

## **POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO**



## ANTECEDENTES

La Constitución Política de Colombia, en sus artículos 209 y 269, incorporó el control interno como un instrumento orientado a garantizar el logro de los objetivos de cada entidad del Estado y el cumplimiento de los principios que rigen la función pública.

Por otra parte, la Ley 87 de 1993, en su artículo 2°, literales a) y f), establece que el control interno está orientado a la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten, y a definir y aplicar medidas para prevenirlos, así como detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

La Ley 1474 de 2011, Estatuto Anticorrupción, dispone en su artículo 73 que todas las entidades deben elaborar anualmente un Programa de Transparencia y Ética Pública, el cual debe incluir el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti tramites y los mecanismos para mejorar la atención al ciudadano.

En tal sentido, la Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del derecho de Acceso a la Información Pública Nacional; en el literal g) del artículo 9 establece el deber de publicar el Programa de Transparencia y Ética Pública, en los sistemas de información del Estado o herramientas que lo sustituyan.

De igual manera, el Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública; señala en su artículo 2.2.21.3.2 que los elementos mínimos del Sistema de Control Interno mencionados en la Ley 87 de 1993 y demás normativa relacionada, conforman cinco (5) grupos que se interrelacionan y que constituyen los procesos fundamentales de la administración: Dirección, Planeación, Organización, Ejecución, Seguimiento y Control (Evaluación). Así mismo, señala que los responsables de fortalecer la interrelación y funcionamiento armónico de los elementos que conforman estos 5 grupos son los servidores públicos en cumplimiento de las funciones asignadas en la normativa vigente, de acuerdo con el área o dependencia de la cual hacen parte.

En esta misma vía, el Decreto 1499 de 2017, actualiza el Modelo Integrado de Planeación y Gestión - MIPG, articulando “el nuevo Sistema de Gestión, que integra los anteriores sistemas de Gestión de Calidad y de Desarrollo Administrativo, con el Sistema de Control Interno actualizado también en la séptima dimensión”, con el fin de “consolidar, en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente, y que esto se refleje en la gestión del día a día”.

Que de acuerdo con el artículo 2.2.23.2 del mismo Decreto, la actualización del Modelo Estándar de Control Interno -MECI, se efectuará a través del Manual Operativo del Modelo Integrado de Planeación y Gestión (MIPG), el cual será de obligatorio cumplimiento y aplicación para las entidades y organismos a que hace referencia el artículo 5° de la Ley 87 de 1993.

Que conforme a la estructura establecida en el Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG, en la Dimensión Séptima “Control Interno”, se define la estructura del Modelo Estándar de Control Interno - MECI el cual se fundamenta en cinco componentes: (I) Ambiente de control, (II) Administración del Riesgo, (III) Actividades de Control, (IV) Información y Comunicación y (V) Actividades de Monitoreo.

Que, atendiendo a los lineamientos del componente de Administración del Riesgo, es necesaria la formulación de la política de administración del riesgo de la Entidad, acorde a lo indicado en el numeral 7.2.2. "Asegurar la gestión del riesgo en la entidad" del Manual Operativo del MIPG y de acuerdo al “concepto técnico emitido por el Departamento Administrativo de la Función Pública sobre la obligatoriedad de la implementación del Modelo Integrado de Planeación y gestión – MIPG, en el cual se concluye que, la Región Metropolitana Bogotá – Cundinamarca, no hacen parte de alguna de las categorías de la rama ejecutiva del orden nacional y territorial señalada en los artículos 38 y 39 de la Ley 489 de 1998, siendo un esquema asociativo territorial, no se encuentra obligada a la implementación integral del Modelo Integrado de Planeación y Gestión, pero al hacer parte de la Administración Pública y cumplir funciones administrativas, sí debe implementar el Modelo Estándar de Control Interno y las políticas de gestión y desempeño que deban adoptar en cumplimiento de la normatividad vigente, para lo cual la entidad debe realizar su propio análisis jurídico, identificando de manera concreta las normas que le son aplicables”<sup>1</sup>.

En concordancia con lo anterior, la 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”, fortaleció los mecanismos de control en las entidades públicas al establecer lineamientos orientados a consolidar la gestión ética, la rendición de cuentas y la integridad en el ejercicio de lo público. Esta norma busca robustecer las herramientas de prevención de actos de corrupción, mejorar la eficiencia en el uso de los recursos públicos y promover una mayor confianza ciudadana en la administración estatal, en armonía con lo dispuesto en la Constitución y en las demás disposiciones que regulan el Sistema de Control Interno.

Que a través del Acto Legislativo 02 del 22 de julio de 2020, que modificó el artículo 325 de la Constitución Política, se creó la Región Metropolitana Bogotá-Cundinamarca, reglamentada por la Ley 2199 del 2022, a través de la cual se expidió el régimen especial de la Región Metropolitana Bogotá - Cundinamarca.

Que en virtud de lo dispuesto en el artículo 3 de la Ley 2199 de 2022, la Región Metropolitana Bogotá-Cundinamarca es una entidad administrativa de asociatividad regional con régimen especial, dotada de personería jurídica de derecho público, autonomía administrativa y patrimonio propio, a través de la cual las entidades territoriales que la integran concurren en el ejercicio de las competencias que les corresponden, con el fin de hacer eficaces los principios constitucionales de coordinación, concurrencia,

---

<sup>1</sup> Concepto Técnico emitido por el Departamento Administrativo de Función Pública del 18 de febrero de 2025  
Plantilla para Elaboración de Políticas V1

complementariedad y subsidiariedad en la función administrativa y en la planeación del desarrollo dada su interdependencia geográfica, ambiental, social o económica.

Por lo anterior, y atendiendo a los lineamientos establecidos por el Departamento Administrativo de la Función Pública – DAFP, Secretaría de Transparencia de la Presidencia de la República y el Ministerio de las Tecnologías de la Información y Comunicaciones- MinTic- a través de la Guía para la Gestión Integral del Riesgo en Entidades Públicas 2025, se formula la Política Integral de Riesgos para la Región Metropolitana Bogotá – Cundinamarca y estará sujeto a futuras modificaciones

## **1. OBJETIVO**

Establecer los lineamientos para la toma de decisiones relacionadas con el tratamiento de los riesgos y sus efectos en la Región Metropolitana Bogotá–Cundinamarca, con el fin de garantizar una gestión adecuada de los riesgos de gestión, fiscales, de seguridad de la información e integridad pública. (Corrupción, soborno y conflicto de interés). Todo ello orientado a disminuir la vulnerabilidad institucional frente a situaciones que puedan afectar el cumplimiento de la misión, así como el logro de los objetivos estratégicos y de los procesos vigentes.

## **2. ALCANCE**

La Política de Administración de Riesgos de la Región Metropolitana Bogotá–Cundinamarca se aplica para todas las dependencias, procesos, servidoras y servidores de la Entidad, en todos los niveles jerárquicos y áreas misionales, estratégicas, de apoyo y de control bajo la responsabilidad de los líderes de proceso.

## **3. DECLARACIÓN DE COMPROMISOS**

La Alta Dirección, el Representante Legal y el Comité Institucional de Coordinación Control Interno (CICCI) de la Región Metropolitana Bogotá–Cundinamarca se comprometen a gestionar los riesgos identificados en el mapa de riesgos institucional. Estos estarán sujetos a monitoreo, seguimiento y actualización, mediante la aplicación de las herramientas y lineamientos establecidos por la Entidad. Asimismo, se garantizará la disposición de los recursos físicos, presupuestales y de talento humano necesarios para la implementación y desarrollo de la presente política.

