

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## POLÍTICA DE ADMINISTRACIÓN DEL RIESGO



	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## Contenido

Política de Administración de Riesgos.....	4
<b>1. Objetivo.....</b>	<b>4</b>
<b>2. Alcance.....</b>	<b>5</b>
<b>3. Tipologías de Riesgos.....</b>	<b>5</b>
<b>4. Metodología.....</b>	<b>8</b>
<b>4.1. Apetito del Riesgo- Nivel de aceptación del riesgo.....</b>	<b>10</b>
<b>4.2. Criterios para calificar Probabilidad e Impacto: .....</b>	<b>12</b>
<b>4.3. Responsabilidad en la Planeación y Ejecución: .....</b>	<b>14</b>
<b>4.4. Responsabilidad en el Monitoreo .....</b>	<b>17</b>
<b>4.5. Accionar ante riesgos materializados.....</b>	<b>19</b>
<b>5. Herramientas para la Administración del Riesgo .....</b>	<b>21</b>
<b>6. Conceptos claves .....</b>	<b>22</b>
<b>7. Documentos Asociados.....</b>	<b>26</b>
<b>8. Referencias.....</b>	<b>27</b>
<b>Control de versiones:.....</b>	<b>28</b>

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## Contenido de Tablas

Tabla 1 Criterios para definir el nivel de PROBABILIDAD en Riesgos de Gestión, Corrupción y Seguridad de la Información .....	13
Tabla 2 Criterios para definir el nivel de IMPACTO en Riesgos de Gestión, Seguridad de la Información y Lavado de activos.....	13
Tabla 3 Criterios para definir el nivel de IMPACTO en Riesgos de Corrupción .....	13
Tabla 4 Niveles de Responsabilidad Líneas de Defensa (Planear y Hacer) .....	14
Tabla 5 Responsabilidades en Monitoreo. Verificar - Líneas de Defensa .....	17
Tabla 6 Acciones ante riesgos materializados.....	19

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## Política de Administración de Riesgos

El compromiso de la Alta Dirección frente al cumplimiento de las metas establecidas en el Plan Distrital de Desarrollo para la Fundación Gilberto Alzate Avendaño - FUGA, integra la identificación y valoración de los riesgos positivos o negativos que pudieran afectar el cumplimiento de la Misión, el Plan Estratégico Institucional y su articulación con el desempeño de los procesos, mediante:

- El establecimiento de acciones de control preventivas<sup>1</sup> y detectivas<sup>2</sup>, para los riesgos identificados.
- La oportuna gestión correctiva<sup>3</sup>, ante la materialización de los riesgos identificados.
- Monitoreo de indicadores de proceso.

La Entidad, toma como referente los lineamientos del Modelo Integrado de Planeación y Gestión, las Dimensiones “Direccionamiento Estratégico y Planeación” y “Sistema de Control Interno”, en lo relacionado con las líneas de defensa, y adopta la *“Guía para la administración de riesgo y diseño de controles en entidades públicas V5*, emitida por el Departamento Administrado de la Función Pública DAFP, así como los lineamientos específicos emitidos por la Alcaldía Mayor de Bogotá y órganos generadores de política.

### 1. Objetivo

Orientar a los servidores en la administración de riesgos, con el fin de minimizar su probabilidad e impacto en la gestión, mejorar la calidad de los procesos, fortalecer la cultura de “control” y proporcionar a la Dirección un aseguramiento razonable con respecto al logro de los objetivos institucionales.

1 **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. Estos controles actúan sobre las “causas” del riesgo y disminuyen la “probabilidad”

2 **Control defectivo:** control accionado durante la “Ejecución” del proceso. Estos controles detectan el riesgo, pero generan reprocesos., pueden “disminuir la materialización” de dicho riesgo y disminuir la “probabilidad”

3 **Control correctivo:** control accionado en la “Salida” del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. En la mayoría de las ocasiones permiten reducir el “Impacto” de dicho riesgo

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## 2. Alcance

La Política de administración de riesgos es aplicable a todos los procesos de la entidad, y niveles de la estructura institucional; es extensiva a todos los servidores y/o contratistas, cargos directivos con poder de decisión o que cumplan funciones de gestión de recursos o de servicios al interior de la FUGA, incluye todas las sedes y los bienes muebles e inmuebles de propiedad de la Fundación, que habiliten el desarrollo de las actividades y la prestación de los servicios. Aplica igualmente, para la identificación de Riesgos de Gestión (en procesos y objetivos estratégicos), Riesgos de corrupción (incluyen riesgos en Trámites y/o Opas y lavado de activos y lineamientos para identificar, detectar, prevenir, controlar, monitorear, investigar situaciones de soborno) más Riesgos de seguridad de la información.

Cabe señalar que, en el marco de los riesgos de corrupción, se emiten lineamientos y estrategias particulares para la “prevención” de riesgos de soborno y cohecho, estipulados en el Anexo 1 “*Política Antisoborno de la Fundación Gilberto Alzate Avendaño*” que hace parte integral de este documento.

Al respecto señalamos que si bien los conceptos de soborno y cohecho<sup>4</sup>, conceptualmente, refieren una diferencia jurídica, a lo largo de este documento y la *GM-PO-02 Política Antisoborno de la Fundación Gilberto Alzate Avendaño*.

se utilizarán los términos sobre la acepción común de “soborno” o “antisoborno”.

## 3. Tipologías de Riesgos

- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias y se identifican a partir de los “procesos” de la Entidad. Dentro de esta tipología, se analizan los “objetivos” institucionales, para identificar los “*Riesgos Estratégicos*” que puedan afectar su éxito o fracaso.

Los riesgos de Gestión, se clasifican en las siguientes categorías: Ejecución y administración de procesos; Fraude externo; Fraude interno; Fallas tecnológicas; Relaciones laborales; Usuarios, productos y prácticas; Daños a activos fijos.

- **Riesgos de corrupción.** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado (recursos o información). Estos

<sup>4</sup> La Veeduría Distrital aclara que si bien existe la diferencia jurídica entre cohecho y soborno (Newman & Ángel, 2017), se utilizará la acepción común de “soborno” o “antisoborno” a lo largo de este documento. Fuente: Guía de Lineamientos antisoborno para el D.C. noviembre 2018

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

riesgos se identifican sobre los “procesos” de la entidad, analizando los procedimientos y puntos críticos en donde exista un posible riesgo de corrupción por Conflicto de Intereses<sup>5</sup>, Lavado de Activos (LA/FT)<sup>6</sup> y/ soborno, identificados en el Direccionamiento Estratégico, actividades y/o procesos de Planeación, Gestión Financiera, Contratación, Información y Comunicación, actividades de Investigación y Sanción, Control Interno de Gestión, Talento Humano, procesos misionales, Trámites y/o Servicios y/o OPAs (reconocimientos de derecho - ganadores de estímulos, entre otros).

Los lineamientos particulares para la prevención de riesgos de soborno y cohecho se estipulan en la *GM-PO-02 Política Antisoborno de la Fundación Gilberto Alzate Avendaño*.

Los riesgos asociados a lavado de activos LA/FT, abordan cuatro clases: Riesgos de Contagio, Riesgo Operativo; Riesgo Reputacional; Riesgo Legal.

