicos

La formulación de los mapas de riesgos de gestión, fiscales y para la integridad pública es revisada por la Oficina Asesora de Planeación y Aseguramiento de Procesos OAPAP, mientras que, para el caso de riesgos de Seguridad de la información, se realiza la revisión por parte del Oficial de Seguridad de la Información de la Gerencia de Tecnología.

Los responsables de procesos de la Unidad deben monitorear permanentemente sus mapas de riesgos para determinar cambios en las diferentes etapas de la Gestión del riesgo.

El seguimiento y la revisión deben:
- Garantizar que los controles son eficaces tanto en el diseño como en la operación.
- Obtener información adicional para valorar el riesgo.
- Analizar y aprender lecciones.
- Verificar, atender e informar la materialización del riesgo.

El seguimiento y la revisión del riesgo y su materialización se efectuará trimestralmente, remitiendo la información a la Oficina Asesora de Planeación y Aseguramiento de Procesos (riesgos de gestión,

corrupción y para la integridad pública) y al Oficial de Seguridad de la Información – Gerencia de Tecnología (riesgos de seguridad de información).

Los responsables deberán generar el seguimiento trimestralmente los primeros diez días hábiles siguientes al corte del trimestre, acorde con lo establecido con el Procedimiento Gestión de riesgos.

Excepcionalmente y por necesidades del servicio, este plazo podrá ampliarse con la aprobación del Jefe de la Oficina Asesora de Planeación y Aseguramiento de Procesos y/o Gerente de Tecnología –Oficial de Seguridad de la Información según corresponda, sin exceder los plazos establecidos para publicación y envío de la información a la Oficina de Control Interno.

Los procesos tendrán un repositorio de información para conservar los soportes trimestrales que dan cuenta o son evidencia de la ejecución de las actividades del plan de manejo de riesgos.

La Oficina Asesora de Planeación y Aseguramiento de Procesos determinará la herramienta a través de la cual se realizará la formulación y seguimiento de los riesgos, la cual podrá ser entre otros, Excel o aplicativo web, de lo cual se detallará su manejo en el procedimiento y/o instructivo asociado.

Si bien no se desarrolla Plan de Manejo de Riesgo a aquellos riesgos situados en zona de riesgo residual baja, estos se monitorean con el seguimiento periódico.

- **Materialización de riesgos**

La materialización de un riesgo ocurre cuando se evidencia un efecto negativo sobre los objetivos de las entidades, debido a eventos potenciales. La identificación de una materialización debe realizarse por parte de la primera línea de defensa, en cuyo análisis podrá tener en cuenta la retroalimentación o asesoría de la segunda o tercera línea.

De manera específica para los riesgos de gestión, la entidad formula indicadores clave que permitan alertar sobre la exposición al riesgo. Estos indicadores cuentan con una descripción y meta, esta última, entendida como un umbral o tolerancia que permite identificar cuándo podría presentarse una materialización, lo cual (para la entidad) toma como base, el evento de riesgo, no el efecto de este. Es importante señalar que, partiendo del resultado de la medición del indicador, se debe realizar el análisis para estimar la materialización, es decir, dependiendo de si el incumplimiento del indicador representa una afectación inmediata o no. Por ejemplo, un indicador relacionado con la ejecución de un plan de trabajo puede presentar un retraso al corte trimestral de la medición, pero solo se constituye en un riesgo materializado si al finalizar la vigencia no se supera la tolerancia o umbral establecido. Cosa diferente sucede, citando otro ejemplo, con el incumplimiento de los términos de ley para dar respuesta a acciones de tutela, lo cual representa la materialización del riesgo establecido para ese caso y el inicio de la implementación de acciones de tratamiento inmediatas.