## **4. ASPECTOS PARA LA IMPLEMENTACIÓN**

Para la implementación de la presente política, se deberán considerar los lineamientos y orientaciones metodológicas establecidos en las guías y herramientas dispuestas por el Departamento Administrativo de la Función Pública (DAFP), la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Dichos lineamientos orientan la administración de los riesgos de gestión, fiscales, de seguridad de la información e integridad pública al interior de la Región Metropolitana Bogotá–Cundinamarca.

Para la identificación de los riesgos se deberán tener en cuenta, en primera instancia, los siguientes aspectos:

- Objetivos y alcance de cada uno de los procesos.
- Análisis de factores internos y externos que pueden derivar en riesgos que afecten el cumplimiento de los objetivos de los procesos e institucionales.

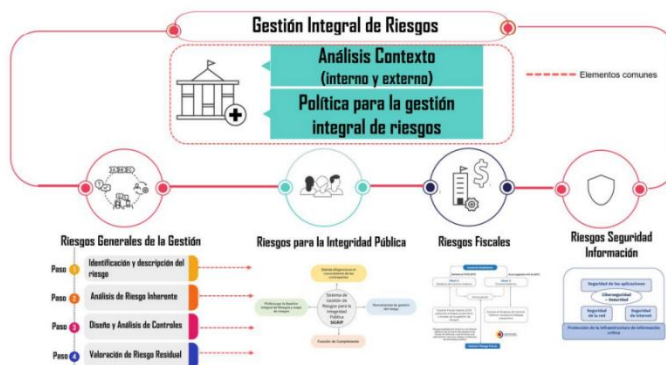
A continuación, se presenta el esquema metodológico adoptado por la Región Metropolitana Bogotá–Cundinamarca, el cual constituye la guía institucional para la identificación, análisis, diseño, valoración y tratamiento de los riesgos de gestión, fiscales, de seguridad de la información e integridad pública

**5. ESQUEMA METODOLÓGICO APLICABLE.**

La Región Metropolitana Bogotá – Cundinamarca adoptará la metodología para la administración y gestión integral de riesgos definida por el Departamento Administrativo de la Función Pública, la cual servirá como marco de referencia para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos institucionales. Para los procesos de identificación, valoración y tratamiento de los riesgos, la RMBC adoptará el formato establecido por el Departamento Administrativo de la Función Pública (DAFP), garantizando la estandarización y coherencia con los lineamientos en materia de gestión del riesgo. Esta metodología contempla lineamientos específicos para la gestión de riesgos de integridad pública, riesgos fiscales, riesgos asociados a la seguridad de la información y riesgos de gestión, asegurando un enfoque articulado y preventivo que fortalezca la transparencia, la eficiencia en el uso de los recursos públicos y la confianza ciudadana.

De igual forma, el análisis integral de los riesgos permitirá identificar y gestionar aquellos factores que puedan afectar el cumplimiento de las funciones y objetivos de la entidad, tales como la afectación al patrimonio público, la vulneración de activos de información, la disminución de la confianza de las partes interesadas en el uso del entorno digital, así como conductas asociadas a comportamientos no éticos que contrarían el ejercicio íntegro del servicio público. En este sentido, a continuación, se presenta de manera gráfica la articulación de estos ámbitos dentro del marco general para la gestión integral del riesgo.

**Ilustración 1. Articulación ámbitos gestión del riesgo**



Fuente: Dirección de Gestión y Desempeño Institucional. DAFP. 2025

Teniendo en cuenta la estructura metodológica general descrita anteriormente, a continuación, se presentan los pasos para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos asociados a la integridad pública, riesgos fiscales, riesgos asociados a la seguridad de la información y riesgos de gestión de la Región Metropolitana Bogotá – Cundinamarca. Este desarrollo metodológico busca garantizar una gestión integral que permita anticipar, mitigar y controlar los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

## 6. RIESGOS DE GESTIÓN

Los riesgos de gestión se refieren a la posibilidad de que ocurran eventos que afecten el cumplimiento y logros de los objetivos de un proceso dentro de la entidad. Estos riesgos pueden surgir de diversos factores internos o externos y pueden tener impactos negativos en la eficiencia, la calidad, la continuidad o la reputación del proceso.

### 6.1 Metodología para el levantamiento del mapa de riesgos de gestión.

#### **Paso 1: Identificación y descripción del riesgo**

La identificación del riesgo es el proceso de reconocer, enumerar y documentar los posibles riesgos que pueden afectar a un proceso específico dentro de la entidad. Implica un análisis exhaustivo de las actividades, los recursos, los procesos y el entorno en el que opera la entidad para determinar qué eventos o situaciones podrían impedir el logro de los objetivos.

A continuación, se detallan los aspectos claves para la identificación de los riesgos de integridad pública, riesgos fiscales, riesgos asociados a la seguridad de la información y riesgos de gestión.

**6.1.1 Identificación de áreas de impacto:** El 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) y reputacional.

**6.1.2 Identificación de áreas de factores de riesgo:** Son las fuentes generadoras de riesgos. Esto en circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. (Ejecución y administración de procesos, talento humano, tecnología, infraestructura y evento externo, Transacción u Operación (aplica para LA/FT/FP).

**6.1.3 Descripción del riesgo:** La descripción del riesgo debe contener todos los detalles necesarios para facilitar su comprensión, tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

- **Impacto:** son las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

- **Causa inmediata:** circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Se plantea ¿por qué puede ocurrir? el evento no deseado, bajo el análisis de la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, información esencial para la definición de controles en el paso 3 de diseño y análisis de controles.

A continuación, se presenta de manera gráfica la estructura orientadora para la redacción de los riesgos, la cual establece los elementos básicos que deben considerarse para su formulación clara y precisa.

**Ilustración 2. Estructura para la redacción del riesgo**



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Paso 2: Análisis de Riesgo Inherente**

El riesgo inherente se define como el nivel de riesgo propio de una actividad. Es el resultado de combinar la probabilidad con el impacto y permite determinar el nivel del riesgo inherente dentro de unas escalas de severidad.

Dentro de este análisis, se deben considerar los aspectos de calificación y evaluación del riesgo; además dependerá de la información obtenida, de la identificación de riesgos y de la disponibilidad de datos históricos y aportes de los líderes de proceso, servidores públicos y contratistas de la entidad.

**6.1.4 Determinar la probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

El análisis busca establecer la probabilidad de ocurrencia de los riesgos, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo (riesgo inherente). Para ello, la Región Metropolitana Bogotá – Cundinamarca adopta las siguientes tablas de probabilidad para la valoración de los riesgos.

**Tabla 1. Criterios para definir el nivel de probabilidad**

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
<b>Muy Baja</b>	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
<b>Baja</b>	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
<b>Media</b>	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
<b>Alta</b>	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
<b>Muy Alta</b>	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**6.1.5 Determinar el impacto:** Son las consecuencias que puede generar para la entidad la materialización de un riesgo. Para el caso de los riesgos fiscales, únicamente aplica la columna de afectación económica, dado que este tipo de riesgos siempre conllevan un impacto económico, en la medida en que el efecto negativo recae sobre un bien, recurso o interés patrimonial de naturaleza pública.

Cuando un riesgo presente impactos de tipo económico y reputacional en diferentes niveles, deberá considerarse siempre el nivel más alto. Por ejemplo, si un riesgo determinado se califica con impacto económico en nivel mayor y con impacto reputacional en nivel moderado, prevalecerá el nivel mayor, a fin de asegurar un tratamiento preventivo más riguroso.