De otra parte, en la descripción de los riesgos de corrupción deben, concurrir los siguientes componentes:

*Acción u omisión + Uso del poder + Desviación de lo público + Beneficio privado (a nombre propio o de terceros)*

- **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.

Los Riesgos inherentes de seguridad de la información se clasifican en: Perdida de Confidencialidad, Pérdida de Integridad, Pérdida de Disponibilidad, sobre los cuales se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

<sup>5</sup> El conflicto de intereses no representa, en sí mismo, corrupción; sin embargo, estos sí se constituyen en riesgos de corrupción o disciplinarios. Transparencia por Colombia (2014) contempla la **materialización del conflicto de intereses**, al precisar que el interés privado “en efecto influye” en la toma de decisiones “...el conflicto de intereses surge cuando un servidor público tiene un interés privado que podría influir, o en efecto influye, en el desempeño imparcial y objetivo de sus funciones oficiales, porque le resulta particularmente conveniente a él, o a su familia, o a sus socios cercanos”. Cuando ocurre esa materialización ya nos encontramos ante una situación disciplinaria, un riesgo de corrupción. (Guía para la identificación y declaración de conflicto de intereses en el sector público colombiano DAFP V2 julio 2019)

<sup>6</sup> **Lavado de Activos (LA):** es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. (Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales Alcaldía Mayor V1 diciembre 2020)

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

En el contexto anterior, la Entidad ha identificado y priorizado activos críticos en las *Bases de Datos*, recopiladas en su gran mayoría en hojas de cálculo, referentes al tratamiento de datos personales de ciudadanos (activos de información bases de datos) y algunos activos críticos vinculados a la *Infraestructura Tecnológica* (activos de información hardware) consolidados en el formato GT-FT-10 activos de información versión 3, dado que el mal funcionamiento o un posible ataque cibernético, afectaría el acceso a la aplicación o a la información contenida, generando un impacto “alto” sobre los servicios que se derivan de dichos activos. Cabe señalar que los activos críticos son fuente de información clave, para la posterior identificación de riesgos.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

#### 4. Metodología

De acuerdo con la “Guía para la Administración del riesgo y el diseño de controles para entidades públicas DAFP V5”, y los lineamientos “particulares” emitidos por la Alcaldía Mayor de Bogotá y órganos generadores de política, para la identificación de Riesgos de Gestión, Corrupción y Seguridad de la información, se aplican los siguientes pasos:

**Paso inicial: Conocimiento y análisis de la Entidad:** Conocer el esquema de direccionamiento estratégico (misión, visión, objetivos estratégicos), la cadena de valor conocida como la interrelación de los procesos, procedimiento, políticas de operación, sistemas de información; le permitirá iniciar con la aplicación de la metodología para identificar riesgo con enfoque “preventivo” en la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a los usuarios de la Entidad.

**Paso 1. Política de Administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo sobre el tratamiento, manejo y seguimiento a los riesgos

**Paso 2. Identificación del Riesgo:** Inicia en el análisis de los objetivos estratégicos y de procesos, y finaliza en la clasificación del riesgo. Los **objetivos**, deben diseñarse con verbos “**fuertes**”, medibles, realistas, evitar frases subjetivas en su construcción, ¿y ser específicos indicando el Que?, **¿Cómo?**, **Para qué?**, **Cuándo y Cuánto?**

Lo anterior, **permitirá** identificar los riesgos que están o no bajo el control de la Entidad, conocer el contexto estratégico en el que opera, la caracterización de cada proceso, su objetivo y alcance, y realizar el análisis frente a los factores internos y externos que pueden **generar** riesgos que afecten el cumplimiento de dichos objetivos.

La identificación de Riesgos de *corrupción* asociados a **trámites y/o Otros Procedimientos Administrativos - OPAs<sup>8</sup>**, inicia, particularmente, con el conocimiento del portafolio completo de trámites y/o OPAs, la caracterización de los grupos de valor, la medición de la satisfacción de los usuarios, denuncias, el análisis particular de los objetivos de los procesos misionales y Procesos de Atención al Ciudadano, sus procedimientos y cada uno de los pasos que deben atender los usuarios para cumplir los requerimientos de un trámite y/o OPAs, entre otros.

En este contexto es necesario analizar dos momentos: a) En el momento de efectuar el trámite y/o OPA propiamente dicho, cuando interactúan el ciudadano y el servidor (es

<sup>7</sup> Características SMART para el análisis de objetivos: Específico, Medible, Alcanzable, Relevante, Temporal.

<sup>8</sup> Lineamientos para la identificación de riesgos de corrupción en Trámites, OPA y consultas de información distritales 2021. Alcaldía Mayor de Bogotá. V4 - 29-09-2022

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

decir de la ventanilla hacia afuera de la entidad); b) En el momento en que se ejecutan los procedimientos al interior de la entidad para dar cumplimiento al trámite y/o OPA (de la ventanilla hacia adentro). Las acciones de prevención y mitigación de los riesgos identificados, deben alinearse con el componente de Racionalización de trámites y/o OPAs en el Plan Anticorrupción y de Atención al Ciudadano PAAC, más los lineamientos particulares para la prevención de riesgos de soborno y cohecho que se estipulan la *GM-PO-02 Política Antisoborno de la Fundación Gilberto Alzate Avendaño*.

La identificación de riesgos de corrupción sobre **lavado de activos**<sup>9</sup> (LA/FT) inicia con la elaboración de un **inventario de los escenarios - eventos** que se presentan en el ámbito operativo, y que pueden determinar a grandes rasgos la “vulnerabilidad” de la entidad frente a la posibilidad de ser utilizada para dar apariencia de legalidad a los recursos de origen ilícito; para tal efecto, se emplean las herramientas particulares, facilitadas en la “ Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales Alcaldía Mayor V1 Dic.2020”. Las acciones para la prevención del lavado de activos, deben alinearse con el componente de Integridad en el Plan Anticorrupción y de Atención al Ciudadano PAAC.

La identificación de Riesgos *de Seguridad de la Información*, inicia con la identificación de **activos de información**<sup>10</sup>, continúa con la identificación, análisis, evaluación y tratamiento de los riesgos, y los articula el Modelo de Seguridad y Privacidad de la información (MSPI) en todas las etapas del PHVA, conforme a los lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Pública DAFP,

**Paso 3. Valoración del Riesgo:** Este paso, continua con el análisis del riesgo y finaliza en el monitoreo de los riesgos.