- **Ajustes a la matriz de riesgos**

Cuando el equipo responsable del proceso, producto del seguimiento y la revisión requiere ajustar, incluir o eliminar algún riesgo (gestión, fiscales, para la integridad pública), éste se realizará en Comité de calidad o por solicitud realizada por medio de correo electrónico al asesor de calidad del proceso, dejando

soporte de la justificación por la cual se realiza la inclusión, modificación o eliminación del riesgo.

Cuando luego de la revisión de un riesgo este pase a riesgo residual bajo y haya tenido plan de tratamiento este no requerirá continuar el plan establecido toda vez que la valoración de controles establece la solidez de estos, con lo que la opción de tratamiento es asumir.

El ajuste de los riesgos de seguridad de la información se realizará de manera conjunta entre el proceso y el Oficial de Seguridad de la información por correo electrónico o mediante actas o registros de reunión.

- **Ajustes producto de la materialización de un riesgo**

De presentarse materialización en los riesgos estos deberán ser revisados de forma integral teniendo en cuenta entre otros, los cambios en el contexto, la descripción del riesgo, causas, probabilidad e impacto, controles, plan de tratamiento). Los resultados de esta revisión deberán ser documentados por correo electrónico o acta. De no ser requerida una actualización o nueva versión del mapa esta deberá ser justificada en el análisis. Las acciones correctivas por realizar en caso de materialización del riesgo se deberán incorporar dentro del plan de tratamiento del riesgo o se documentarán a partir de una no conformidad.

Si luego de una materialización y con el análisis del riesgo este queda en zona de riesgo residual baja y por ende no requiere plan de tratamiento, en todo caso se deberá documentar la no conformidad para tratar la materialización.

Cuando el proceso en desarrollo de su rol de primera línea de defensa identifique una materialización, no requerirá esperar a que se realice el reporte trimestral para revisar y ajustar la matriz, sino que deberá hacerlo luego de identificada la materialización.

Por otra parte, como insumo para la actualización de los mapas de riesgos también se consideran las revisiones que con ocasión de hallazgos u observaciones internos y externos puedan identificar situaciones fuente de materializaciones de riesgo.

En el evento de materializarse un riesgo para la integridad pública, la entidad deberá asegurar la continuidad en la prestación del servicio y/o su operación normal, con independencia de las actuaciones que, por competencia, correspondan a las autoridades.

En cuanto a seguridad de la información, en el evento de presentarse un incidente de seguridad sobre un activo o grupo de activos de información se debe tener presente lo siguiente:

a) Si el activo o grupo de activos no se encuentren identificados en el inventario general de activos o instrumento de gestión de la información pública es necesaria la actualización de estos, su valoración y su correspondiente análisis de riesgos.
b) Si no existe ningún riesgo asociado con el incidente presentado es necesario incluir el riesgo actualizando la matriz de riesgos del proceso.

Asimismo, en cuanto a seguridad de la información, una vez finalizado el plan de tratamiento deberá ser revaluado el riesgo.

Por otra parte, el Oficial de Seguridad de Información verificará con periodicidad anual, si en los planes de tratamiento de los riesgos, se han incluido nuevos controles adicionales a los establecidos en la declaración de aplicabilidad -DdA de la Unidad, en cuyo caso deberá proceder a su ajuste.

- **Información, comunicación y reporte**

Corresponde a los jefes de oficina, gerentes, subgerentes, responsables de proceso (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.

La Oficina Asesora de Planeación y Aseguramiento de Procesos y el Oficial de Seguridad de la Información – Gerencia de Tecnología (en cuanto a riesgos de seguridad de la información) son los responsables de la difusión y asesoría de la presente metodología, para lo cual deberán adelantar procesos de socialización de esta, así como de realizar el seguimiento a los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.

Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas, los soportes de estos reposarán en la Oficina Asesora de Planeación y Aseguramiento de Procesos y en la Gerencia de Tecnología (riesgos de seguridad de la información).