En la siguiente tabla se presentan los criterios que orientan la valoración del nivel de impacto, constituyéndose en un referente para la gestión integral de riesgos de la Región Metropolitana Bogotá – Cundinamarca.

**Tabla 2. Criterios para definir el nivel de impacto**

	AFECTACIÓN ECONÓMICA	AFECTACIÓN REPUTACIONAL
<b>Leve 20%</b>	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
<b>Menor 40%</b>	Mayor a 10 y Menor a 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.
<b>Moderado 60%</b>	Mayor a 50 y Menor a 100 SMLMV.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
<b>Mayor 80%</b>	Mayor a 100 y Menor a 500 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
<b>Catastrófico 100%</b>	Mayor a 500 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Actualizada Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

### Paso 3: Diseño y Análisis de Controles

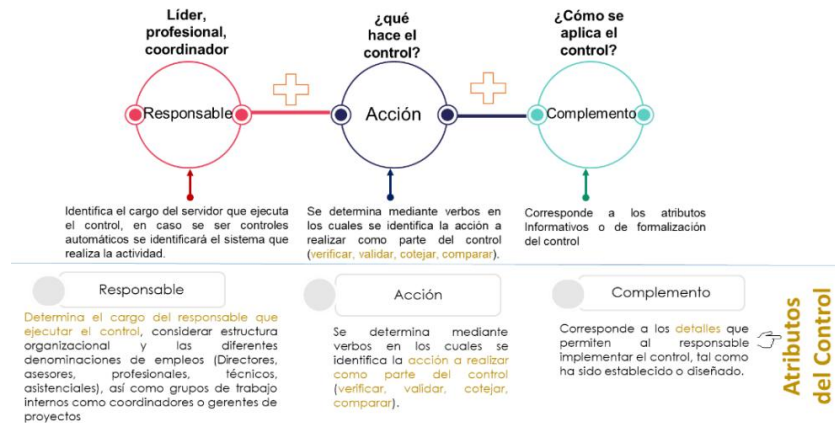
Los controles corresponden a las medidas de tratamiento que permiten modificar el riesgo, porque actúan sobre alguna de las dos variables de su medición (probabilidad o impacto), bien sea para detectarlo a tiempo (evitar que se materialice) o reducirlo (minimizar las consecuencias). Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

**6.1.6 Estructura para la Descripción del Control:** para un adecuado diseño de las actividades de control se propone una estructura para su redacción que agrupa los atributos necesarios para garantizar su implementación de forma efectiva. A continuación, se detalla la estructura propuesta para el diseño de los controles:

- **Responsable:** Determina el cargo del responsable que ejecuta el control, se deberá considerar la estructura organizacional y las diferentes denominaciones de empleos (directores, asesores, profesionales, técnicos, asistenciales), así como su despliegue en grupos de trabajo internos e incluir coordinadores o gerentes de proyectos. Cuando se trate de controles automáticos se identificará el responsable de su calibración o parametrización periódica en el sistema de información o software a través del cual opere el control.
- **Acción:** Determina para qué se realiza el control, se deben utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar
- **Complemento:** Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:
  - ✓ **Documentación:** se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
  - ✓ **Frecuencia:** corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
  - ✓ **Evidencia:** permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
  - ✓ **Ejecución:** permite establecer cómo se ejecuta el control (fuentes de información que sean confiables), así mismo qué acciones se toman en caso de desviaciones o situaciones que se detecten.

**Ilustración 3. Estructura para la redacción de controles**



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

**6.1.7 Tipologías de Controles:** se identifican las siguientes tipologías de controles, las cuales constituyen los mecanismos preventivos, detectivos y correctivos que permiten mitigar la probabilidad de ocurrencia y/o el impacto de los riesgos, fortaleciendo así la gestión institucional y el cumplimiento de los objetivos de la Región Metropolitana Bogotá – Cundinamarca:

- **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.
- **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.

Asimismo, de acuerdo con la forma en que se ejecutan, se tienen los siguientes controles:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** ejecutados por un sistema o software previamente programado o diseñado.

**6.1.8 Valoración de Controles:** determina la forma como se califican los atributos o características de eficiencia, todos los demás atributos informativos o de formalización del control. A continuación se detalla la valoración de controles y el análisis de atributos formalización del control.

**Tabla 3. Valoración de controles**

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivos	10%
Implementación	Automático	25%
	Manual	15%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional, 2020

**Tabla 4 Análisis atributos formalización del control**

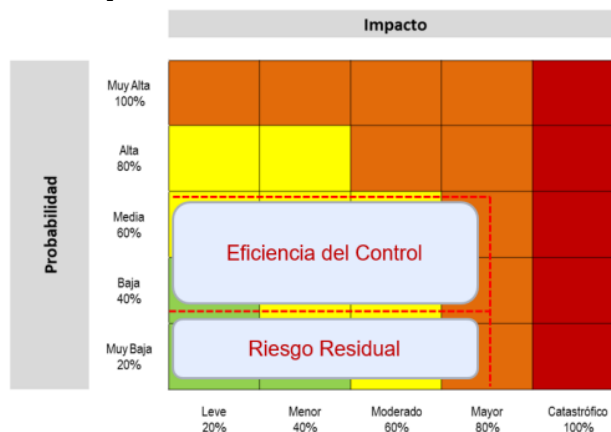
Características de Eficiencia		Descripción
<b>Documentación</b>	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
<b>Frecuencia</b>	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).	
<b>Evidencia (Trazabilidad de la ejecución)</b>	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
<b>Ejecución (Fuentes de información internas o externas)</b>	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional, 2025

**Paso 4: Valoración de Riesgo Residual**

El riesgo residual corresponde al resultado de aplicar la efectividad de los controles sobre el riesgo inherente. La evaluación del riesgo es el producto de confrontar los resultados de la evaluación del riesgo inicial (riesgo inherente) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual). Para esto se utiliza el siguiente mapa de calor.

**Ilustración 4. Mapa de calor para la determinación del nivel de severidad del riesgo**



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

## 6.2 Tratamiento de los riesgos.

La Región Metropolitana Bogotá–Cundinamarca establece, para la administración de los riesgos institucionales, los siguientes niveles: Extremo, Alto, Moderado y Bajo. En concordancia con dichos niveles, el tratamiento de los riesgos se orienta a la toma de decisiones acordes con las características de los riesgos identificados, considerando especialmente el riesgo residual. En este sentido, el líder del proceso deberá definir la alternativa de tratamiento más adecuada entre las siguientes: Aceptar, reducir o evitar

- **Aceptar el riesgo.** Si el nivel de riesgo residual se encuentra en zona BAJA se define asumir el riesgo y no se requiere formular acciones para su mitigación.
- **Reducir el riesgo.** Si el nivel de riesgo residual se encuentra en las zonas MODERADO, ALTO, EXTREMO se deberá realizar un análisis por parte del líder del proceso de acuerdo con los siguientes criterios, y considerar cuál es la mejor opción para el tratamiento, ya sea mitigar o transferir el riesgo.
  - a) **Mitigar el riesgo:** Después de realizar un análisis de acuerdo con los criterios establecidos frente al riesgo residual, esto para los procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente, se implementa un plan de acción que permita mitigar el nivel del riesgo. No necesariamente es un control adicional.
  - b) **Compartir el riesgo:** Después de realizar un análisis, de acuerdo con los criterios establecidos frente al riesgo residual, esto para los procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente, se considera que la mejor estrategia es 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 sobre el tema reputacional
- **Evitar el riesgo.** Cuando los escenarios de riesgo identificados se consideran demasiado EXTREMO se puede tomar una decisión para evitar el riesgo, mediante la cancelación de la actividad o un conjunto de actividades. Es decir, se puede determinar no asumir la actividad que genera el riesgo.