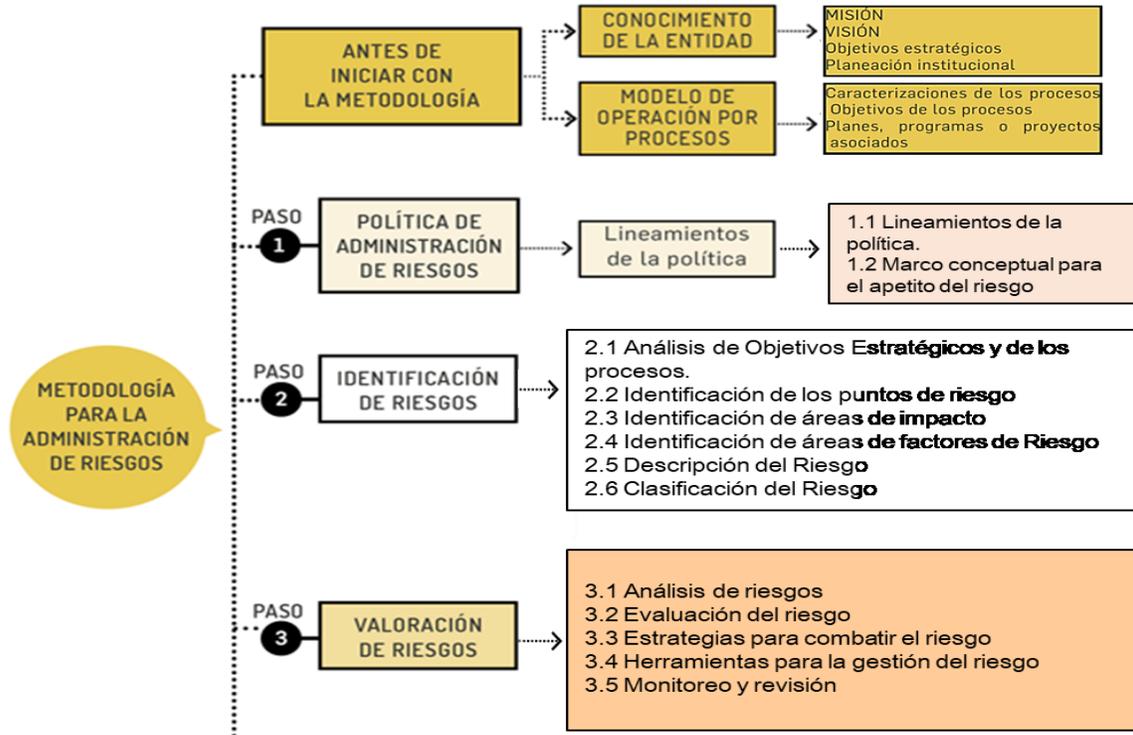
Lo anterior permite establecer la probabilidad de ocurrencia del riesgo, el nivel de consecuencia o impacto, estimar la zona de riesgo inicial (Riesgo Inherente) y definir las estrategias para combatir el riesgo

9 Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales Alcaldía Mayor V1 Dic.2020

10 Guía para la administración de riesgo y diseño de controles en entidades públicas DAFP V5 2020, - Anexo 4 “Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas DAFP v2 2019”

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

Ilustración 1 Metodología para la Administración del Riesgo



Fuente: 1 Guía Riesgos DAFF v5 2020

#### 4.1. Apetito del Riesgo- Nivel de aceptación del riesgo

La alta dirección en el marco del Comité Institucional de Coordinación de Control Interno CICCI, determina y revisa “anualmente” el **Apetito de riesgo** - Nivel de aceptación del Riesgo; al igual que la Tolerancia y **Capacidad** del riesgo, dejando constancia en las actas de reunión formalizadas, y documentando los resultados en las “fichas y matriz de riesgos”, aplicando los siguientes pasos:

**4.1.1. Capacidad de riesgo:** Se determina, identificando el *máximo* valor del nivel de riesgo que la Fundación puede soportar y a partir del cual se considera que no sería posible el logro de los objetivos de la entidad; por lo tanto, con la participación y aprobación de la alta dirección en el marco del Comité Institucional de Coordinación de Control Interno CICCI, se debe determinar lo siguiente:

- a. Valor máximo de la *escala* que resulta de combinar la *probabilidad* y el *impacto*.
- b. Valor máximo que, según el buen *criterio de la alta dirección* y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder

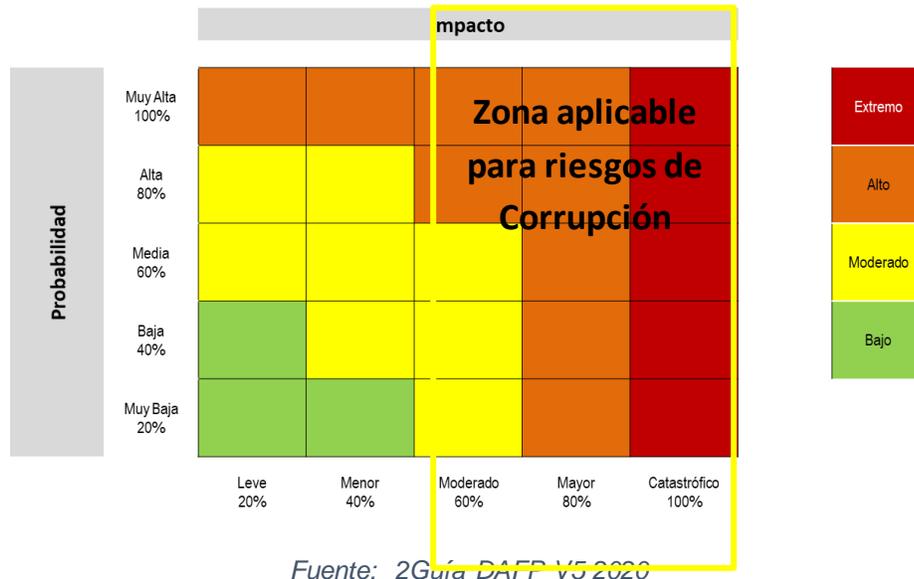
	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

**4.1.2. Apetito del Riesgo:** Luego de determinada la capacidad de riesgo por parte de la alta dirección y Comité CICCI, estas mismas instancias deben determinar el *valor máximo deseable del nivel de riesgo* que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión MIPG en la Fundación.

Niveles de Riesgo - (Niveles de severidad): Surgen de la combinación entre probabilidad e impacto, aplicables a los riesgos Inherentes y Residuales.

Ilustración 2: Matriz de calor con los niveles de riesgos o niveles de severidad



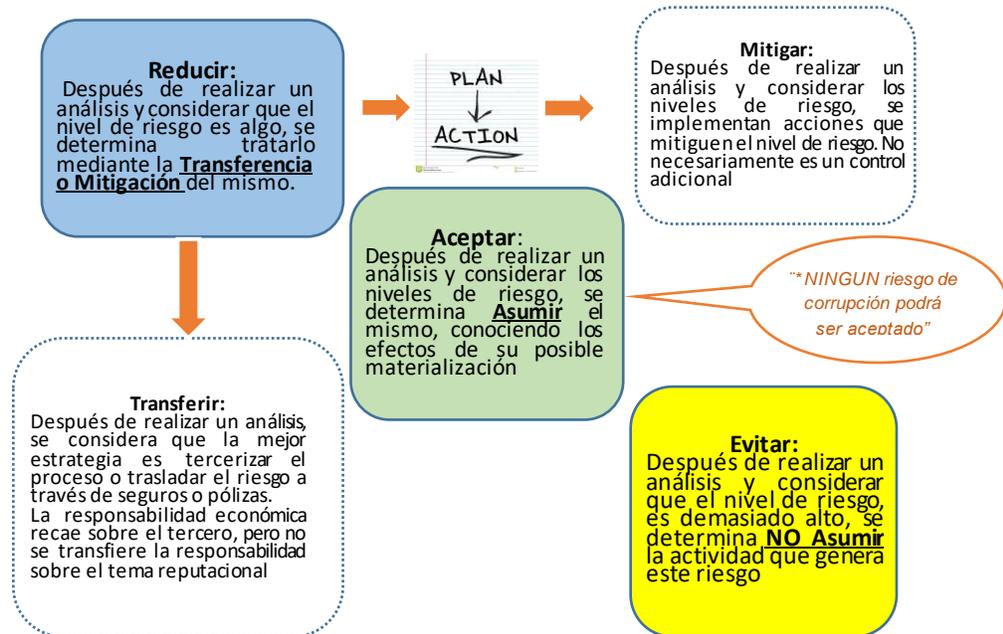
**4.1.3. Tolerancia de riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Luego de determinar el apetito del riesgo, por parte de la alta dirección y Comité CICCI; estas mismas instancias, definen un *valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo*; este valor, no puede ser superior al valor de la capacidad de riesgo.