En relación, a la gestión del riesgo de LA/FT/FP, toda operación sospechosa, incluso la intentada, debe ser objeto de reporte, al margen de la materialización del delito de Lavado de Activos. Dicho reporte deberá ser remitida ante el Equipo SARLAFT para su evaluación y por su parte la Oficina Asesora de Planeación y Aseguramiento de Procesos OAPAP, deberá realizar Reporte de Operación Sospechosa (ROS) ante la Unidad de Información y Análisis Financiero (UIAF).

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar en todas las etapas del proceso para la gestión del riesgo.

La Oficina de Control Interno, debe realizar la evaluación independiente sobre la Gestión del Riesgo en la Entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría, y por tanto debe dar a conocer el Plan Anual de Auditorías basado en riesgos, y los resultados de la evaluación de la Gestión del Riesgo.

Para la revisión por la dirección o para presentar al Comité Institucional de Gestión y Desempeño y/o Comité Institucional de Coordinación de Control Interno, se elabora un informe de riesgos, este es realizado según su competencia y de forma independiente por la Oficina Asesora de Planeación y Aseguramiento de Procesos, la Oficina de Control Interno y el Oficial de Seguridad de la Información (Gerencia de Tecnología).

ANEXO 1. Amenazas – Anexo C ISO27005:2008

Tipo	Amenazas	Origen
Daño físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción del equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o de aire acondicionado	A, D
	Pérdida de suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de la posición	D

Tipo	Amenazas	Origen
Fallas técnicas	Falla del equipo A	A
	Mal funcionamiento del equipo A	A
	Saturación del sistema de información A, D	A, D
	Mal funcionamiento del software A	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E
Datos personales	Modificación o alteración no autorizada de datos personales	D
	Pérdida o borrado de datos personales	A, D
	Acceso no autorizado a los datos personales	D
	Ausencia de procedimientos para el ejercicio de derechos	D
	Corrupción de datos	A, D
	Tratamiento de datos personales no autorizado	
	Recuperación de medios o documentos desechados o reciclados	D
	Robo de medios o documentos	D
	Pérdida, destrucción, acceso o uso no autorizado	
	Alteración de documentos	
	Ausencia de legitimidad para el tratamiento de los datos personales	D
	Tratamiento ilícito de datos personales	A, D

Fuente: Anexo C ISO27005:2008

ANEXO 2. Vulnerabilidades – Anexo D ISO27005:2008

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo	Destrucción de equipos o de medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de contraseñas	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables.	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de la documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario.	Error en el uso

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de la información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falso o copiado
Datos personales	Ausencia de procedimientos para que los titulares puedan ejercer sus derechos	Ausencia de procedimientos para el ejercicio de derechos
	Acceso intencionado por parte de personal no autorizado	Acceso no autorizado a los datos personales
	Perdidas de dispositivos móviles	Acceso no autorizado a los datos personales
	Uso ilegítimo de datos personales	Acceso no autorizado a los datos personales
	Errores en los procesos de recopilación y captura de información	Modificación o alteración no autorizada de datos personales
	Ausencia o indebida asignación de privilegios para el tratamiento de datos personales	Modificación o alteración no autorizada de datos personales
	Ataque para la suplantación de identidad	Modificación o alteración no autorizada de datos personales
	Contraseñas y datos sensibles no cifrados	Tratamiento de datos personales no

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
		autorizado
	Ausencia de control de acceso	Pérdida, destrucción, acceso o uso no autorizado
	Borrado de datos personales por error humano	Pérdida o borrado intencionado de datos personales
	Ataque intencionado que provoca borrado o pérdida de datos personales	Pérdida o borrado intencionado de datos personales

Fuente: Anexo D ISO27005:2008

C. DEBIDA DILIGENCIA

La Unidad Administrativa Especial de Catastro Distrital (UAECD), en el marco de su compromiso con la prevención del lavado de activos y la financiación del terrorismo (LA/FT), adopta como parte de su sistema de administración del riesgo (SAR), un lineamiento institucional de debida diligencia para el conocimiento de contrapartes. Este lineamiento establece criterios y directrices para aplicar medidas razonables y proporcionales que permitan identificar y comprender adecuadamente la contraparte (beneficiario final), la estructura de titularidad, la claridad sobre los objetivos del negocio, el seguimiento de transacciones realizadas y su consistencia, así como conservar y actualizar la información.