## 6.3 Apetito del riesgo

La Región Metropolitana ha definido niveles de apetito de riesgo que orientan la gestión institucional. Conforme a estos lineamientos, se establecen los niveles de aceptación que determinan hasta qué punto la RMBC está dispuesta a asumir riesgos para alcanzar sus objetivos estratégicos.

**Tabla 5. Apetito del riesgo.**

Nivel de Riesgo Residual	Decisión Institucional (RMBC)	Acciones a implementar
<b>Zona de riesgos residual BAJO</b>	Se asume el riesgo.	<p><b>La RMBC acepta el riesgo</b>, el cual se gestiona mediante las actividades propias del proceso y no requiere un plan de acción adicional.</p> <p>Los riesgos de corrupción, lavado de activos (LA), financiación del terrorismo (FT) y financiación de la proliferación (FP) no serán aceptados por la Región Metropolitana Bogotá–Cundinamarca (RMBC).</p>
<b>Zona de riesgos residual MODERADO - ALTO</b>	No se acepta el riesgo	<p><b>La RMBC no acepta el riesgo</b>; por ello, se adoptarán medidas para <b>mitigarlo</b> mediante la formulación e implementación de planes de acción o <b>compartirlo</b>, mediante la tercerización de la actividad que lo genera, o mediante el traslado del riesgo a través de seguros o pólizas.</p>
<b>Zona de riesgos residual EXTREMO</b>	No se acepta el riesgo	<p><b>La RMBC no acepta el riesgo</b>; por ello, se adoptarán medidas para <b>mitigarlo</b> mediante la formulación e implementación de planes de acción o <b>compartirlo</b>, mediante la tercerización de la actividad que lo genera, o mediante el traslado del riesgo a través de seguros o pólizas.</p> <p>De igual manera, cuando los escenarios de riesgo identificados se consideran demasiado extremos, se puede tomar la decisión de <b>evitar el riesgo</b> mediante la cancelación de la actividad o del conjunto de actividades. Es decir, se puede determinar no asumir la actividad que genera el riesgo</p>

Fuente: Elaboración Región Metropolitana Bogotá – Cundinamarca

## 7. GESTIÓN DE RIESGOS FISCALES

Los riesgos fiscales corresponden a todas aquellas actividades asociadas a la gestión fiscal que han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, y que potencialmente pueden ocasionar daños a un bien, recurso o interés de naturaleza patrimonial. Estos riesgos inciden directamente en la eficiencia y efectividad del control fiscal.

### 7.1 Definición y elementos del riesgo fiscal:

El riesgo fiscal se define de la siguiente manera: *Efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un **evento potencial**.*

A continuación, se describen los elementos que componen la definición de riesgo fiscales

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

Lo anterior se puede resumir de la siguiente manera:

$$\text{Riesgo Fiscal} = \text{Evento Potencial (Potencial Conducta)} + \text{Efecto dañoso (Potencial Daño)}$$

## 7.2 Metodología para el levantamiento del mapa de riesgos fiscales.

Si bien la metodología aplicable para la identificación, clasificación, valoración y control del riesgo fiscal corresponde a lo dispuesto en los capítulos 6 de la presente política, es preciso señalar que, debido a las particularidades propias de este tipo de riesgos, a continuación, se desarrolla la especificidad correspondiente a los riesgos de naturaleza fiscal, con el propósito de fortalecer la protección de los recursos, bienes e intereses patrimoniales del Estado.

### **Paso 1:** identificación de riesgos fiscales.

**7.2.1 Puntos de riesgo y las circunstancias inmediatas:** los puntos de riesgo fiscal son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal, para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal. En cuanto a las circunstancias inmediatas son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.

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

**7.2.3. Identificar el efecto económico:** El efecto económico del riesgo fiscal es el potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público.

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

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

- ✓ Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- ✓ Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero, es decir, de alguien que no tenga la calidad de gestor público

- ✓ Multas impuestas por hechos que no comportan gestión fiscal
- ✓ Existencia de actuación de cobro coactivo por parte de la entidad.
- ✓ Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, ésta se encuentra regulada como aceptable, normal u ordinaria dentro de la actividad del servidor público, tal como los que suceden por desgaste natural.

**7.2.4. Identificación de la causa raíz o potencial hecho generador:** la causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.

**7.2.5. Descripción del Riesgo Fiscal:** para redactar un riesgo fiscal, se debe tener en cuenta:

Iniciar con la expresión: *Posibilidad de*, dado que nos estamos refiriendo al evento potencial.

- ✓ **Impacto:** corresponde al qué. Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).
- ✓ **Circunstancia inmediata:** corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
- ✓ **Causa Raíz:** corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño.

A continuación, se muestran algunos ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso.

**Tabla 6. Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso**

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 aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la omisión en el cumplimiento de la licencia ambiental de los proyectos de infraestructura.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por no tener incluidos todos los bienes muebles e inmuebles de la entidad en el contrato de seguro, a causa de la omisión en la actualización de bienes que cubren de dicho contrato.
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la aplicación de medidas de prevención frente a posibles sobrecargas eléctricas.	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 no devolución al tesoro público de los rendimientos financieros generados por recursos de anticipo, a causa de la omisión por parte de la interventoría y/o supervisión de la interventoría al no exigir la devolución al contratista

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

### **Paso 2: Valoración del riesgo fiscal**

En esta etapa se realiza la Evaluación de riesgos que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

- ✓ **Probabilidad:** La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.
- ✓ **Impacto:** Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública.

**7.2.6 Determinación del nivel de riesgo inherente:** para la evaluación del riesgo fiscal, se aplicarán las tablas de frecuencia e impacto descritos en los (capítulos 6, paso 2) de la presente política.

### **Paso 3. Diseño y Valoración de controles**

Para el análisis y evaluación de los controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Se aplican los lineamientos para la redacción del control descritos en el (capítulo 6, paso 3) de la presente política.

### **Paso 4: Valoración de Riesgo Residual**

Para el análisis y evaluación del riesgo residual se aplican los lineamientos para la redacción del control descritos en el (capítulo 6, paso 4) de la presente política.

## **8. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

Los riesgos de seguridad de la información se refieren a las amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de la información dentro de la entidad, y que podrían causar una pérdida o daño en un activo de información.

### **8.1 Metodología para el levantamiento del mapa de riesgos de seguridad de la información.**

Si bien la metodología aplicable para la identificación, clasificación, valoración y control del riesgo seguridad de la información corresponde a lo dispuesto en los capítulos 6 y 10 de la presente política, es preciso señalar que, debido a las particularidades propias de este tipo de riesgos, a continuación, se desarrolla la especificidad correspondiente a los riesgos de seguridad de la información.