Teniendo en cuenta que la determinación de la tolerancia de riesgo es optativa y su uso está limitado a definir el tipo de acciones para abordar los riesgos, la Entidad define acciones en función del valor del *nivel de riesgo “Residual”* obtenido (para procesos en funcionamiento), y del *nivel de riesgo “Inherente”* en procesos nuevos; y los compara con el apetito y tolerancia de riesgo.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

En este contexto, la Fundación asume decisiones para Aceptar<sup>11</sup>, Reducir o Evitar, y definir “planes de acción<sup>12</sup>” dentro del “Mapa de Riesgos Institucional”, como se ilustra a continuación:

Ilustración 3 Estrategias para combatir el riesgo



#### 4.2. Criterios para calificar Probabilidad e Impacto:

Se adoptan los criterios para calificar la **PROBABILIDAD** en los términos cualitativos y cuantitativos definidos a continuación:

<sup>11</sup> Ningún riesgo de corrupción podrá ser aceptado.

<sup>12</sup> **Plan de Acción:** Al adoptar la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

Tabla 1 Criterios para definir el nivel de **PROBABILIDAD** en Riesgos de Gestión, Corrupción y Seguridad de la Información

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

Pie de tabla 1P Estos criterios aplican “particularmente” para los Riesgos de Corrupción de Lavado de Activos.

Se adoptan los criterios para calificar el **IMPACTO** (Consecuencias) en los términos cualitativos y cuantitativos definidos en la guía de administración del riesgo DAFP

Tabla 2 Criterios para definir el nivel de **IMPACTO** en Riesgos de Gestión, Seguridad de la Información y Lavado de activos

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Pie de tabla 2 Estos criterios aplican para los Riesgos de Corrupción de Lavado de Activos

Tabla 3 Criterios para definir el nivel de **IMPACTO** en Riesgos de Corrupción

	Tabla 16 Criterios para calificar el impacto en riesgos de corrupción Guía DAFP
Moderado	1-5 preguntas afirmativas
Mayor	6-11 preguntas afirmativas
Catastrófico	12-19 preguntas afirmativas y adicionalmente, si la respuesta a la pregunta 16 (- ¿Ocasiona Lesiones físicas o pérdida de vidas humanas?) es afirmativa, el riesgo se considera Catastrófico

Pie de tabla 3 Estos criterios No aplican para Riesgos de Corrupción de Lavado de Activos

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

#### 4.3. Responsabilidad en la Planeación y Ejecución:

Las responsabilidades de las líneas de defensa se enmarcan en el ciclo de mejora continua PHVA (Planear, Hacer, Verificar y Actuar)

Tabla 4 Niveles de Responsabilidad Líneas de Defensa (Planear y Hacer)

<b>Línea Estratégica</b>		
Responsable	Comité Institucional de Gestión y Desempeño	Comité Institucional de Coordinación de Control Interno CICI
<b>Responsabilidades frente al riesgo</b>	<p><b>Este comité analiza la gestión del riesgo y define las mejoras. Da a conocer los cambios en el entorno que pueden afectar el logro de los objetivos institucionales</b></p> <ul style="list-style-type: none"> <li>Define el <b>Apetito de riesgo</b> - Nivel de aceptación del Riesgo; al igual que la <b>Tolerancia</b> y <b>Capacidad</b> del riesgo, una vez identificados los riesgos. Esta actividad se documenta en las "fichas y/o matriz de riesgos"</li> </ul>	<p><b>Este comité analiza eventos y riesgos críticos</b></p> <ul style="list-style-type: none"> <li>Define y aprueba la Política de administración del riesgo como marco general para la gestión del riesgo, teniendo en cuenta la metodología, alcance, los niveles de responsabilidad, niveles de aceptación (apetito del riesgo), niveles para calificar probabilidad e impacto, la periodicidad y responsables del seguimiento en la entidad.</li> </ul>



	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

- 13 *Gestión de Tecnología* identifica y prioriza los Activos críticos identificados, formalizarlos y priorizados, en el marco del Modelo de Seguridad y Privacidad de la Información y gestiona la vinculación en

Línea de Defensa	1ª Línea	2ª Línea	3ª Línea
<b>Responsable</b>	<b>Gerentes públicos y Líderes de Procesos</b>	<b>Colaboradores</b>	<b>Oficina Asesora de Planeación OAP</b>
<b>Responsabilidad frente al riesgo</b>	<p><b>Gestionar los riesgos en el día a día y hace seguimiento en 1ª línea:</b></p> <ul style="list-style-type: none"> <li>Desarrolla e implementa políticas, procesos y procedimientos internos, asegurando que sean compatibles con los objetivos estratégicos y metas de la entidad.</li> <li>A partir de los procesos que lidera, identifica los riesgos, los analiza, valora y monitorea.</li> <li>Al identificar los riesgos, elabora planes de contingencia "Control Correctivo" frente a su materialización. Lo anterior le permitirá al proceso responder, recuperar, reanudar y restaurar el normal funcionamiento de sus actividades.</li> <li>En el marco de los riesgos de seguridad digital, el área identifica y valorar los activos de información de los procesos a cargo, y con el</li> </ul>	<p><b>OAP - Definir metodología, capacitar, acompañar, generar recomendaciones, y monitorear en 2ª línea:</b></p> <ul style="list-style-type: none"> <li>Orienta metodológicamente al equipo directivo en la construcción de la Política de Administración del Riesgo de la entidad.</li> <li>Diseña y socializa instrumentos, para asegurar la correcta implementación de la política de riesgos en la entidad y las diferentes tipologías de riesgos</li> <li>Orienta metodológicamente a los líderes de proceso y a sus equipos, en: <ul style="list-style-type: none"> <li>i. El adecuado desdoblamiento de los objetivos institucionales (estratégicos) y en la alineación con los objetivos de proceso, para garantizar una adecuada identificación del riesgo;</li> <li>ii. <i>Planeación y Gestión de Tecnología</i><sup>*13</sup> apoyan metodológicamente a las áreas en la estandarización de actividades para la identificación y valoración de activos de información, vitales en la identificación de riesgos de seguridad de la información.</li> <li>iii. Articula acciones de alistamiento con el PAAC, para determinar el grado de vulnerabilidad de la entidad ante riesgos de corrupción en procesos, tramites y/o OPAs y prevención de Lavado de Activos (LA/FT)</li> <li>iv. La identificación y valoración de riesgos en las diferentes tipologías</li> </ul> </li> <li>Consolida el Mapa de Riesgos Institucional y realiza monitoreo periódico verificando que los controles estén diseñados apropiadamente que sean implementados por la 1ª línea.</li> </ul>	<p><b>Proporcionar información razonable sobre la efectividad del Sistema de Control Interno SCI, con el más alto nivel de independencia y objetividad, y enfoque basado en riesgos.</b></p> <ul style="list-style-type: none"> <li>Dar a conocer el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo mediante el Comité Institucional de Coordinación de Control Interno.</li> <li>Asesorar a la línea estratégica, 1a y 2a línea de defensa en la metodología para la administración de riesgos.</li> </ul>