Así mismo, la debida diligencia es una herramienta de gestión de riesgos para la integridad pública ya que, al realizar una adecuada identificación de las contrapartes, contribuye no solo a la gestión de riesgos LA/FT, sino también a la gestión de riesgos de soborno y corrupción, y por tanto todos los riesgos identificados cuya causa inmediata sea la conducta de soborno o LA/FT deberá aplicar controles según la complejidad de la vulnerabilidad identificada.

Este lineamiento busca asegurar que la UAECD cuente con elementos suficientes para tomar decisiones informadas, evaluar la exposición al riesgo y prevenir su utilización indebida como vehículo para operaciones de LA/FT.

1. PRINCIPIOS ORIENTADORES

La debida diligencia adoptada por la UAECD se rige por tres principios esenciales:

- Razonabilidad: en la medida en que se aplican medidas acordes con la naturaleza y magnitud del vínculo con la contraparte.
- Prevención: al constituirse en una herramienta anticipativa que permite establecer controles desde la fase de vinculación.
- Proporcionalidad: ajustando el nivel de profundidad del conocimiento según el nivel de riesgo identificado. Teniendo en cuenta los resultados del análisis de severidad o riesgo inherente se establecen tres niveles de debida diligencia:

Tabla 5. Niveles de debida diligencia

Riesgo inherente	Vulnerabilidad	Complejidad de la debida diligencia
Bajo	Baja	Simplificada
Moderado	Media	Estándar
Alto y Extremo	Alta	Intensificada

Fuente: Elaboración propia basado en Documento Técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades de Distrito Capital de la Secretaría General, 2022

2. SEGMENTACIÓN DE CONTRAPARTES Y NIVELES DE DILIGENCIA

En función del análisis de riesgo institucional y las características de las relaciones contractuales, la UAECD segmenta a las contrapartes en niveles que orientan el alcance del conocimiento requerido, adoptando tres enfoques:

- Debida diligencia simplificada: Aplicable a personas naturales vinculadas mediante contratación directa de prestación de servicios y selección abreviada mínima cuantía.
- Debida diligencia estándar: Dirigida a personas jurídicas, asociaciones o entidades con quienes se establecen vínculos contractuales de selección abreviada y concurso de méritos.
- Debida diligencia intensificada: Aplicable a contrapartes clasificadas como de alto riesgo, como personas expuestas políticamente (PEP), procesos de licitación pública, selección abreviada subasta inversa, alianzas estratégicas o relaciones donde se identifiquen señales de alerta o antecedentes sensibles.

Esta segmentación permite que las medidas aplicadas se ajusten al perfil de riesgo, garantizando un equilibrio entre control efectivo y eficiencia institucional.

3. ALCANCE Y APLICACIÓN DEL LINEAMIENTO

El lineamiento de debida diligencia es de aplicación transversal en la UAECD, y debe ser observado en todos los procesos que involucren la vinculación de personal, contratación de contrapartes y pagaduría. Las áreas responsables de dichos procesos deberán asegurar que previo al perfeccionamiento de cualquier relación, se haya recopilado y analizado la información mínima requerida conforme al nivel de diligencia correspondiente.

El conocimiento de la contraparte debe considerar aspectos como su identidad, trayectoria, estabilidad financiera, antecedentes jurídicos, cumplimiento tributario y cualquier otro factor que permita evaluar su confiabilidad y transparencia.

En los casos donde el análisis determine un riesgo medio o alto, se podrán establecer controles adicionales, solicitar documentación complementaria o escalar la revisión al grupo de trabajo SARLAFT para su valoración técnica.