**Paso 1: Identificación y descripción de riesgos de seguridad de la información**

**8.1.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados:** en primer lugar, se deben identificar los activos de Información mediante las actividades descritas en los “*Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional*” del MSPI, en esta se presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad. Los riesgos de seguridad de la información estarán asociados a la pérdida de uno o más de los siguientes factores:

- Pérdida de Confidencialidad
- Pérdida de Integridad
- Pérdida de Disponibilidad

**Tabla 7. Conceptualización activos de información**

<b>¿QUÉ SON LOS ACTIVOS?</b>	<b>¿POR QUÉ IDENTIFICAR LOS ACTIVOS?</b>
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: <ul style="list-style-type: none"> <li>- Aplicaciones de la organización</li> <li>- Servicios web -Redes</li> <li>- Información física o digital</li> <li>- Tecnologías de información TI</li> <li>- Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital</li> </ul>	Permite determinar qué es lo más importante que cada entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).  La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

**8.1.2 Identificación de áreas de impacto:** el área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

**8.1.3 Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos. En la siguiente tabla se definen los elementos necesarios:

**Tabla 8. Amenazas y Vulnerabilidades**

<b>MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN</b>	
<b>Amenazas (Causa Inmediata)</b>	<b>Vulnerabilidades (Causa raíz)</b>

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- ✓ **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022)
- ✓ **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022)

**8.1.4 Descripción del riesgo:** en este paso se identifican:

**Tabla 9. Riesgos de Seguridad de la Información**

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

**Tipo de Riesgo:** Este campo solo admite uno de estos 3 valores:

- ✓ Pérdida de Disponibilidad
- ✓ Pérdida de Integridad
- ✓ Pérdida de Confidencialidad

**8.1.5 Descripción del Riesgo:** En este campo se describe la situación específica que da como resultado el correspondiente riesgo.

*“Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, los cuales la entidad pública debe identificar, valorar y posteriormente tratar si el nivel de dicho riesgo lo amerita.”*

**Paso 2: Análisis de Riesgo Inherente**

En este paso metodológico, se aplican las tablas y matrices definidas en el (capítulos 6, paso 2) de la presente política, que desarrolla los lineamientos para los riesgos generales de la gestión.

**8.1.6 Determinar la probabilidad:** En esta actividad se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

**Tabla 10. Frecuencia**

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Frecuencia	% Probabilidad inherente	Probabilidad inherente

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- ✓ **Frecuencia:** Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.
- ✓ **% Probabilidad Inherente:** Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa. (Ver capítulo 6 tabla 1), Criterios para definir el nivel de probabilidad.
- ✓ **Probabilidad inherente:** Este campo corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa. Ver capítulo 6 tabla 1), Criterios para definir el nivel de probabilidad

**8.1.7 Determinar el impacto:** En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos.

**Tabla 11. Impacto**

IMPACTO	
% Impacto Inherente	Impacto Inherente

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

**% Impacto Inherente:** Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa. (Ver Capítulo 6 tabla 2), Criterios para definir el nivel de impacto.

**Impacto Inherente:** Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa. (Ver Capítulo 6 tabla 2), Criterios para definir el nivel de impacto.

**Paso 3: Diseño y Análisis de Controles**

En esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

**Tabla 12. Afectación**

No. Control	Control Anexo A	Descripción del Control
-------------	-----------------	-------------------------

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

**No. Control:** Este campo es un consecutivo de los controles a establecer.

**Control Anexo A:** Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.

**NOTA:** Las entidades pueden crear controles adicionales a los listados en el anexo A de la norma ISO 27001:2022 de acuerdo a sus necesidades.

**Descripción del Control:** Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad.

**NOTA:** Se recomienda que la entidad establezca para cada control técnico el correspondiente control administrativo, de tal manera que estos se complementen y potencialicen.

**8.1.8 Valoración de Controles**

**Afectación**

En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

**Tabla 13. Afectación**

AFECTACIÓN	
Probabilidad	Impacto

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

**Probabilidad:** En este campo se especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.

**Impacto:** En este campo se especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

**Atributos:**

En esta actividad se establecen los atributos de la implementación del control, donde se consideran atributos de eficiencia y los de formalización del control, de acuerdo con el (capítulo 6 Tabla 3 y 4) de la presente política

**Paso 4: Valoración de Riesgo Residual**

Para el análisis y evaluación del riesgo residual se aplican los lineamientos establecidos en el capítulo 6, paso 4) de la presente política.

## 9. SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP es un conjunto articulado de elementos que operan e interactúan entre sí, orientado a fortalecer la gestión institucional y a garantizar un entorno íntegro en el ejercicio de lo público.

Su propósito principal es que la Región Metropolitana Bogotá–Cundinamarca identifique, valore y gestione los riesgos que puedan afectar la integridad pública, al tiempo que refuerce los mecanismos de prevención y control frente a la corrupción, el fraude, el soborno, los conflictos de interés, así como el lavado de activos y la financiación del terrorismo (LA/FT/FP). De igual manera, promueve que la gestión de riesgos se integre en la operación institucional, asegurando su articulación con el Programa de Transparencia y Ética Pública.

De esta forma, el SIGRIP contribuye a que los colaboradores de la Región Metropolitana Bogotá–Cundinamarca actúe con transparencia, ética y responsabilidad, protegiendo la confianza ciudadana, la integridad de los servidores públicos, el patrimonio del Estado y garantizando el uso adecuado de los recursos público.

La estructura del SIGRIP, compuesta por sus elementos centrales y de apoyo, se presenta a continuación, como marco orientador para la gestión de riesgos en materia de integridad pública dentro de la entidad.

**Ilustración 6. Sistema de Gestión de Riesgos para la Integridad Pública**



Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

**9.1 Liderazgo del Sistema**

El Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP– contará con niveles claramente definidos de responsabilidad frente a su planificación, implementación y seguimiento en la Región Metropolitana Bogotá–Cundinamarca. Dichos niveles reconocen que la gestión del riesgo es un proceso integral que involucra a toda la organización, en el que la participación institucional resulta esencial para garantizar su eficacia. En este sentido, el SIGRIP se articula con el Modelo Estándar de Control Interno –MECI–, asegurando coherencia entre los mecanismos de prevención, control y aseguramiento, y fortaleciendo la capacidad institucional para anticipar, mitigar y responder de manera efectiva a los riesgos que puedan afectar la integridad pública. A continuación, se presentan los roles y responsabilidades asociados al SIGRIP acorde al esquema de líneas de defensa.

**Tabla 14. Roles y responsabilidades SIGRIP**

LÍNEA DE DEFENSA	RESPONSABILIDAD FRENTE AL SIGRIP
<b>LÍNEA ESTRATÉGICA</b>  Instancia decisoria del Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP recae sobre Alta Dirección, Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno	Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP
<b>PRIMERA LÍNEA DE DEFENSA:</b>  Esta bajo la responsabilidad de directores, subdirectores, asesores y líderes de proceso, servidores y colaboradores	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.
<b>SEGUNDA LÍNEA DE DEFENSA:</b>  Está, principalmente, bajo la responsabilidad, de la Dependencia o servidor público designada por la Alta Dirección para la implementación del SIGRIP	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento
<b>TERCERA LÍNEA DE DEFENSA:</b>  Bajo la responsabilidad de la Oficina de Control Interno.	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

## 9.2 Operación del SIGRIP

Para garantizar una adecuada planificación e implementación del Sistema de Gestión de Riesgos para la Integridad Pública –SIGRIP– en la Región Metropolitana Bogotá–Cundinamarca, el servidor o servidora pública designada por la Alta Dirección como función de cumplimiento deberán asumir un rol central en la coordinación del sistema. El propósito de esta función es asegurar que las directrices de la política integral de gestión de riesgos se apliquen de manera uniforme en toda la organización, promoviendo la integridad, la transparencia y el fortalecimiento de los mecanismos de control. En este sentido, la función de cumplimiento deberá desarrollar, como mínimo, las siguientes funciones

### 9.2.1 Funciones de cumplimiento

- a) Velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados en su conjunto.
- b) Evaluar el SIGRIP y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Las evaluaciones deberán contemplar, además:
  - ✓ Los resultados de la gestión desarrollada en el marco de la función de cumplimiento.
  - ✓ Los reportes de operaciones generados en el marco de la gestión del riesgo.
  - ✓ Los planes de mejoramiento del SIGRIP implementados, en el marco del proceso de mejora continua.
- c) Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.
- d) Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.
- e) Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP, así como el desarrollo de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.
- f) Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.
- g) Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda
- h) Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.