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

*responsable de Seguridad de la Información* prioriza el alcance de los activos más críticos

- Elabora un inventario de los escenarios – eventos, que se presentan en el ámbito operativo, y que pueden determinar riesgos de Lavado de Activos (LA)

---

la Política de riesgos, clave para la identificación de riesgos de seguridad de la información.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

#### 4.4. Responsabilidad en el Monitoreo

Tabla 5 Responsabilidades en Monitoreo. **Verificar** - Líneas de Defensa

Líneas	Insumos	Monitoreo y seguimiento	Resultados
<p><b>Línea Estratégica</b></p> <p><b>Primera Línea de Defensa</b></p>	<ul style="list-style-type: none"> <li>Planeación estratégica</li> <li>Cambios en el contexto</li> <li>Informes de seguimiento realizados por la Oficina Asesora de Planeación con recomendaciones.</li> <li>Informes de resultado de auditorías internas de la OCI y externas de Entes de Control.</li> </ul> <ul style="list-style-type: none"> <li>Política de administración de riesgos</li> <li>Herramientas de administración de riesgos (Fichas y Mapa de riesgos)</li> <li>Informes de seguimiento y de auditorías</li> </ul>	<p><b>Comité Institucional de Gestión y Desempeño – Comité Institucional de Coordinación de Control Interno:</b> analiza la gestión del riesgo y define las mejoras.</p> <p><b>SEMESTRALMENTE</b> realiza reuniones para:</p> <ul style="list-style-type: none"> <li>- Analizar el Informe de monitoreo realizado por la Oficina Asesora de Planeación, y recomendaciones sobre el mapa de calor, el reporte de riesgos materializados con las causas.</li> <li>- Analizar los Informes de Auditoría y/o seguimientos presentados por la Oficina de Control Interno y Entes de Control.</li> </ul> <p><b>Gerentes públicos, Líderes de Procesos y Colaboradores:</b> <b>revisan y</b> autocontrolan los riesgos.</p> <p><b>PERIODICAMENTE</b> y por lineamientos de la alta dirección revisan y actualizan los riesgos <b>TRIMESTRALMENTE</b> realizan seguimiento por autoevaluación a TODOS los tipos de riesgos, en los siguientes términos:</p> <ol style="list-style-type: none"> <li>Si los riesgos están correctamente identificados.</li> <li>Si las actividades de control se encuentran documentadas y actualizadas en los procedimientos y si se implementaron los controles;</li> <li>Si se ejecutaron las tareas del plan de tratamiento de riesgos.</li> <li>Si se están cumpliendo los objetivos de los procesos a cargo, de acuerdo a los indicadores formulados,</li> <li>Identificar posibles riesgos que se están materializando y documentar las Acciones Correctivas correspondientes</li> </ol>	<ul style="list-style-type: none"> <li>Toma Decisiones basadas en recomendaciones de: <ul style="list-style-type: none"> <li>- Oficina Asesora de Planeación, relativas al apetito del riesgo (niveles de aceptación) y opciones de tratamiento</li> <li>- Oficina de Control Interno Entes de control</li> </ul> </li> <li>Mapa de Riesgos, con el reporte del seguimiento y evidencias consolidadas, reportadas a la Oficina Asesora de Planeación</li> <li>Fichas de riesgos, con riesgos y Planes de tratamiento ajustados según pertinencia.</li> <li>Acciones Correctivas y/o de mejora, elaboradas.</li> </ul>

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

Líneas	Insumos	Monitoreo y seguimiento	Resultados
<b>Segunda Línea de Defensa</b>	<ul style="list-style-type: none"> <li>Política de administración de riesgos</li> <li>Normatividad internacional/ Nacional</li> <li>Mapa de Riesgos con el reporte del seguimiento y evidencias de la 1ª. línea de defensa</li> </ul>	<p><b>Oficina Asesora de Planeación:</b> monitorear el cumplimiento de las etapas de la gestión de riesgos:  <b>ANUALMENTE</b> revisa la política, metodología, normativa y demás herramientas de apoyo para la gestión de riesgos.  <b>SEMESTRALMENTE</b> monitorea los riesgos institucionales:</p> <ul style="list-style-type: none"> <li>Realiza seguimiento sobre el estado de la Implementación de la metodología, controles, planes de tratamiento, materialización de riesgos y generar recomendaciones, verificando que los riesgos sean monitoreados por la 1ª. línea de defensa.</li> <li>Revisa los cambios en el direccionamiento estratégico o en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad.</li> <li>Revisa la adecuada definición y desdoblamiento de los objetivos institucionales (estratégicos y estructurales) a los objetivos de los procesos en la definición de riesgos y realiza recomendaciones.</li> <li>Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de gestión, corrupción y de seguridad de la información. * <i>El informe de Implementación de riesgos de seguridad de la información, se coordinará entre el proceso de Gestión de Mejora y Proceso Gestión de Tecnologías.</i></li> </ul> <p><b>Nota 1:</b> La Efectividad de los controles, se determina mediante su Eficiencia<sup>14</sup> y Eficacia<sup>15</sup>.  <b>Nota 2:</b> Consultar los contenidos mínimos de los “Informes de segunda línea en el Anexo “Orientaciones Monitoreo de Riesgos de Segunda Línea” disponible en la intranet.</p>	<ul style="list-style-type: none"> <li>Política de administración de riesgos actualizada</li> <li>Formato de Herramientas de administración de riesgos ajustadas (Fichas de riesgos)</li> <li>Mapa de Riesgos por proceso consolidado con monitoreo de 2ª línea de todos los tipos de riesgos</li> <li>Informe de monitoreo realizado por la Oficina Asesora de Planeación, y con recomendaciones, reportado a la 1ª. línea de defensa, Oficina de Control -interno y al CICC</li> </ul>
		<b>Tercera Línea de Defensa</b>	

14 Eficiencia: se define a través de los atributos y el diseño de los controles

15 . Eficacia: se define a través de los eventos “riesgos materializados”

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

#### 4.5. Accionar ante riesgos materializados

Cuando el riesgo se materializa, se deben corregir los efectos inmediatos de la materialización (correcciones) implementando planes de contingencia; posteriormente formula acciones correctivas para evitar su recurrencia; de otra parte, la segunda línea “gestiona los eventos<sup>16</sup>” integrando al mapa de riesgos los riesgos materializados y controla la trazabilidad.