El resultado de la debida diligencia no deriva en inhabilidades o incompatibilidades para las personas

involucradas en la operación, sino que permitirá:

- La identificación de señales de alerta que deberán ser atendidas por cada proceso.
- La necesidad de implementar controles adicionales, especiales o revisar los controles existentes para ajustarlos a los resultados de la segmentación de contrapartes y niveles de diligencia.
- La necesidad de hacer ajustes en los equipos a cargo del relacionamiento con la contraparte, o que se requieran aprobaciones adicionales, para continuar con la relación.
- En circunstancias excepcionales, podrá evaluarse la necesidad de terminar con la relación o abstenerse de iniciarla.
- Un monitoreo especial a las operaciones que se realicen en el marco del relacionamiento para garantizar los reportes de operaciones inusuales o sospechosas.

4. REGISTRO, TRAZABILIDAD Y MEJORA CONTINUA

Toda la información recabada en el marco de la aplicación del lineamiento de debida diligencia debe ser registrada, organizada y conservada conforme a las políticas institucionales de archivo, confidencialidad y protección de datos personales. La trazabilidad de estos registros permitirá a la UAECD responder de manera oportuna a los requerimientos de autoridades competentes, auditores o entes de control.

El lineamiento será objeto de revisión y actualización periódica por parte del responsable SARLAFT, con el fin de incorporar nuevas tipologías, ajustes normativos y buenas prácticas derivadas del análisis de casos concretos, evaluaciones internas o recomendaciones de organismos especializados como la Alcaldía de Bogotá, entre otras fuentes de información.

5. CONFIDENCIALIDAD DE LA INFORMACIÓN

La Unidad Administrativa Especial de Catastro Distrital (UAECD) reconoce que la implementación y operación de la Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo implica el tratamiento de información sensible, tanto institucional como de terceros vinculados a procesos administrativos, contractuales o jurídicos. En consecuencia, establece como principio fundamental la confidencialidad de la información derivada del funcionamiento del sistema, garantizando su manejo seguro, reservado y limitado exclusivamente a los fines establecidos en el marco legal y normativo vigente.

Toda la información recolectada, analizada, producida o almacenada en el desarrollo del SARLAFT, incluyendo datos personales, antecedentes, reportes de operaciones inusuales o sospechosas, soportes documentales, bases de datos y reportes internos, será tratada bajo estrictas medidas de reserva y solo podrá ser conocida por el personal autorizado que, por razón de sus funciones, deba acceder a ella. Esta obligación comprende tanto a servidores públicos, contratistas, proveedores y demás personas que, de manera directa o indirecta, intervengan en los procesos relacionados con el SARLAFT.

El incumplimiento de las obligaciones de confidencialidad dará lugar a las responsabilidades disciplinarias, civiles, fiscales o penales a que haya lugar, de acuerdo con las normas que regulan el acceso y tratamiento de la información en el sector público colombiano, particularmente la Ley 1581 de 2012 sobre protección de datos personales y el Código Penal en lo relativo a delitos contra la administración pública y la reserva legal

de información.

Así mismo, la UAECD adopta medidas técnicas y administrativas para asegurar que los sistemas de información, documentos físicos y archivos electrónicos asociados al SARLAFT cuenten con mecanismos de seguridad que prevengan el acceso, divulgación, alteración o destrucción no autorizada. Este compromiso con la confidencialidad se articula con las políticas institucionales de seguridad de la información y el Programa de Transparencia y Ética Pública (PTEP).

3. DOCUMENTOS REFERENCIA

- Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. 2025. DAFP.
- Manual Operativo Sistema de Gestión MIPG, Modelo Integrado de Planeación y Gestión. Versión 6.1.2026
- Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno nacional, territoriales y sector público. Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Modelo de Gestión de Riesgos de Seguridad Digital. Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas. Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Documento Técnico Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades de Distrito Capital. Secretaría General, 2022.