- i) Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- j) Reportar a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad que corresponda, las operaciones intentadas o sospechosas que se hayan identificado conforme a los criterios definidos y el procedimiento institucional adoptado.

**9.2.2 Requisitos para asignar la función de cumplimiento:** La función de cumplimiento puede ser asignada dentro de las plantas de personal existentes en la mayoría de las entidades públicas. Lo anterior, sin perjuicio de que la entidad decida crear un cargo específico.

En ese orden de ideas, para asignar la función de cumplimiento, deberán tenerse en cuenta los siguientes aspectos:

- a) La función puede ser asignada a una persona, grupo o dependencia, según las capacidades de la entidad. Se recomienda tener en cuenta: la estructura organizacional, la planta y cargas de trabajo, la complejidad de las operaciones y el nivel de exposición a los riesgos para la integridad pública, para determinar la capacidad que debe tener la persona, grupo o dependencia que tendrá la función de cumplimiento.
- b) La función debe estar asignada dentro del segundo nivel jerárquico de la entidad. Es decir, la persona, grupo o dependencia debe responder directa y exclusivamente a la Alta Dirección.
- c) La persona, grupo o dependencia, preferiblemente, debe dedicarse exclusivamente a desarrollar la función de cumplimiento. Sin embargo, en el evento en que la función se asigne a una persona, grupo o dependencia que no tenga dedicación exclusiva y desempeñe funciones adicionales, la Entidad debe contar con mecanismos para prevenir y gestionar los conflictos de intereses que puedan surgir producto del ejercicio de otras funciones que podrían ser objeto de evaluación.
- d) La entidad debe asegurar que la persona, grupo o dependencia se capacite de forma permanente en temas de gestión de riesgos, transparencia, integridad, sistemas de gestión antisoborno, antifraude y de cumplimiento; además deben estar actualizados en los lineamientos de la Política Nacional Antilavado de Activos, contra la Financiación del Terrorismo y contra la Financiación de la Proliferación de Armas de Destrucción Masiva.
- e) A quien se asigne la función de cumplimiento o quienes integren el grupo de trabajo o dependencia, deberán ser personas reconocidas dentro de la organización por su probidad, ética y que cumplan diligentemente con sus obligaciones, en consecuencia: no podrá haber investigaciones de ningún tipo en su contra; los resultados de sus evaluaciones de desempeño deben ser satisfactorios; deberá haber realizado las declaraciones de bienes y rentas, y de conflictos de interés, de forma oportuna y mantenerlas actualizadas según la normativa vigente.

### 9.3 Metodología para el levantamiento de los riesgos de integridad Pública.

Si bien la metodología aplicable para la identificación, clasificación, valoración y control del riesgo de integridad pública se encuentra definida en los capítulos 6 y 10 de la presente política, resulta necesario precisar que, debido a las particularidades de este tipo de riesgos, a continuación, se expone la especificidad correspondiente a los riesgos de integridad.

#### **Paso 1: Identificación y descripción del riesgo**

**9.3.1 Identificación de los puntos de riesgo:** En la gestión del riesgo de LA/FT/FP, los puntos de riesgo corresponden a las operaciones que implican intercambio de recursos, tanto cuando la entidad paga por bienes o servicios como cuando los entrega a cambio de un pago. Estos son los momentos críticos para identificar riesgos de lavado de activos, financiación del terrorismo o de la proliferación de armas. En cuanto al riesgo de corrupción y sus manifestaciones (soborno, fraude y conflictos de interés), los puntos de riesgo pueden encontrarse en cualquier actividad del proceso, no solo en las operaciones.

**9.3.2 Identificación de áreas de impacto:** En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

- **Consecuencia legal:** corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Así pues, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.
- **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**, atendiendo a lo indicado en el en (capítulo 6, paso 1) de la presente política.

**9.3.3 Identificación de factores de riesgo:** Los factores mínimos a considerar en el análisis del riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas –LA/FT/FP– son: contrapartes, productos, canales y jurisdicciones, los cuales en conjunto configuran el concepto de “transacción” u “operación”. Estos factores permiten a la Región Metropolitana Bogotá Cundinamarca fortalecer el conocimiento de las contrapartes, diseñar y aplicar señales de alerta, identificar operaciones inusuales y reportar oportunamente aquellas sospechosas.

Para lograr una gestión efectiva, es necesario implementar procesos de segmentación de los factores de riesgo, a través de los cuales se identifican grupos con características y comportamientos homogéneos internamente y heterogéneos entre sí. Esta segmentación

facilita la definición de parámetros normales de comportamiento transaccional y, a partir de ellos, la detección de operaciones que se apartan de la normalidad, generando señales de alerta que orientan la labor de la función de cumplimiento.

**9.3.3. Descripción del riesgo:** La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en el (capítulo 6, paso 1) de la presente política. Todos los riesgos identificados iniciarán con la fórmula “*Posibilidad de*”, y deben señalar el impacto, la causa inmediata y la causa raíz.

Las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP. A continuación, se presentan algunos ejemplos de referente a posibles riesgos de integridad:

- *Posibilidad de afectación económica por Corrupción en la evaluación 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.*

En el caso particular del riesgo LA/FT/FP, debe hacerse referencia particularmente a las actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo

- *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 de Riesgo Inherente**

En este paso metodológico, se aplican las tablas y matrices definidas en el (capítulo 6, paso 2) de la presente política, que desarrolla los lineamientos para los riesgos generales de la gestión.

**Paso 3: Diseño y Análisis de Controles**

Para el diseño y análisis de controles, en primera instancia se deberá considerar el *Manual para el Desarrollo del Principio de Debida Diligencia* de la Región Metropolitana Bogotá–Cundinamarca, contar con la función de cumplimiento asignada y aplicar las políticas, procedimientos, códigos y demás instrumentos de gestión orientados a la adecuada administración de los riesgos de integridad pública, de conformidad con los lineamientos establecidos en la *Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7*. Estos elementos podrán servir como insumos para la definición y aplicación de los controles diseñados.

Por lo demás, para el diseño y análisis de controles deberán referirse a los lineamientos establecidos en el (capítulo 6, paso 3), de la presente política.

**Paso 4: Valoración de Riesgo Residual**

En este paso metodológico, se aplica los lineamientos establecidos en el (capítulo 6, paso 4) de la presente política.

**10. RESPONSABILIDAD FRENTE A LA ADMINISTRACIÓN DE RIESGOS.**

La estructura del Modelo Estándar de Control Interno – MECI- se acompaña por un esquema de asignación de responsabilidades, adaptado del Modelo “Líneas de Defensa”, el cual otorga responsabilidad a todos los niveles de la Entidad. A continuación, se relacionan los roles y responsabilidades para la administración integral de los riesgos en la Región Metropolitana Bogotá – Cundinamarca.