Tabla 6 Acciones ante riesgos materializados

Zona de Riesgo “Residual”	TIPO DE RIESGO	
	RIESGOS DE GESTION y RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	RIESGOS DE CORRUPCION
Baja	1 quien detecte la materialización de un riesgo de gestión, informará al líder del proceso respectivo.	1. Toda persona, servidor o colaborador que tenga conocimiento o sospecha de la comisión del delito de soborno y/o conducta asociada con corrupción y/o que detecte la materialización de un riesgo de corrupción y/o posible acto de corrupción, así como la existencia de inhabilidades, incompatibilidades o conflicto de intereses, podrá informarlos mediante los canales dispuestos para la recepción de denuncias : Línea 195, Oficina de Atención al Ciudadano, Oficina de Correspondencia, Página web institucional ( <a href="https://www.fuga.gov.co/atencion-servicios-ciudadania/punto-de-atencion-y-defensor-del-ciudadano">https://www.fuga.gov.co/atencion-servicios-ciudadania/punto-de-atencion-y-defensor-del-ciudadano</a> ) o Intranet ( <a href="https://intranet.fuga.gov.co/quejas-y-conflictos-de-intereses">https://intranet.fuga.gov.co/quejas-y-conflictos-de-intereses</a> ) , los cuales serán canalizados por el Proceso de Servicio al Ciudadano, y radicados en el Sistema Distrital para la Gestión de Peticiones Ciudadanas – “Bogotá te escucha”
Moderada	2. El líder de proceso y su equipo establecen las <b>acciones correctivas</b> de acuerdo a los tiempos definidos en el GM- PD- 01 <u>Procedimiento de Plan de Mejoramiento</u> ; posteriormente, verifica la <b>calificación y ubicación del riesgo</b> para su actualización en el mapa de riesgos, con la asesoría metodológica de la Oficina Asesora de Planeación.	
Alta y Extrema	3. El líder de proceso informar a la Oficina Asesora de Planeación (segunda línea) sobre el hallazgo y las acciones tomadas.  4. La Oficina Asesora de Planeación, informa al Comité Institucional de Coordinación de Control Interno CICCI sobre la materialización del riesgo e integra al mapa de riesgos, la gestión de los eventos asociados.  5 la Oficina de Control Interno, verifica que se tomaron las acciones correctivas y evalúa su ejecución.  <b>Nota 1:</b> Cuando la Oficina de Control Interno,	2. Una vez radicados en “Bogotá te escucha” se clasifican por la tipología “Denuncia por acto de corrupción “y se direcciona automáticamente al Proceso de Control Interno Disciplinario quien garantizará la gestión eficiente de las denuncias por actos de corrupción que ingresan a la FUGA y generara los informes correspondientes a la Dirección Distrital de Asuntos Disciplinarios de la Secretaría Jurídica Distrital y demás entidades

<sup>16</sup> Gestionar Eventos: Controlar registro de riesgos materializados y datos históricos que permiten revisar si el riesgo fue identificado y qué sucedió con los controles.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

detecte en el marco de Auditorías, la materialización del riesgo, lo informará al Comité Institucional de Coordinación de Control Interno CICCI.

**Nota 2:** Ante la materialización de Riesgos de Seguridad en la Información, el Proceso de Gestión de Tecnologías y Gestión de Mejora, orientan a las áreas en la aplican los pasos anteriores, y en paralelo se aplican los lineamientos del “Procedimiento de Gestión de Incidentes, amenazas y debilidades de seguridad GT-PD-09”, y formato GT-FT-04, quien proyecta un “Informe de incidentes de seguridad de la información” a terceros (entes de control, reguladores, superintendencias, instancias o autoridades en la materia, entre otros), conforme lo estipulan los entes y las buenas prácticas en seguridad de la información<sup>17</sup>

relacionadas. Lo anterior, conforme a los lineamientos de la GS-GU-06 Guía Gestión de Conflictos Intereses y GS-CA-01 Proceso Gestión de Talento Humano – Control Interno Disciplinario

3. Surtido el conducto regular y los procesos disciplinarios particulares; el Proceso de Control Disciplinario, generará las alertas e informará al Comité Institucional de Coordinación de Control Interno CICCI, sobre los hechos encontrados.
4. El Comité Institucional de Coordinación de Control Interno – Comité de Dirección, emitirá lineamientos para la adopción de las Acciones Correctivas correspondientes, de acuerdo a los tiempos definidos en el GM- PD- 01 Procedimiento de Plan de Mejoramiento; así como la revisión y/o actualización de los riesgos de corrupción identificados. Lo anterior, con la asesoría metodológica de la Oficina Asesora de Planeación.
5. La Oficina Asesora de Planeación, integra al mapa de riesgos la gestión de los eventos sobre riesgos materializados identificados por las líneas de defensa, servidores o ciudadanos.
6. Control Interno, verifica que se tomaron las acciones correctivas y evalúa su ejecución.

**Nota 1:** En todos los canales de atención al ciudadano, y los procesos disciplinarios particulares, deberá garantizarse la protección de identidad del denunciante y la reserva de la información suministrada.

**Nota 2:** Cuando la oficina de Control Interno, detecte la materialización de riesgos, en el marco de Auditorías, informará lo correspondiente al Comité Institucional de Coordinación de Control Interno CICCI y a la Autoridad competente.

<sup>17</sup> Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en Entidades Públicas V2 de agosto de 2019

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## 5. Herramientas para la Administración del Riesgo

- **“Fichas de Riesgos”** con el despliegue de la metodología, para identificar los tipos de riesgo de Gestión, Corrupción y Seguridad de la Información, empleadas por la primera línea de defensa para el registro de los riesgos, en las fases (identificación, valoración y plan de tratamiento).

Al respecto se diseñarán dichas de riesgos con las metodologías particulares aplicables para la identificación de riesgos de gestión; corrupción; corrupción en trámites y/o OPAS; corrupción por lavado de activos; y Riesgos Seguridad de la Información. Instrumentos ubicados en Intranet Institucional (<http://www.intranet.fuga.gov.co/mapa-de-riesgos-por-procesos> ).

- **“Mapa de riesgos institucional”**: Instrumento que consolida los riesgos de Gestión, Corrupción y Seguridad de la Información, con el monitoreo de primera, segunda y tercera línea de defensa; contiene la **Gestión de Eventos**<sup>18</sup>; es decir el registro de riesgos materializados y datos históricos que permiten revisar si el riesgo fue identificado y qué sucedió con los controles.

Si el riesgo materializado no está identificado, se agrega a la matriz de riesgos y desplegar metodología completa. Instrumento ubicado en la intranet institucional (<http://www.intranet.fuga.gov.co/mapa-de-riesgos-por-procesos> )

- **“Indicadores clave de riesgo - proceso”**: hace referencia a la Matriz de Indicadores, ubicada en la intranet institucional (<http://www.intranet.fuga.gov.co/indicadores-sig>) con la colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos y sugiere que algo no funciona adecuadamente; por lo tanto, se debe investigar y evaluar a través de su tendencia, la eficacia de los controles aplicados para controlar el indicador y mitigar los riesgos..

<sup>18</sup> Un “Evento” es un riesgo materializado. Fuentes como: Mesas de Ayuda, PQRS; Líneas de denuncia; Oficina Jurídica, etc., prov en referentes históricos sobre algo que no funciona adecuadamente y, por lo tanto, se debe investigar.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## 6. Conceptos claves

- **Acción Correctiva:** Acción o conjunto de acciones tomadas para eliminar la(s) causa(s) de una No Conformidad detectada y evitar que vuelva(n) a ocurrir.
- **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.
- **Activos de Información:** Es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.
- **Administración del riesgo y/o Gestión del Riesgo:** Capacidad que tiene la organización para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia. Actividades encaminadas a la identificación, valoración, evaluación manejo y monitoreo.
- **ALA/CFT:** Antilavado de Lavado de activos y Contra la Financiación del Terrorismo.
- **Apetito de riesgo:** es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Área de Impacto:** es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal)
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual la Alta Dirección considera que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo
- **Causa Inmediata:** Circunstancias o situaciones más evidentes bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo. son la base para la definición de controles en la etapa de valoración del riesgo. Tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas. Los controles entran a atacar las sub causas.
- **Cohecho Propio.** El servidor público que reciba para sí o para otro, dinero u otra utilidad, o acepte promesa remuneratoria, directa o indirectamente, para retardar u omitir un acto propio de su cargo, o para ejecutar uno contrario a sus deberes oficiales. Artículo 405 Código Penal.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

- **Cohecho impropio:** El servidor público que acepte para sí o para otro, dinero u otra utilidad o promesa remuneratoria, directa o indirecta, por acto que deba ejecutar en el desempeño de sus funciones Artículo 406 Código Penal.
- **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.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
- **Control:** Medida que permite reducir o mitigar un riesgo. Los responsables de implementar y monitorear los controles son los dueños de proceso. Se establecen tres tipologías: Preventivos; Defectivos y Correctivos
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Estrategias para combatir el riesgo:** Decisión que se toma frente a un determinado nivel de riesgo (residual) dicha decisión puede ser Aceptar, Reducir, Evitar o Transferir
- **Estrategia para Aceptar:** Después de realizar el análisis y considerar los niveles de riesgos, se determina asumir el riesgo; sin adoptar medidas y se asume el riesgo, conociendo los efectos de su posible materialización. (Ningún riesgo de corrupción podrá ser aceptado).
- **Estrategia para reducir:** Para niveles de riesgo ALTO, se adoptan medidas para “transferir” (tercerizar el proceso o trasladarlo a seguros o pólizas) o “mitigar” el riesgo. No necesariamente es un control adicional. Para mitigar el riesgo, se requerirá la definición de un plan de acción (diferente a un plan de contingencia) que especifique responsable, fecha de implementación, y fecha de seguimiento.
- **Estrategia para Evitar:** Aplica a niveles de riesgo EXTREMO. Se determina NO asumir la actividad que genera este riesgo
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos. Ejemplo: Factor Procesos<sup>19</sup>, Talento Humano<sup>20</sup>, Tecnología, Infraestructura, Evento externo
- **Fichas de Riesgos:** Herramienta donde se registran los riesgos identificados estratégicos, de gestión, de corrupción y de seguridad de la información
- **Impacto:** Consecuencias que pueden ocasionar a la organización la materialización del riesgo, determinadas por niveles (leve, menor moderado, mayor, catastrófico)
- **Integridad: Propiedad de exactitud y completitud.**
- **Lavado de Activos (LA):** es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero sucio parezca limpio, haciendo que las

<sup>19</sup> Factor Procesos: Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización

<sup>20</sup> Factor Humano: Incluye Seguridad y Salud en el Trabajo, Se analiza posible dolo o intención frente a la corrupción

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

organizaciones criminales o delincuentes puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.

- **Líneas de Defensa (1ra., 2da. y 3ra.):** corresponde a la estructura de control interno de la gestión de la entidad, son las diferentes instancias de la entidad responsables de las acciones, métodos, procedimientos de control y de gestión del riesgo, para la prevención, verificación y evaluación de éste, con el fin de entregar a los ciudadanos lo mejor de la gestión de la entidad y, en consecuencia, producir cambios en las condiciones de vida, mayor valor público en términos de bienestar y prosperidad general y fortalecer la lucha contra la corrupción.
- **Línea Estratégica:** es quien define el marco general para la gestión del riesgo y el control en la entidad (Política de Administración del Riesgo). A cargo de la Alta Dirección y Comité Institucional de Coordinación de Control Interno.
- **Mapa de Calor de Riesgos:** Matriz de criticidad del riesgo; priorización de la probabilidad de ocurrencia del riesgo vs. la calificación de impacto; su intersección corresponderá al nivel de criticidad del riesgo.
- **Mapa de Riesgos Institucional:** Documento en Excel consolidado por la Oficina Asesora de Planeación con la información resultante de la identificación de los riesgos de la entidad su monitoreo y gestión de eventos.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Otro procedimiento administrativo - OPA.** Conjunto de requisitos, pasos o acciones dentro de un proceso misional, que determina una entidad u organismo de la administración pública o particular que ejerce funciones administrativas para permitir el acceso de los ciudadanos, usuarios o grupos de interés a los beneficios derivados de programas o estrategias cuya creación, adopción e implementación es potestativa de la entidad.
- **Plan de Contingencia:** Se enmarca dentro del Plan de Continuidad de Negocio<sup>2</sup> y se consideraría un control correctivo. De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio
- **Primera línea de defensa:** Se encarga de la gestión operacional de la entidad, identifica, evalúa, controla y mitiga los riesgos, así como del mantenimiento efectivo de controles internos, ejecuta procedimientos de riesgo y el control sobre una base del día a día. A cargo de los líderes de procesos de la entidad y sus equipos.
- **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.
- **Proceso:** Es un conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. (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).
- **Responsable operativo:** Todos los servidores de la entidad, que hacen parte de las diferentes dependencias que gestionan y ejecutan las actividades de los procesos.
- **Riesgo inherente:** Nivel de riesgo propio de la actividad. Es el resultado de **combinar la probabilidad con el impacto**, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** Es el resultado de **aplicar la efectividad de los controles** al riesgo inherente.
- **Riesgos de Contagio:** Esta es una clase de riesgos de lavado de activos (LA), y se define como la posibilidad de pérdida o daño que puede sufrir una entidad directa o indirectamente, por acción de una persona natural o jurídica que posee vínculos con la entidad”.
- **Riesgo Legal:** Esta es una clase de riesgos de lavado de activos (LA), y se define como la posibilidad de pérdida o daño que puede sufrir una entidad al ser sancionada, multada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones, obligaciones contractuales, fallas en los contratos y transacciones, derivados de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos transaccionales”.
- **Riesgo Operativo:** Esta es una clase de riesgos de lavado de activos (LA), y se define como la probabilidad de pérdida o daño que puede sufrir una entidad al incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología la infraestructura, por fraude o corrupción o por la ocurrencia de acontecimientos externos, entre otros”
- **Riesgo Reputacional:** Esta es una clase de riesgos de lavado de activos (LA), y se define como la probabilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, verdadera o no, respecto de la institución y sus prácticas de negocios, que cause una disminución de su base de clientes, disminución de los negocios o ingresos, o incurrir en procesos judiciales.
- **Segunda línea de defensa:** Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente. A cargo de la Oficina Asesora de Planeación.
- **Sistema de Control Interno – SCI:** Sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