LÍNEA DE DEFENSA	ROL PRINCIPAL	RESPONSABILIDAD FRENTE A LA ADMINISTRACIÓN DE RIESGOS.
<p><b>LÍNEA ESTRATÉGICA:</b></p> <p>Instancia decisoria dentro del Sistema de Control Interno, cuya responsabilidad recae en la Alta Dirección (Director(a))</p>	<p>Analizar los riesgos que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (Política integral del Riesgo)</p>	<p>Establecer y aprobar la Política Integral de Riesgos y hacer seguimiento para su posible actualización.</p> <p>Hacer seguimiento a la implementación de la Política integral de Riesgos al interior de la Entidad.</p>

LÍNEA DE DEFENSA	ROL PRINCIPAL	RESPONSABILIDAD FRENTE A LA ADMINISTRACIÓN DE RIESGOS.
<p>General, subdirectores y Jefes de Oficina), el Comité De Dirección, el Comité Institucional de Gestión y Desempeño y el Comité Institucional de Coordinación de Control Interno.</p>		<p>Asignar los recursos suficientes para el desarrollo de la gestión integral de riesgos en la Región Metropolitana Bogotá - Cundinamarca (presupuesto, tiempo, personal, sistemas de información y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos.</p> <p>Revisar y analizar el informe de seguimiento a la administración de riesgos integrales presentado por la Oficina de Control Interno, y tomar las decisiones pertinentes para el mejoramiento.</p>
<p><b>PRIMERA LÍNEA DE DEFENSA:</b></p> <p>Está, principalmente bajo la responsabilidad de los líderes de procesos y de sus equipos de trabajo (en general servidores públicos y contratistas de todos los niveles de la Entidad),</p>	<p>El mantenimiento efectivo de controles internos, la implementación y ejecución de las metodologías, manuales, procedimientos y demás instrumentos para la gestión integral de riesgos establecidos por la entidad.</p> <p>Los actores de la primera línea identifican, evalúan, controlan y mitigan los riesgos a través del <b>"Autocontrol"</b>.</p>	<p>Implementar las metodologías y lineamientos para la administración de riesgos establecidos por la Región Metropolitana Bogotá - Cundinamarca.</p> <p>Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar el logro del objetivo de su proceso y realizar seguimiento al mapa de riesgos a cargo.</p> <p>Realizar monitoreo a los controles y acciones establecidas en el mapa de riesgos a su cargo para mitigar los riesgos identificados.</p> <p>Proponer mejoras a la gestión integral de riesgos en su proceso y reportar en el sistema o esquema definido por la entidad los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.</p> <p>Reportar a la dependencia</p>

LÍNEA DE DEFENSA	ROL PRINCIPAL	RESPONSABILIDAD FRENTE A LA ADMINISTRACIÓN DE RIESGOS.
		designadas de las funciones de cumplimiento ( <i>segunda línea de defensa</i> ) y a la Oficina de Control Interno ( <i>tercera línea de defensa</i> ), la información solicitada para el monitoreo y seguimiento al mapa de riesgos.
<p><b>SEGUNDA LÍNEA DE DEFENSA:</b></p> <p>Está, principalmente, bajo la responsabilidad, de la Oficina o dependencia de la Función de Cumplimiento, Oficina Asesora de Planeación Institucional, y los Líderes de Sistemas de Gestión que no hacen parte de la línea estratégica, quienes responden de manera directa por el aseguramiento de la operación en materia de riesgos.</p>	<p>Garantizar que los procesos de identificación, análisis, diseño y valoración de los riesgos identificados por la Primera Línea de Defensa sean adecuados y operen de manera efectiva.</p> <p>Los actores de esta línea consolidan y analizan información sobre asuntos clave para la entidad, con el propósito de prevenir la materialización de riesgos, en el marco de la <b>“autogestión”</b>.</p>	<p>Acompañar y orientar técnicamente a los líderes de proceso y a su equipo de trabajo, en la identificación, análisis, diseño y valoración de los riesgos a su cargo, de acuerdo con la metodología y lineamientos establecidos por la Región Metropolitana Bogotá - Cundinamarca.</p> <p>Consolidar y socializar el mapa de riesgos institucional</p> <p>Monitorear la gestión del riesgo y los controles establecidos por la primera línea de defensa, acorde con la información suministrada por los líderes de procesos.</p> <p>Comunicar a los líderes de proceso, los resultados del monitoreo, con el fin de que se tomen las acciones necesarias de mejora, en caso de requerirse.</p>
<p><b>SEGUNDA LÍNEA DE DEFENSA:</b></p> <p>Está, principalmente, bajo la responsabilidad, de la Oficina de Tecnologías de la Información quien responden de manera directa por el aseguramiento de la operación en materia de riesgos de seguridad de la información</p>	<p>Garantizar que los procesos de gestión del riesgo en materia de seguridad de la información, a cargo de la Primera Línea de Defensa, sean adecuados y operen de manera efectiva.</p> <p>Los actores de esta línea consolidan y analizan información sobre asuntos clave para la entidad, con el fin de prevenir la materialización de riesgos de seguridad de la</p>	<p>Acompañar y orientar a los líderes de proceso y a su equipo de trabajo en la identificación, análisis, diseño y valoración de los riesgos de seguridad de la información de acuerdo con la metodología y lineamientos establecidos por la entidad.</p> <p>Consolidar y socializar el mapa de riesgos de seguridad de la información.</p> <p>Monitorear los controles y</p>

LÍNEA DE DEFENSA	ROL PRINCIPAL	RESPONSABILIDAD FRENTE A LA ADMINISTRACIÓN DE RIESGOS.
	<p>información, en el marco de la “autogestión”.</p>	<p>acciones de los riesgos de seguridad de la información establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos.</p> <p>Comunicar a los líderes de proceso, los resultados del monitoreo, con el fin de que se tomen las acciones necesarias de mejora, en caso de requerirse.</p>
<p><b>TERCERA LÍNEA DE DEFENSA:</b></p> <p>Bajo la responsabilidad de la Oficina de Control Interno.</p>	<p>La función de la auditoría interna, mediante un enfoque basado en riesgos, proporcionará un aseguramiento objetivo e independiente sobre la eficacia de la gestión de riesgos, así como recomendaciones orientadas a fortalecer la gestión del riesgo, mejorar los procesos y contribuir al logro de los objetivos estratégicos de la entidad.</p>	<p>Asesorar en la metodología para la identificación, análisis, diseño y valoración de los riesgos, en coordinación con la segunda línea de defensa</p> <p>Proporcionar aseguramiento objetivo sobre la efectividad de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.</p> <p>Llevar a cabo el seguimiento al mapa de riesgo institucional de conformidad con el Plan Anual de Auditoría y de acuerdo con los lineamientos del Departamento Administrativo de lo Función pública - DAFP y reportar los resultados al Comité Institucional de Coordinación de Control Interno.</p> <p>Comunicar al Comité Institucional de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías.</p> <p>Alertar sobre la identificación y materialización de riesgos de gestión, fiscales, seguridad de la información y/o integridad pública</p>

### 6.1 Acciones frente a los de riesgos materializados

En el evento de materialización de un riesgo, los responsables deberán emprender acciones en el marco de sus roles, de la siguiente manera:

LÍNEA DE DEFENSA	ROL PRINCIPAL	ACCIONES EN CASO DE MATERIALIZACIÓN
<p><b>PRIMERA LÍNEA DE DEFENSA:</b></p> <p>Está, principalmente bajo la responsabilidad de los líderes de procesos y de sus equipos de trabajo (en general servidores públicos y contratistas de todos los niveles de la Entidad),</p>	<p>En el marco del seguimiento al mapa de riesgos bajo su responsabilidad, deberá identificar oportunamente la materialización de los riesgos asignados, reportar los eventos ocurridos y activar las acciones de respuesta correspondientes para su adecuada gestión</p>	<p>Informar a la dependencia que cumpla la Función de Cumplimiento, Oficina Asesora de Planeación Institucional y a la Oficina de Tecnologías de la Información y Comunicaciones, cuando se trate de los riesgos de seguridad de la información (<i>segunda línea de defensa</i>) y a la oficina de Control Interno (<i>tercera línea de defesa</i>) sobre el riesgo materializado para tomar las acciones necesarias.</p> <p>Iniciar de manera inmediata el análisis de causas y determinar las acciones correctivas a las que haya lugar.</p> <p>Formular el plan de mejoramiento para los riesgos materializados, el cual permitirá minimizar los impactos o efectos negativos que este pueda ocasionar.</p>
<p><b>SEGUNDA LÍNEA DE DEFENSA:</b></p> <p>Está, principalmente, bajo la responsabilidad, de la dependencia u oficina que cumpla la función de cumplimiento, Oficina Asesora de Planeación Institucional, y Oficina de Tecnologías de la Información y Comunicaciones, cuando se trate de riesgos de seguridad de la información</p>	<p>Garantizar el acompañamiento a la Primera Línea de Defensa en la formulación y seguimiento de los planes de mejoramiento, con el fin de fortalecer los controles, reducir la probabilidad de recurrencia y asegurar la continuidad de la gestión institucional."</p>	<p>Acompañar a los gerentes públicos y/o líderes de proceso en la formulación del plan de mejoramiento para determinar las acciones correctivas a implementar.</p> <p>Monitorear el cumplimiento del plan de mejoramiento y acciones correctivas definidas en el marco de la materialización de los riesgos.</p> <p>Comunicar al Comité Institucional de Coordinación de Control Interno sobre los riesgos materializados.</p>
<p><b>TERCERA LÍNEA DE DEFENSA</b></p> <p>Bajo la responsabilidad de la Oficina de Control Interno.</p>	<p>Evaluar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.</p>	<p>Cuando en el marco de un ejercicio de evaluación independiente o seguimiento, la Oficina de Control Interno identifique la materialización de un riesgo,</p>

LÍNEA DE DEFENSA	ROL PRINCIPAL	ACCIÓNES EN CASO DE MATERIALIZACIÓN
		<p>deberá informar a los líderes de proceso sobre el hecho detectado, los cuales emprenderán las acciones descritas para la primera línea de defensa en este numeral</p> <p>Cuando se trate de los riesgos de corrupción, fiscal y/o integridad pública y una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance realizar la denuncia ante la instancia de control correspondiente.</p>

**11. INDICADORES CLAVE DE RIESGOS.**

Los Indicadores Clave de Riesgo (KRI) para la Región Metropolitana Bogotá–Cundinamarca serán definidos e identificados con base en los instrumentos y lineamientos establecidos dentro del marco de la planeación institucional. De esta manera, la gestión del riesgo se articulará con las prioridades estratégicas y las metas de la entidad.

**12. MONITOREO Y REVISIÓN A LA ADMINISTRACIÓN DE RIESGOS.**

El monitoreo y revisión al mapa de riesgos, estará a cargo de los Gerentes Públicos, Líderes de proceso, Líderes de Proyectos/Programas y equipos de trabajo y supervisores de contratos, en conjunto con su equipo de trabajo (*primera línea de defensa*), su finalidad principal es monitorear permanentemente la gestión del riesgo y de los controles, y de esta manera, sugerir los correctivos y ajustes cuando sea necesario para asegurar un efectivo manejo de riesgo.

El monitoreo del mapa de riesgos y de los controles establecidos se realizará de manera semestral, salvo cuando los lineamientos o la normatividad aplicable definan ciclos distintos de seguimiento y revisión. Los ciclos de control se revisarán y, de ser necesario, se ajustarán para adaptarse a los cambios, situaciones o circunstancias que puedan presentarse en la Región Metropolitana Bogotá–Cundinamarca.

**SEGUIMIENTO Y EVALUACIÓN INDEPENDIENTE**

La Oficina de Control Interno bajo el rol de evaluación de la gestión del riesgo, realizará las evaluaciones independientes que sean pertinentes, teniendo en cuenta la priorización de auditorías y los recursos asignados atendiendo la normatividad dispuesta en esta materia por parte del Departamento Administrativo de la Función Pública - DAFP y de la Secretaría de Transparencia.

### 13. DIVULGACIÓN

La Política para la Gestión Integral del Riesgo se divulgará al interior de la Región Metropolitana Bogotá - Cundinamarca, a través de los canales y medios de comunicación establecidos por la entidad.

### 14. DEFINICIONES

De conformidad con la *Guía para la Gestión Integral del Riesgo en Entidades Públicas*, expedida por el Departamento Administrativo de la Función Pública, los conceptos técnicos en materia de gestión integral del riesgo se fundamentan en los lineamientos, principios y metodologías allí establecidos, los cuales orientan a la Región Metropolitana Bogotá - Cundinamarca en la identificación, valoración, tratamiento y seguimiento de los riesgos.

- **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.
- **Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar un aseguramiento razonable con respecto al logro de los objetivos.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del riesgo:** es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Bien de uso público:** Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejm. Las calles, plazas, puentes, vías, parques etc.
- **Bien público:** Son todos aquellos muebles e inmuebles de propiedad pública (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)
- **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. Ejm. Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.
- **Causa inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- **Conflicto de interés:** Se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011)
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos; ataca el impacto.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos; devuelve el proceso a los controles preventivos, este control ataca la probabilidad.
- **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 a las causas del riesgo, ataca la probabilidad de ocurrencia del riesgo.
- **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 8 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)
- **Daño reputacional:** Es la afectación al buen nombre y a la credibilidad en términos de integridad y transparencia, que puede sufrir la entidad pública como consecuencia de la materialización de un riesgo.
- **Debida diligencia en el conocimiento de la contraparte (debida diligencia del cliente):** proceso que le permite a la entidad conocer aspectos relevantes de sus contrapartes, sean partes vinculadas o relacionadas, para poder gestionar el riesgo que cualquier vinculación o relacionamiento genera.
- **Financiación del Terrorismo (FP):** el artículo 345 de la Ley 599 de 2000, define el delito de lavado de activos como la conducta desplegada por quien “directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a

actividades terroristas”. La Financiación del Terrorismo puede darse por: recaudación, transmisión, utilización.

- **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)
- **Fraude:** errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima. (A partir de ISO37001:2025)
- **Función de cumplimiento:** función que debe distribuirse dentro de la organización que asigna a una persona, grupo o dependencia la responsabilidad de adoptar medidas para promover el cumplimiento interno, administrar los riesgos para la integridad pública de conformidad con las políticas institucionales de gestión de riesgos, apoyar los procesos de evaluación de los Sistemas de Gestión del Riesgo, realizar un control de segunda línea y asesorar a la Alta Dirección en el direccionamiento estratégico de la organización desde un enfoque basado en riesgos para proteger la integridad pública.
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **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
- **Mapa de riesgos:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **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.
- **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.
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **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 Fiscal:** efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **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.
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgo:** efecto que, causado sobre los objetivos de las entidades, debido a eventos potenciales. 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.
- **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
- **Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP:** esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.
- **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.
- **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)
- **Vulnerabilidad:** representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

**CONTROL DE DOCUMENTOS**

<b>Versión</b>	<b>Fecha de aprobación</b>	<b>Descripción de la modificación</b>
1	15/12/2025	Creación del documento.

<b>ELABORÓ</b>	Iván Leonardo Cifuentes	Contratista	Oficina Asesora de Planeación Institucional
<b>REVISÓ TÉCNICAMENTE</b>	Camilo Peña Carbonell	Contratista	Oficina Asesora de Planeación Institucional
<b>REVISÓ METODOLÓGICAMENTE</b>	Luis Alberto Colorado Aldana	Jefe Oficina	Oficina Asesora de Planeación Institucional
<b>APROBÓ</b>	Miembros Institucionales de Coordinación de Control Interno	Comité Institucional de Coordinación de Control Interno	Comité Institucional de Coordinación de Control Interno