- **Soborno:** Cuando una persona entrega o promete dinero u otra utilidad a un testigo para que falte a la verdad o la calle total o parcialmente en su testimonio (Artículo 444 del Código Penal, modificado por el artículo 31 de la Ley 1474 de 2011).
- **Tercera línea de defensa:** Proporciona Información a la línea estratégica (Comité Institucional de Coordinación de Control Interno), sobre la efectividad del Sistema de Control Interno de la entidad, la operación de la 1ª y 2ª línea de defensa con un enfoque basado en riesgos. A cargo de la Oficina de Control Interno.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **Trámites.** Son los mecanismos a través de los cuales los ciudadanos, usuarios y grupos de valor acceden a sus derechos y cumplen con sus y se caracterizan porque:
  - A través de ellos se accede a un derecho o se cumple un deber u obligación
  - Están creados o autorizados por la ley o por un decreto.
  - La tarifa del trámite debe contar con soporte legal.
  - Están relacionados con procesos y funciones misionales.
  - Son solicitados por la ciudadanía o grupos de interés a entidades del Estado, particulares que ejercen funciones públicas o prestan servicios públicos.
  - Se obtiene la entrega efectiva de un producto.
  - Son exigibles y vinculantes para la ciudadanía o grupos de interés y para la entidad. Para que el trámite sea exigible (oponible al ciudadano) debe estar publicado en el SUIT.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## 7. Documentos Asociados

- GM-FT-09 Ficha de Riesgos: de Gestión; Corrupción - trámites y/o Opas; Lavado de Activos y Financiación del Terrorismo (LA/FT); Riesgos de Seguridad de la Información
- GM-FT-10 Matriz consolidada de Riesgos
- GM-FT-03 Matriz y Fichas Técnicas de Indicadores
- PPT - Orientaciones Monitoreo de Segunda Línea
- GM-PO-01 Política Antisoborno

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

## 8. Referencias

Alcaldía Mayor de Bogotá. Directiva 015 de 2015 “Directrices para la atención y gestión de denuncias por posibles actos de corrupción, y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses y protección de identidad del denunciante” octubre de 2015. Disponible en: (<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=63146>)

Veeduría Distrital. Guía de Lineamientos Antisoborno del D.C. noviembre de 2018. Disponible en; ([https://old.integracionsocial.gov.co/anexos/documentos/2019paac/12022019\\_b2\\_Guia%20de%20lineamientos%20antisoborno%20para%20el%20Distrito%20VF%20\(29%20dic%2018\).pdf](https://old.integracionsocial.gov.co/anexos/documentos/2019paac/12022019_b2_Guia%20de%20lineamientos%20antisoborno%20para%20el%20Distrito%20VF%20(29%20dic%2018).pdf) )

Modelo Nacional de Gestión del Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4 – DAFP) V2 de agosto de 2019. Disponible en: ([https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document\\_library/bGsp2IjUBdeu/view\\_file/34316499](https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499))

Ministerio de Tecnologías de la Información y las Comunicaciones- MINTIC. Registro de Activos de Información. [Registro de activos de información | Vigencia 2020](#) / [Resolución 318 de 2019 - Instrumentos de gestión de la información](#) / [Registro de activos de información | Vigencia 2019](#) / [Registro de activos de información](#) / Disponibles en: (<https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135888:Registro-de-Activos-de-Informacion> )

Departamento Administrativo de la Función Pública DAFP. Guía para la identificación y declaración de conflicto de intereses en el sector público colombiano V2 Julio de 2019. Disponible en: (<https://www.funcionpublica.gov.co/documents/36031014/36151539/Guia-identificacion-declaracion-conflicto-intereses-sector-publico-colombiano.pdf/81207879-d5debec7-6a7e-8ac1882448c2?t=1572381672818> )

Departamento Administrativo de la Función Pública DAFP. Guía para la administración de riesgos y el diseño de controles en entidades públicas V5 diciembre 2020. Disponible en: ([https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document\\_library/bGsp2IjUBdeu/view\\_file/34316499](https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499))

Alcaldía Mayor de Bogotá. Ruta Metodológica para la Implementación del SARLAFT en las Entidades Distritales V1 diciembre de 2020. Disponible en:

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

(<https://secretariageneral.gov.co/transparencia/informacion-interes/lineamientos-distritales/ruta-metodologica-la-implementacion-del-sarlaft-las-entidades-distritales>)

Decreto Distrital 189 de 2020 “Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones”. Disponible en: (<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=95985>)

Alcaldía Mayor de Bogotá. Lineamientos para la identificación de riesgos de corrupción en Trámites, OPA y consultas de información distritales 2021. Facilitado por: Subsecretaria de Servicio al Ciudadano y Secretaría Jurídica Distrital Circular 006 de 26abr2021

Alcaldía Mayor de Bogotá. Directiva 001 de 2021 “Directrices para la atención y gestión de denuncias por posibles actos de corrupción, y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses y protección de identidad del denunciante” marzo 2021. Disponible en: (<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=108172>)

#### Control de versiones:

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
23//08/2018	1	Versión inicial, aprobada en Comité Institucional de Coordinación de Control Interno	Sonia Córdoba Alvarado – jefe Oficina Asesora Planeación
30/04/2019	2	Se actualiza la Política de riesgos, adoptando la Guía de administración de riesgos DAFP versión 4 2018.	Luis Fernando - jefe Oficina Asesora de Planeación Deisy Estupiñán – Contratista Equipo SIG
24/06/2021	3	Se actualiza la Política de riesgos, adoptando la Guía de administración de riesgos DAFP versión 5 2020, así como los lineamientos “particulares” emitidos por la Alcaldía Mayor de Bogotá y órganos generadores de política para riesgos de corrupción en Trámites y/o OPAs, y Lavado de Activos	Luis Fernando Mejía- jefe Oficina Asesora de Planeación y Deisy Estupiñán – Contratista Equipo SIG
29/09/2022	4	Se actualiza la Política de riesgos en los numerales 2 Alcance, 3 Tipologías riesgos (Corrupción), Paso 2 Identificación de riesgos, 6 Conceptos Clave, 8 Referencias, integrando lineamientos preventivos de cohecho y soborno, articulados con la GM-PO-02 Política Antisoborno de la FUGA, conforme a la Guía de Lineamientos de la Veeduría Distrital. De otra parte, se integran en el Numeral 3 Tipología riesgos (Seguridad Información) la relación de activos críticos identificados, formalizarlos y priorizados, en el marco del Modelo de Seguridad y Privacidad de la Información) conforme al Orfeo 20222900090123, como lo	Luis Fernando Mejía- jefe Oficina Asesora de Planeación y Deisy Estupiñán – Contratista SIG Alba Rojas - Contratista MIPG

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4

Fecha	Versión	Razón del cambio	Responsable Equipo SIG
		dicta el paso 7 de la guía de activos de información Fuga.	

<b>Elaboró:</b> Alba Cristina Rojas / Contratista Apoyo Planeación MIPG – SIG  Deisy Estupiñán / Contratista Apoyo Planeación SIG  Edwin Diaz – Profesional Apoyo Gestión de Tecnologías	<b>Revisó:</b> Luis Fernando Mejía Jefe Oficina Asesora de Planeación  Angélica Hernández Rodríguez Jefe Oficina Control Interno	<b>Aprobó:</b> Comité de Dirección del 29 de septiembre de 2022
--	---	---

	<b>Proceso:</b>	Gestión de mejora		
	<b>Documento:</b>	Política de administración del riesgo	<b>Código:</b> GM-PO-01	<b>Versión:</b> 4